

Rethinking the Cyber Regulatory Framework for Data Access Consent: Legal Challenges and Reform in the Hashemite Kingdom of Jordan

Mohammed Ali Khaled Al-Shurman^{1*}, Wail Abouabaid², Hasan Jassam
Ahmed³, Maher Ali Ahmad Al-Khaldi⁴, Jamal Awwad Alkharman⁵, Hamdan
Ghunemat⁶

¹Amman Arab University, Jordan

²Abu Dhabi University, United Arab Emirates

³University of Diyala, Iraq

⁴Zarqa University, Jordan

⁵Jadara University, Jordan

⁶Al-Balqa Applied University, Jordan

*Corresponding Author: m.alshorman@aaau.edu.jo

| Received: 26-01-2026 | Revised: 28-06-2026 | Accepted: 03-08-2026 | Published On: 10-08-2026

Abstract: The rapid expansion of digital technologies and cross-border data flows has fundamentally transformed the ways in which personal data are accessed, processed, and exchanged, creating new challenges for cyber regulation and individual data rights. In the Hashemite Kingdom of Jordan, the development of data protection regulations has not yet fully addressed the legal complexities associated with data access consent, technological transformation, and emerging forms of digital exploitation. This study aims to critically examine Jordan's cyber regulatory framework governing personal data access and consent by evaluating its conceptual foundations, legislative coherence, enforcement capacity, and responsiveness to contemporary technological developments. The study employs a descriptive-analytical legal approach to examine statutory provisions, regulatory instruments, and relevant legal principles governing personal data, consent, privacy, intellectual property, and cybersecurity. A comparative approach is also employed selectively to identify regulatory practices from contemporary data protection frameworks that may inform legal reform in Jordan. The findings demonstrate a persistent regulatory gap between the pace of technological innovation and the capacity of existing legal mechanisms to provide effective and enforceable protection. Particular weaknesses emerge in the regulation of informed consent, personal data rights, data-related intellectual property interests, institutional enforcement, and cross-border data transfers. The study further finds that consent-based regulation can serve as a central mechanism for reconciling individual autonomy, data protection, and legitimate access to personal data, provided that consent is transparent, informed, specific, and effectively

Copyright (c) 2026 Mohammed Ali Khaled Al-Shurman et. al.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

enforceable. Scientifically, this study contributes a reform-oriented framework for strengthening Jordan's cyber regulatory architecture through legislative modernization, clearer institutional responsibilities, stronger cross-border cooperation, accountable data-consent platforms, technological safeguards, and enhanced public legal awareness. These reforms are essential for developing a rights-based and technologically responsive data governance regime in Jordan.

Keywords: Cyber Regulations; Cyber Space; Hashemite Kingdom of Jordan; Intellectual Property; Personal Data Rights.

INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed the ways in which personal data are collected, accessed, processed, transmitted, and exchanged.¹ Data are no longer confined to specific institutions or territorial jurisdictions but have become strategic resources circulating through interconnected digital platforms, cloud infrastructures, artificial intelligence systems, social media, and cross-border commercial networks.² This transformation has generated what may be described as a data-consent era, in which individual consent increasingly functions as a legal mechanism for determining whether and under what conditions personal data may be accessed and processed. While this development creates opportunities for innovation, economic growth, digital public services, and information exchange, it simultaneously generates complex juridical questions concerning privacy, individual autonomy, lawful access, data security, intellectual property, and accountability.³ The growing value of personal data therefore creates a fundamental regulatory dilemma: how can legal systems facilitate legitimate access to data while ensuring that individuals retain meaningful control over information relating to them?

This dilemma is particularly significant in the Hashemite Kingdom of Jordan, where digital transformation has developed rapidly alongside the expansion of cyber regulation. Jordan has progressively established a legal

¹ Enas Mohammed AlQodsi et al., 'The Legal Framework Governing Personal Data Protection: Challenges and Mechanisms for Enhancing Security in the Digital Age—an Analytical Study', *Security Journal* 39, no. 1 (June 2026): 37, <https://doi.org/10.1057/s41284-026-00547-y>.

² Daniel Chibuike Okoro, 'An Evaluation of Cybersecurity Frameworks and Privacy Regulations for Companies in the Digital Age: A Legal Approach', *Asian Journal of Economics, Business and Accounting* 25, no. 4 (April 2025): 431–440, <https://doi.org/10.9734/ajebe/2025/v25i41761>.

³ Rand Al-Dmour et al., 'Impact of AI and Big Data Analytics on Healthcare Outcomes: An Empirical Study in Jordanian Healthcare Institutions', *Digital Health* 11 (January 2025): 20552076241311051, <https://doi.org/10.1177/20552076241311051>.

framework to respond to cybercrime, digital security, and personal data protection.⁴ The Cybercrime Law, initially enacted in 2010 and subsequently amended, provides a legal basis for addressing unauthorized access to data, hacking, online fraud, and other forms of cyber-related misconduct. Its broader objective is to protect individuals and digital systems against the misuse and exploitation of information in an increasingly interconnected environment. However, the rapid development of digital technologies has generated regulatory challenges that cannot be fully addressed through a traditional cybercrime-oriented framework.⁵ The central issue is no longer merely whether unauthorized access constitutes an offence, but also whether access that is formally authorized through consent is genuinely informed, voluntary, specific, transparent, and capable of being withdrawn.

Jordan took an important legislative step through Law No. 24 of 2023 on Personal Data Protection, published in the Official Gazette on 17 September 2023 and becoming effective on 17 March 2024. The law represents a significant development in Jordan's data governance architecture because it regulates the processing of personal and sensitive data and extends its application to certain controllers located outside Jordan. It also addresses domestic and cross-border data transfers and recognizes several individual rights, including the right to information, access, correction, objection, withdrawal of consent, restriction of processing, erasure, and data portability. In principle, these provisions establish a rights-based framework capable of strengthening individual control over personal information.⁶ The law further requires consent to be explicit, informed, and documented before personal data are processed unless a legally recognized exception applies.

Nevertheless, the existence of statutory rights does not necessarily guarantee effective protection in practice. The rapid evolution of artificial intelligence, cloud computing, biometric identification, social media, and automated data processing creates circumstances in which individuals may formally provide consent without possessing meaningful knowledge of how their information will subsequently be used, shared, transferred, or combined with

⁴ Tahegga Primananda Alfath and Waskita Cahya, 'Bridging the Gap Between Policy and Practice: Evaluating Indonesia's Cybersecurity Regulatory Framework (2020–2023)', *Data : Journal of Information Systems and Management* 2, no. 1 (January 2024): 14–24, <https://doi.org/10.61978/data.v2i1.695>.

⁵ Mohammad Airout, 'Criminal Protection Against Cybercrime: A Comparative Legal Analysis of Jordanian, Arab, and International Legislations', *Journal of Posthumanism* 5, no. 4 (2025): 1459–1472.

⁶ Jasmin Gider, Luc Renneboog, and Tal Strauss, 'The Regulation of Data Privacy and Cybersecurity', *Annals of Corporate Governance* 10, no. 1 (May 2026): 1–101, <https://doi.org/10.1108/ACG-07-2025-0050>.

other datasets.⁷ Consent may consequently become a formal procedural requirement rather than a substantive expression of individual autonomy. The problem becomes more complicated when access to essential digital or public services is dependent upon the acceptance of data-processing conditions, raising questions about whether consent remains genuinely voluntary.⁸ Cross-border data transfers further complicate this issue because personal information may be processed beyond Jordanian territory under regulatory regimes that provide different levels of protection and enforcement.

Recent scholarship has begun to examine these developments, but important analytical gaps remain. Ababneh et al. (2026)⁹, in their multidimensional perspective on cyber risk regulation, demonstrate that cybersecurity has evolved from a predominantly technical concern into a broader legal and ethical governance issue. Their study compares regulatory approaches concerning cybersecurity, cybercrime, due diligence, privacy, and cross-border data governance and emphasizes the importance of integrating data protection with ethical principles and emerging technologies. However, their analysis remains primarily comparative and macro-regulatory, addressing cyber risk regulation across jurisdictions rather than examining the specific legal architecture of consent-based personal data access in Jordan. Consequently, the question of whether individual consent provides an effective legal mechanism for balancing data access and personal autonomy within Jordan's regulatory system remains insufficiently explored.

A second relevant study by Hamdon and Al Smadi (2026) examines digital transformation, social media platforms, media policies, and digital security in Jordan between 2020 and 2025.¹⁰ Their findings identify tensions between cybersecurity objectives and fundamental freedoms, particularly freedom of expression, and characterize aspects of Jordan's regulatory development as reflecting a form of digital authoritarian governance. The study consequently calls for a more balanced model of digital governance that can reconcile security with

⁷ Eddy Sumartono et al., 'The Legal Implications of Data Privacy Laws, Cybersecurity Regulations, and AI Ethics in a Digital Society', *The Journal of Academic Science* 1, no. 2 (July 2024): 103–110, <https://doi.org/10.59613/29qypw51>.

⁸ Louise Thomas et al., 'A Framework for Data Privacy and Security Accountability in Data Breach Communications', *Computers & Security* 116 (May 2022): 102657, <https://doi.org/10.1016/j.cose.2022.102657>.

⁹ Jafar Ababneh et al., 'Cybersecurity Laws, Digital Crimes, and Ethical Considerations: A Multidimensional Perspective on Cyber Risk Regulation (MPoCRR)', *Journal of Cloud Computing* 15, no. 1 (June 2026): 91, <https://doi.org/10.1186/s13677-025-00824-y>.

¹⁰ 'Digital Transformation, Social Media Platforms, and the Reshaping of Media Policies in Jordan (2020–2025): A Political-Legal Approach to Governance, Legitimacy, and Digital Security | Request PDF', *ResearchGate*, ahead of print, 19 May 2026, <https://doi.org/10.57239/prn.26.03410082>.

individual rights. Although this research provides important insights into Jordan's broader cyber governance environment, its principal concern is media regulation, freedom of expression, and the political dimensions of cybersecurity. It does not specifically examine personal data consent as an independent legal institution or investigate the relationship between consent, data access rights, data controllers, and cross-border processing under the Personal Data Protection Law of 2023.

The third study, Al-Hussaini (2026), provides a more direct examination of Jordan's Personal Data Protection Law by critically analyzing the relationship between digital governance and fundamental rights.¹¹ The study highlights tensions between the statutory guarantees contained in the Personal Data Protection Law and their implementation, particularly in relation to the mandatory Sanad digital identity system. It also raises concerns regarding the institutional autonomy of the Personal Data Protection Council, governmental influence, consent requirements, and the potential erosion of privacy through compulsory biometric registration. This research is particularly important because it demonstrates that formal recognition of data rights does not automatically translate into effective protection. Nevertheless, its principal emphasis is on governmental digital governance, institutional autonomy, and fundamental rights. It does not develop a comprehensive legal reconstruction of consent as a mechanism for regulating lawful data access, nor does it systematically connect consent regulation with cross-border data flows, data-related intellectual property interests, technological safeguards, and the responsibilities of private data-consent platforms.

These three studies collectively demonstrate the existence of a significant research gap. Existing scholarship has examined cyber risk regulation from a comparative perspective, digital governance and media freedom in Jordan, and the fundamental-rights implications of Jordan's Personal Data Protection Law. However, insufficient attention has been given to the specific legal architecture of data access consent as the intersection between cybersecurity regulation, personal data protection, individual autonomy, and legitimate access to information in Jordan. This gap is increasingly important because the effectiveness of data protection depends not only on prohibiting unauthorized access but also on establishing clear legal standards for authorized access. In other words, the central regulatory question has shifted from "who may access data?" to "under what legal conditions may data be accessed, on what basis is

¹¹ Tuffaha Al Hussaini Rand Ihab M. H, 'Digital Governance and Fundamental Rights: A Critical Analysis of Jordan's Data Protection Law', *PERSPECTIVES OF LAW AND PUBLIC ADMINISTRATION* 15, no. 1 (2026): 26–49, <https://doi.org/10.62768/PLPA/2026/15/1/02>.

consent valid, and what safeguards remain applicable after consent has been provided?”

Against this background, this study seeks to rethink Jordan’s cyber regulatory framework by placing data access consent at the center of the legal analysis. Unlike previous studies that predominantly examine cybersecurity, digital governance, or fundamental rights separately, this research integrates these dimensions into a single legal framework and evaluates whether the existing regulatory structure is sufficiently capable of protecting individual data rights while enabling legitimate data access. The novelty of the study lies in proposing a consent-centered and rights-based reconstruction of Jordan’s cyber regulatory framework, connecting substantive consent requirements with institutional accountability, cross-border data governance, technological safeguards, and effective enforcement. The study therefore moves beyond assessing whether Jordan has enacted data protection legislation and instead evaluates whether the existing framework provides meaningful legal control over the entire lifecycle of consent and data access.

Accordingly, this study addresses the following research question: How should Jordan’s cyber regulatory framework be reformed to ensure that data access consent provides effective protection for personal data rights while facilitating legitimate and technologically responsive access to data? The significance of this research is both theoretical and practical. Theoretically, it contributes to contemporary cyber law and data governance scholarship by conceptualizing consent not merely as a procedural requirement for lawful processing but as a substantive mechanism for protecting autonomy, privacy, and accountability in digital environments. Practically, the study provides a legal basis for strengthening Jordan’s regulatory framework through clearer standards of informed and revocable consent, stronger institutional oversight, improved regulation of data-consent platforms, enhanced safeguards for cross-border data transfers, and greater use of technological mechanisms to support compliance and accountability. The findings are expected to contribute to the development of a more coherent and adaptive regulatory model capable of reconciling cybersecurity, innovation, legitimate data access, and individual rights. In this respect, Jordan’s experience offers a broader contribution to jurisdictions confronting similar challenges in adapting traditional legal frameworks to the rapidly changing realities of data-driven societies.

METHOD

This study employs a qualitative doctrinal legal research design to critically examine the legal framework governing data access consent and personal data protection in the Hashemite Kingdom of Jordan. The doctrinal approach is used to analyze statutory provisions, legal principles, regulatory

instruments, and relevant jurisprudential concepts concerning personal data, consent, privacy, cybersecurity, and cross-border data processing. The primary legal materials consist principally of Jordan's Personal Data Protection Law No. 24 of 2023, the Jordanian Cybercrime Law and its amendments, relevant implementing regulations, and other official regulatory instruments governing personal data processing and cyber governance. Secondary legal materials include peer-reviewed journal articles, scholarly books, legal commentaries, theses, research reports, and comparative studies concerning data protection and consent-based data governance. The literature and supporting legal materials were collected through systematic document searching in Scopus, Web of Science (WoS), Google Scholar, and relevant official governmental and institutional repositories. Searches employed combinations of keywords including "Jordan Personal Data Protection Law," "data access consent," "personal data protection," "cyber regulation," "data governance," "privacy," "cross-border data transfer," and "consent." Materials were selected based on their relevance to the research question, legal authority, scholarly quality, and substantive contribution to understanding data consent and personal data governance in Jordan. Materials that addressed cybersecurity or digital technology only generally without substantive relevance to personal data protection or consent were excluded.

The collected materials were analyzed using qualitative thematic content analysis through a structured process of identification, classification, interpretation, and synthesis. The analysis focused on four interconnected themes: the legal status and requirements of data access consent; the rights of data subjects and corresponding obligations of data controllers; institutional and enforcement mechanisms for personal data protection; and regulatory challenges arising from technological development and cross-border data processing. Particular attention was given to Article 4 of Jordan's Personal Data Protection Law No. 24 of 2023 and related provisions concerning explicit, informed, and documented consent, access rights, withdrawal of consent, data security, and lawful processing. A limited comparative analysis was also undertaken to contextualize Jordan's framework against contemporary international data protection principles, particularly those reflected in the EU General Data Protection Regulation (GDPR), without treating foreign legislation as directly applicable law. Data interpretation was guided by a rights-based and consent-centered analytical framework, assessing whether Jordan's existing regulations provide meaningful individual autonomy while allowing legitimate and proportionate access to personal data. The validity of the legal analysis was strengthened through source triangulation by comparing primary legislation and official regulatory materials with authoritative secondary literature and relevant comparative legal scholarship. Interpretive consistency was further maintained

through cross-checking legal provisions against established principles of privacy, informed consent, accountability, proportionality, and data protection. This validation process enabled the study to distinguish between the formal existence of legal protections and their substantive capacity to provide effective protection in Jordan's evolving digital environment.

RESULTS AND DISCUSSION

The Legal Paradigm between theory and practice:

Subsequently, Jordan faces a major issue regarding the educational and training programs needed to prepare professionals to work in an environment that increasingly relies on artificial intelligence. Legislation and regulatory policies must be implemented to ensure the ethical and responsible use of artificial intelligence. Research and development in personal data protection consent must be supported to ensure this technology develops in ways that benefit everyone.¹² The public is unfortunately oblivious to the uses, benefits, and risks of seeking consent for the use of personal data, leading to typical hysteria, which circumvents realistic engagement.¹³ Therefore, the Ministry of Digital Economy and Entrepreneurship in Jordan adopts technologies that are scientifically and methodologically compatible with data protection to develop a smart administration capable of achieving the state's vision and mission of providing services to citizens at a quality and cost that match their financial situation.¹⁴

The core issue is to narrow down the gap of theory and practice, as Jordan is located in a volatile region of the globe, where adversaries next door can cause substantial damage to the critical infrastructure of the country, with a small population of under 30 Million, all citizens of the country must protect their personal data, and must not remain in oblivion, when seeking consent for data usage is concerned.¹⁵ Personal Data Rights in Cyber Space and the Associated Legal Challenge of The regulation of Personal Data rights in the case of Data consent is associated with several legal problems because the Data

¹² Mazen Hasan Basha, 'Digitization and the Recovery of Economy: Evidence from Jordan', in *From Machine Learning to Artificial Intelligence: The Modern Machine Intelligence Approach for Financial and Economic Inclusion*, ed. Abdalmuttaleb M. A. Musleh Al-Sartawi et al. (Cham: Springer Nature Switzerland, 2025), 461–470, https://doi.org/10.1007/978-3-031-76011-2_31.

¹³ 'Jordanian Cybercrime Law No. (17) of 2023 between Regulating Social Media Sites and Restricting Freedom of Opinion', *ResearchGate*, ahead of print, 17 June 2026, <https://doi.org/10.36348/sijlcj.2024.v07i09.002>.

¹⁴ Khaled Khwaileh, 'Digital Diplomacy in the Middle East: Jordan's Role in Regional Digital Trade Integration', SSRN Scholarly Paper no. 5906354 (Rochester, NY: Social Science Research Network, 12 December 2025), <https://doi.org/10.2139/ssrn.5906354>.

¹⁵ Obieda Altobaishat et al., 'Examining the Burden of Mental Disorders in Jordan: An Ecological Study over Three Decades', *BMC Psychiatry* 25, no. 1 (March 2025): 218, <https://doi.org/10.1186/s12888-025-06658-x>.

consent environment is constantly changing, as are approaches to creating and distributing Data consent information. The following section analyzes the influence of the Data consent revolution on Personal Data rights by considering the key legal problems that have emerged from the spread of Data consent.

Table 1. Key Legal Challenges, Research Gaps, and Regulatory Recommendations for Data Access Consent in Jordan

Subsection	Key Focus	Main Issues Identified	Implications / Recommendations
The Inevitable Research Question	Gap between technological advancements in electronic Personal Data and legislative protections	- Inadequate legal protection for electronic Personal Data - Unnecessary limitations on individuals communicating data electronically - Difficulty of legal authority adapting to new technology	- Implement protective measures in Jordan to mitigate negative impacts of data consent - Strengthen legislative adaptability to technological change
The Legal Paradigm Between Theory and Practice	Preparing professionals and institutions for AI-driven environments	- Lack of educational/training programs for AI ethics and responsible use - Public obliviousness to risks/benefits of data consent - Hysteria undermines realistic engagement	- Support R&D in personal data protection consent - Implement legislation ensuring ethical AI use - Ministry of Digital Economy to adopt scientifically compatible technologies for smart administration
The Crux of Our Discussion	Bridging the gap between theory and practice in a volatile geopolitical context	- Vulnerability of critical infrastructure in Jordan - Citizens unaware of personal data risks - Constantly changing data consent environment creates legal challenges	- Promote citizen awareness of personal data rights - Develop adaptive legal frameworks for evolving consent practices - Strengthen resilience of national infrastructure through robust data governance

Table 1 illustrates three interconnected dimensions of the legal challenges surrounding data access consent in Jordan. The first dimension, the Inevitable Research Question, highlights the widening gap between rapid technological developments in electronic personal data and the capacity of existing legislative protections to respond effectively. The increasing volume, speed, and complexity of digital data processing create circumstances in which conventional legal

mechanisms may provide insufficient protection while simultaneously imposing unnecessary restrictions on legitimate electronic communication.¹⁶ This situation demonstrates that the principal challenge is not merely the existence of legal rules, but their ability to remain adaptive to technological change. The second dimension, The Legal Paradigm Between Theory and Practice, emphasizes the institutional and human-capacity challenges associated with AI-driven digital environments. The absence of adequate education and training concerning AI ethics, responsible data use, and consent contributes to limited public understanding of both the risks and potential benefits of personal data processing. Consequently, regulatory responses may be influenced by technological anxiety rather than evidence-based legal and policy considerations. The table therefore identifies the need for stronger research and development, ethical AI regulation, and institutional capacity within Jordan's digital governance framework.

The third dimension, The Crux of Our Discussion, brings these legal and institutional challenges together by focusing on the need to bridge the gap between normative principles and their practical implementation within a rapidly changing geopolitical and technological environment. Jordan's critical digital infrastructure remains exposed to evolving cyber risks, while limited public awareness may weaken individuals' ability to exercise their rights effectively. At the same time, constantly changing data-processing practices create difficulties for static regulatory frameworks, particularly concerning the validity, scope, and withdrawal of consent. The table consequently indicates that meaningful reform requires more than legislative amendment alone. Jordan needs an adaptive and rights-based regulatory framework supported by public awareness, institutional accountability, technological resilience, and robust data governance. Taken together, these findings reinforce the central argument of this study that data access consent should be treated as a substantive mechanism of personal autonomy and data protection rather than merely as a formal condition for lawful data processing. Such an approach can help reconcile legitimate access to personal data with privacy, cybersecurity, technological innovation, and fundamental individual rights.

Data Consent Transformation and Its Impact on Personal Data

Data consent transformation entails integrating Data consent technologies across all spheres of social and economic life, resulting in a radical

¹⁶ Bambang Suheryadi et al., 'Bridging Legal Traditions in Consumer Protection: Criminal Liability in Comparative Jurisprudence and Contemporary Islamic Law', *MILRev: Metro Islamic Law Review* 5, no. 1 (April 2026): 492–532, <https://doi.org/10.32332/milrev.v5i1.12863>.

change in how Personal Data is generated and shared.¹⁷ In sectors such as education, science, and creativity, the use of Data consent media has become virtually mandatory, creating a new landscape for information and Personal Data exchange.

While Data consent transformation plays an important role in the swift and efficient sharing of Personal Data, it also creates a complicated environment filled with legal issues. First, there is a need to develop regulations that effectively protect Personal Data rights in a non-territorial space and clarify the obligations of the actors involved in generating and using Data consent Personal Data. Additionally, the rise of sharing websites that allow individuals to post content without adhering to conventional restrictions exacerbates these difficulties.

Legal Challenges of Consent to Personal Data Rights

The legal implications of consent to personal data rights pose many challenges that may prevent their effective use in the current Data consent era. The rapid technological advancement in AI and digitization has made it difficult to determine how intellectual property rights can coexist with the rights of persons and companies.¹⁸ Furthermore, owing to this rapid development, it has become imperative that new laws be introduced and existing laws be updated to address cross-border Data consent crimes and keep pace with these changes. Personal Data protection intersects with privacy rights due to the risks posed by the collection, analysis, and use of personal data. In recent years, scholars have stressed the importance of developing constitutional approaches to ensuring personal data privacy within the broader framework of Personal Data rights, as the growth of Data consent surveillance and data processing can infringe upon basic rights without proper legal measures. The implementation of Data consent Personal Data rights laws can be problematic because there is limited capacity to enforce compliance with Data consent content and to address rights violations across national borders. Territorial limitations within domestic legal frameworks hinder efforts to address violations that occur across multiple jurisdictions unless adequate international cooperation is in place. In addition, some Data consent forums do not collaborate with IP law enforcement agencies, further compounding shortcomings in the protection of Data consent rights. In this fast-changing technological environment, it is now very important to examine both the current legal framework that protects Data consent and personal data rights

¹⁷ Mohamed Abouyounes, 'The Legal Underpinnings of Jordanian and Iraqi Law's Administrative Penalty Systems', *Al-Biruni Journal of Humanities and Social Sciences* 3, no. 9 (September 2025): 1, <https://doi.org/10.64440/BIRUNI/BIR003>.

¹⁸ Zainab Al-Mousawi, 'The Transformation of the Legal Basis of Administrative Liability for Public Employees' Errors in Administrative Contracts: A Comparative Study in Light of the Evolution of Administrative Judiciary and Public Governance', *Al-Biruni Journal of Humanities and Social Sciences*, 9 February 2026, 1, <https://doi.org/10.64440/BIRUNI/BIR0013>.

and the mechanisms a regulatory model can implement to protect them. This section will focus on legislative and institutional models for protecting Data consent rights, as well as practical models of how the Cyber Regulations structure operates and whether it adequately addresses new issues.

Mechanisms for Implementing Cyber Regulations of Personal Data Rights

Judicial systems play a very important role in defending the rights to Data consent Personal Data by enforcing Data consent laws regarding data privacy and intellectual property.¹⁹ Some countries have also created specialized courts to address Data consent intellectual property litigation, helping speed up Data consent dispute resolution. Research has shown that judicial support enhances Data consent innovation by allowing businesses and creators to protect their rights against threats. However, there are still major obstacles to cross-border enforcement due to differing definitions and methodologies used within each jurisdiction's legal system to define rights and methods of protection. Therefore, cross-border prosecutions involving Data consent crimes will require cooperation between the executive and legislative branches of government at the state level. Data consent platforms have become key players in ensuring that legal regulation of Personal Data rights is implemented through terms of use agreements for users and technical protection methods such as DRM (Data consent rights management), both of which serve as means of regulating usage.²⁰ The platforms regulate content monitoring and dispute resolution related to their use, while simultaneously seeking to balance free publication with the protection of intellectual property, as multimedia platforms thus provide a self-regulatory mechanism for the flow of information on the Internet.²¹ The platform model, however, has come under significant scrutiny. Consequently, they can enforce excessively stringent levels of protection, thereby limiting individuals' ability to access Personal Data freely. Alternatively, enforcement models may be insufficiently developed to address sophisticated technological misuse. This

¹⁹ Denny Suwondo et al., 'Consumer Legal Protection Against Standard Clauses in Contemporary Peer-To-Peer Lending: An Islamic Economic Law Perspective', *MILRev: Metro Islamic Law Review* 5, no. 2 (August 2026): 1296–1329, <https://doi.org/10.32332/milrev.v5i2.12643>.

²⁰ Rand Al-Dmour et al., 'Impact of AI and Big Data Analytics on Healthcare Outcomes: An Empirical Study in Jordanian Healthcare Institutions', *DIGITAL HEALTH* 11 (May 2025): 20552076241311051, <https://doi.org/10.1177/20552076241311051>.

²¹ Konstantinos Tsimachidis, 'Self-Regulation in Digital Exercise: Perceived Service Quality and Connectivity as Predictors of Autonomous Motivation', *International Journal of Physical Education, Sports and Health* 12, no. 6 (2025): 620–626, <https://doi.org/10.22271/kheljournal.2025.v12.i6i.4154>.

necessitates involvement from both government agencies and Data consent platforms.²²

The Need to Update Legislative Frameworks

A major finding in current legal scholarship is that traditional lawmaking is limited in its ability to address the complex issues posed by a Data-consent-advanced society, especially in areas such as intellectual property, data, and cross-border Data-consent services.²³ Some authors have emphasized the need for adaptable legal structures that can continually evolve to accommodate rapid technological change and avoid relying on static legal codes that quickly become outdated. Updating statutory law involves integrating principles from Data consent, human rights, data protection, and traditional IP law into coherent statutes that provide a framework for emerging technologies such as AI and Blockchain. Updating statutory law also requires engaging scientific/technical disciplines in its development, rather than merely allowing it to be developed through existing legislative institutions.²⁴

Strengthening International Cooperation to Harmonize Legal Standards

A lack of coordination in protecting Data consent and personal data rights across national legal systems will continue to impede international cooperation, as significant gaps remain in the legislation governing their enforcement. It would appear necessary, therefore, to establish an international framework for coordinating the development of national laws and to revise agreements currently in force (such as the TRIPS agreement) and similar treaties to provide clear language on the rights of Data consent producers and the obligations placed upon companies that operate the world's largest Data consent networks.²⁵ There has been significant interest in improving IP protections and developing best practices for all countries. Evidence of this can be seen in the holding of international meetings and conferences that attract public

²² Baker Akram Falah Jarah et al., 'Review of the Literature Related to Audit Quality and Integrated Reporting Quality in Jordanian Companies', *Edelweiss Applied Science and Technology* 8, no. 6 (September 2024): 124–133, <https://doi.org/10.55214/25768484.v8i6.2029>.

²³ Nibrosu Rohid et al., 'Reconstructing the Legal Enforcement Framework for Digital Activism in an Era of Technological Disruption', *Nusantara: Journal of Law Studies* 5, no. 2 (July 2026): 881–901, <https://doi.org/10.66325/nusantaralaw.v5i2.236>.

²⁴ Ma'en Juwaihian, Hamzeh Abu Issa, and Mohammad Nasr Khater, 'The Crime of Counterfeiting or Imitating a Trademark under Jordanian Trademarks Law', *The Journal of World Intellectual Property* 28, no. 2 (2025): 589–611, <https://doi.org/10.1111/jwip.12346>.

²⁵ Andrew Mazen Dahdal and Adel Abdel Ghafar, 'The Digital Silk Road: "Tech-Diplomacy" as a Paradigm for Understanding Technological Adoption and Emerging Digital Regulations in MENA', *Asian Journal of Law and Society* 12, no. 2 (June 2025): 163–188, <https://doi.org/10.1017/als.2024.30>.

policymakers and academics, who discuss IP protections for developing technologies.

Promoting Data Consent Legal Education and Awareness

Cyber Regulations of the Internet go beyond the development of legislative tools and public institutions. It involves creating a legal Data consent culture by raising awareness and providing training among several stakeholders, such as private citizens, artists, businesses, and lawmakers.²⁶ Promoting understanding of the importance of Personal Data rights on the Internet can contribute to greater compliance with applicable laws and fewer unintended breaches.²⁷ Technological advancements in governance, whether at the federal or local level, can assist authorities in monitoring Data consent IPRs (intellectual property rights) more effectively; provide evidence of the originality of Data consent content; and facilitate quicker and more transparent enforcement of those rights.²⁸

Additionally, it strengthens that incorporating technology into the governance of laws helps eliminate administrative corruption on Data consent platforms and strengthens self-governance on these platforms, which together create an environment where trust and security enable the sharing of information.²⁹ Henceforth, Personal Data may be readily accessible to third parties, potentially harming their reputations. The so-called right to be forgotten was established in response to people's urge to have information previously published about them removed. This issue has arisen in light of the development of digital publication.³⁰ The absence of legal texts that protect this right, and occasionally the existence of legal texts that may contradict this right, such as the right to freedom of expression and the controversy about the practicality of

²⁶ Isabella Rose M. Harding, 'Governance, Transparency, and Financial Regulation in the Global Digital Economy', *Journal of Nusantara Economy* 4, no. 2 (December 2025): 112–134, <https://doi.org/10.66325/nusantaraeconomy.v4i2.368>.

²⁷ Muhammad Azam et al., 'AI-Driven Sharia Governance in Islamic Digital Payment Systems: Developing a Contemporary Islamic Law Framework for Ethical and Regulatory Compliance', *Nusantara: Journal of Law Studies* 5, no. 2 (July 2026): 849–880, <https://doi.org/10.66325/nusantaralaw.v5i2.339>.

²⁸ 'Criminal Protection to the Digital Right to Be Forgotten in Jordan', *International Journal of Electronic Security and Digital Forensics*, n.d., accessed 10 August 2026, <https://www.inderscienceonline.com/doi/10.1504/IJESDF.2025.145865>.

²⁹ Dr Mamdouh Mohd Mamdouh Alresheidat and Mohammad Awad Hammad Zubid, 'Authenticity Of Ordinary Bond In Evidence Payment: A Case Study Of Jordan Law', *Lex Localis - Journal of Local Self-Government* 23, no. S6 (October 2025): 484–495, <https://doi.org/10.52152/rpfm9917>.

³⁰ Andrii Volodymyrovych Shevchenko, 'International Trade, Investment Flows, and Economic Integration between Asia-Pacific and Europe', *Journal of Nusantara Economy* 4, no. 2 (December 2025): 135–159, <https://doi.org/10.66325/nusantaraeconomy.v4i2.383>.

establishing a right to be forgotten, are among the issues that may affect or prevent the enjoyment of this right and expose it to a violation.³¹ The most significant barrier to implementing effective Internet governance policies is likely the lack of understanding of the legal goals of Internet transformation; therefore, there is an increasing demand for specialized educational courses on the subject.³²

Key Findings on Data Access Consent and Cyber Regulatory Challenges in Jordan

The study finds that legal regulation remains the most effective mechanism for protecting data access consent and personal data rights, particularly because an effective regulatory framework incorporates transparency, accountability, legal certainty, and the rule of law. However, the existence of formal legal provisions does not necessarily guarantee effective protection. Significant weaknesses remain in both the legislative design and enforcement mechanisms, particularly in translating statutory consent requirements into meaningful protection for data subjects. The findings further demonstrate a substantial disparity between the rapid development of technologies used to create, collect, distribute, process, and utilize personal data and the capacity of traditional legal frameworks to regulate these developments. Existing regulations often fail to adequately accommodate the distinctive characteristics of contemporary digital environments, including automated processing, artificial intelligence, platform-based data ecosystems, and rapidly evolving forms of data sharing. This regulatory lag consequently reduces the practical effectiveness of legal protection and creates uncertainty regarding the rights and responsibilities of individuals, data controllers, and other digital actors.

The study also identifies significant challenges concerning data-related intellectual property and accountability, particularly the ease with which digital content and personal data can be reproduced and redistributed and the difficulty of determining liability when artificial intelligence is involved in generating or processing digital content. At the same time, data-consent and digital platform providers increasingly exercise a form of indirect regulatory power through their terms of service, privacy policies, content-management practices, and data-access mechanisms. Although these practices influence how personal data are accessed and used, their regulatory legitimacy and effectiveness remain limited in the absence of clear public-law oversight. A further challenge arises from the cross-

³¹ AbdelKarim Fawwaz AlBataineh, 'The Effect of Smart Contracts (Blockchain Technology) on Jordan's Land Registry and Survey Department for Sustainable Development', *Discover Sustainability* 6, no. 1 (February 2025): 69, <https://doi.org/10.1007/s43621-025-00797-7>.

³² Farouq Ahmad Faleh Alazzam and Khaled Khalaf Abed Rabbo Aldrou, 'Artificial Intelligence and Data Privacy in International Trade Law', *Multidisciplinary Science Journal* 7, no. 8 (February 2025): 2025379–2025379, <https://doi.org/10.31893/multiscience.2025379>.

border nature of contemporary data flows. Differences among national legislation, divergent standards of consent and data protection, and weak mechanisms for international enforcement make it difficult to provide consistent protection for personal data beyond Jordanian jurisdiction. Taken together, these findings indicate that Jordan requires a more adaptive, rights-based, and technologically responsive cyber regulatory framework that combines effective legislative protection, stronger institutional enforcement, accountable platform governance, clearer liability rules for AI-related data processing, and enhanced international cooperation. Such reforms are essential to ensure that data access consent operates as a substantive safeguard for individual autonomy and personal data rights rather than merely as a formal requirement for lawful data processing.

CONCLUSION

This study concludes that Jordan's existing cyber regulatory framework provides an important legal foundation for addressing cybercrime and protecting personal data, but significant gaps remain between statutory protection and the realities of a rapidly evolving digital environment. The findings demonstrate that the effectiveness of data access consent depends not only on the formal recognition of individual rights but also on transparency, accountability, enforceability, and institutional capacity. In particular, weaknesses remain in the regulation of informed and meaningful consent, data minimization, purpose limitation, data-breach notification, individual rights to access, rectify, erase, and withdraw consent, platform accountability, and cross-border data governance. The study therefore argues that Jordan's framework should be progressively harmonized with internationally recognized data protection principles, including those reflected in the EU GDPR, while remaining responsive to Jordan's own legal and institutional context. Stronger enforcement mechanisms, clearer liability standards, consistent sanctions, independent oversight, and international cooperation are also necessary to ensure that personal data rights remain effectively protected across increasingly borderless digital networks.

Future research should move beyond doctrinal assessment by empirically examining how government institutions, private-sector data controllers, digital platforms, and other stakeholders in Jordan implement the Personal Data Protection Law and related cyber regulations. Particular attention should be given to whether consent is genuinely informed and voluntary in practice, how individuals exercise their rights, and how regulatory authorities respond to data breaches, AI-driven processing, and cross-border data transfers. Comparative research involving Jordan and other Middle Eastern jurisdictions, as well as longitudinal studies of regulatory implementation following the enactment of the Personal Data Protection Law, would also provide valuable evidence regarding the effectiveness of ongoing reforms. Such research could further investigate the

relationship between technological innovation, public awareness, institutional independence, and regulatory enforcement, thereby contributing to the development of an adaptive, rights-based, and technologically responsive cyber governance model for Jordan and comparable jurisdictions.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Rector and the entire academic community of Amman Arab University, Jordan, for their valuable support, institutional assistance, and academic environment throughout the completion of this research. The authors also appreciate the contributions and encouragement of colleagues and academic staff whose insights and support helped facilitate the research process. Their institutional and academic support has been instrumental in the successful completion of this study.

AUTHOR CONTRIBUTIONS STATEMENT

Mohammed Ali Khaled Al-Shurman contributed to the conceptualization of the study, development of the research framework, and formulation of the research objectives. Wail Abouabaid contributed to the literature review, analysis of relevant legal and regulatory frameworks, and interpretation of the findings. Hasan Jassam Ahmed contributed to the research methodology, collection and examination of legal materials, and the analytical process. Maher Ali Ahmad Al-Khaldi contributed to the comparative legal analysis, critical interpretation of the results, and development of the theoretical discussion. Jamal Awwad Alkharman contributed to the drafting and substantive revision of the manuscript, including the integration of scholarly arguments and recommendations. Hamdan Ghunemat contributed to manuscript editing, review of the final version, and refinement of the conclusions and policy implications. All authors participated in reviewing and revising the manuscript, approved the final version, and agreed to be accountable for all aspects of the work.

AI USAGE STATEMENT

The authors acknowledge the use of artificial intelligence (AI)-assisted tools during the preparation of this manuscript, particularly for language refinement, grammar checking, and improving the clarity and readability of the English language. AI tools were not used to generate or determine the research findings, legal analysis, interpretations, conclusions, or scholarly arguments. All substantive content was independently reviewed, verified, and validated by the authors. The authors take full responsibility for the accuracy, originality, integrity, and academic content of the manuscript and remain accountable for any errors or omissions.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest, whether financial, personal, professional, or institutional, that could have influenced the research, analysis, interpretation of the findings, or publication of this manuscript.

REFERENCES

- Ababneh, Jafar, Abdulmajeed Alzara, Hani Attar, Ala'a Al-Shaikh, Amer Abu-Jassar, and Mohamed Hafez. 'Cybersecurity Laws, Digital Crimes, and Ethical Considerations: A Multidimensional Perspective on Cyber Risk Regulation (MPoCRR)'. *Journal of Cloud Computing* 15, no. 1 (June 2026): 91. <https://doi.org/10.1186/s13677-025-00824-y>.
- Abouyounes, Mohamed. 'The Legal Underpinnings of Jordanian and Iraqi Law's Administrative Penalty Systems'. *Al-Biruni Journal of Humanities and Social Sciences* 3, no. 9 (September 2025): 1. <https://doi.org/10.64440/BIRUNI/BIR003>.
- Airout, Mohammad. 'Criminal Protection Against Cybercrime: A Comparative Legal Analysis of Jordanian, Arab, and International Legislations'. *Journal of Posthumanism* 5, no. 4 (2025): 1459–1472.
- Alazzam, Farouq Ahmad Faleh, and Khaled Khalaf Abed Rabbo Aldrou. 'Artificial Intelligence and Data Privacy in International Trade Law'. *Multidisciplinary Science Journal* 7, no. 8 (February 2025): 2025379–2025379. <https://doi.org/10.31893/multiscience.2025379>.
- AlBataineh, AbdelKarim Fawwaz. 'The Effect of Smart Contracts (Blockchain Technology) on Jordan's Land Registry and Survey Department for Sustainable Development'. *Discover Sustainability* 6, no. 1 (February 2025): 69. <https://doi.org/10.1007/s43621-025-00797-7>.
- Al-Dmour, Rand, Hani Al-Dmour, Eatedal Basheer Amin, and Ahmed Al-Dmour. 'Impact of AI and Big Data Analytics on Healthcare Outcomes: An Empirical Study in Jordanian Healthcare Institutions'. *Digital Health* 11 (January 2025): 20552076241311051. <https://doi.org/10.1177/20552076241311051>.
- . 'Impact of AI and Big Data Analytics on Healthcare Outcomes: An Empirical Study in Jordanian Healthcare Institutions'. *DIGITAL*

HEALTH 11 (May 2025): 20552076241311051.
<https://doi.org/10.1177/20552076241311051>.

Alfath, Tahegga Primananda, and Waskita Cahya. 'Bridging the Gap Between Policy and Practice: Evaluating Indonesia's Cybersecurity Regulatory Framework (2020–2023)'. *Data: Journal of Information Systems and Management* 2, no. 1 (January 2024): 14–24.
<https://doi.org/10.61978/data.v2i1.695>.

Al-Mousawi, Zainab. 'The Transformation of the Legal Basis of Administrative Liability for Public Employees' Errors in Administrative Contracts: A Comparative Study in Light of the Evolution of Administrative Judiciary and Public Governance'. *Al-Biruni Journal of Humanities and Social Sciences*, 9 February 2026, 1. <https://doi.org/10.64440/BIRUNI/BIR0013>.

AlQodsi, Enas Mohammed, Ibrahim Al Shawabkeh, Magdi Shouaib, and Abouelwafa Ibrahim. 'The Legal Framework Governing Personal Data Protection: Challenges and Mechanisms for Enhancing Security in the Digital Age—an Analytical Study'. *Security Journal* 39, no. 1 (June 2026): 37. <https://doi.org/10.1057/s41284-026-00547-y>.

Alresheidat, Dr Mamdouh Mohd Mamdouh, and Mohammad Awad Hammad Zubid. 'Authenticity of Ordinary Bond in Evidence Payment: A Case Study Of Jordan Law'. *Lex Localis - Journal of Local Self-Government* 23, no. S6 (October 2025): 484–895. <https://doi.org/10.52152/rpfm9917>.

Altobaishat, Obieda, Mohamed Abouzid, Deemah Omari, Walid Sange, Ahmad K. Al-Zoubi, Abdallah Bani-Salameh, and Yazan A. Al-Ajlouni. 'Examining the Burden of Mental Disorders in Jordan: An Ecological Study over Three Decades'. *BMC Psychiatry* 25, no. 1 (March 2025): 218. <https://doi.org/10.1186/s12888-025-06658-x>.

Azam, Muhammad, Rawdah Abdul Karim Mohammad Pharaon, Elsoghair Mahdy, Manal Abdellatif Issa Albabili, Burhan Alsyouf, and Bagdat Bagayev. 'AI-Driven Sharia Governance in Islamic Digital Payment Systems: Developing a Contemporary Islamic Law Framework for Ethical and Regulatory Compliance'. *Nusantara: Journal of Law Studies* 5, no. 2 (July 2026): 849–880.
<https://doi.org/10.66325/nusantaralaw.v5i2.339>.

Basha, Mazen Hasan. 'Digitization and the Recovery of Economy: Evidence from Jordan'. In *From Machine Learning to Artificial Intelligence: The Modern*

<https://doi.org/10.66325/nusantaralaw.v5i2.367>

Machine Intelligence Approach for Financial and Economic Inclusion, edited by Abdalmuttaleb M. A. Musleh Al-Sartawi, Manaf Al-Okaily, Anas Ali Al-Qudah, and Fadi Shihadeh, 461–70. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-76011-2_31.

‘Criminal Protection to the Digital Right to Be Forgotten in Jordan’. *International Journal of Electronic Security and Digital Forensics*, n.d. Accessed 10 August 2026. <https://www.inderscienceonline.com/doi/10.1504/IJESDF.2025.145865>.

Dahdal, Andrew Mazen, and Adel Abdel Ghafar. ‘The Digital Silk Road: “Tech-Diplomacy” as a Paradigm for Understanding Technological Adoption and Emerging Digital Regulations in MENA’. *Asian Journal of Law and Society* 12, no. 2 (June 2025): 163–188. <https://doi.org/10.1017/als.2024.30>.

‘Digital Transformation, Social Media Platforms, and the Reshaping of Media Policies in Jordan (2020–2025): A Political-Legal Approach to Governance, Legitimacy, and Digital Security | Request PDF’. *ResearchGate*, ahead of print, 19 May 2026. <https://doi.org/10.57239/prn.26.03410082>.

Gider, Jasmin, Luc Renneboog, and Tal Strauss. ‘The Regulation of Data Privacy and Cybersecurity’. *Annals of Corporate Governance* 10, no. 1 (May 2026): 1–101. <https://doi.org/10.1108/ACG-07-2025-0050>.

H, Tuffaha Al Hussaini Rand Ihab M.’ Digital Governance and Fundamental Rights: A Critical Analysis of Jordan’s Data Protection Law’. *PERSPECTIVES OF LAW AND PUBLIC ADMINISTRATION* 15, no. 1 (2026): 26–49. <https://doi.org/10.62768/PLPA/2026/15/1/02>.

Harding, Isabella Rose M.’ Governance, Transparency, and Financial Regulation in the Global Digital Economy’. *Journal of Nusantara Economy* 4, no. 2 (December 2025): 112–134. <https://doi.org/10.66325/nusantaraeconomy.v4i2.368>.

Jarah, Baker Akram Falah, Abdul Razzak Alshehadeh, Murad Ali Ahmad Al-Zaqeba, Fuad A. Al-Bataineh, and Haneen A. Al-khawaja. ‘Review of the Literature Related to Audit Quality and Integrated Reporting Quality in Jordanian Companies’. *Edelweiss Applied Science and Technology* 8, no. 6

<https://doi.org/10.66325/nusantaralaw.v5i2.367>

(September 2024): 124–133.
<https://doi.org/10.55214/25768484.v8i6.2029>.

'Jordanian Cybercrime Law No. (17) of 2023 between Regulating Social Media Sites and Restricting Freedom of Opinion'. *ResearchGate*, ahead of print, 17 June 2026. <https://doi.org/10.36348/sijlcj.2024.v07i09.002>.

Juwaihan, Ma'en, Hamzeh Abu Issa, and Mohammad Nasr Khater. 'The Crime of Counterfeiting or Imitating a Trademark under Jordanian Trademarks Law'. *The Journal of World Intellectual Property* 28, no. 2 (2025): 589–611. <https://doi.org/10.1111/jwip.12346>.

Khwaileh, Khaled. 'Digital Diplomacy in the Middle East: Jordan's Role in Regional Digital Trade Integration'. SSRN Scholarly Paper No. 5906354. Rochester, NY: Social Science Research Network, 12 December 2025. <https://doi.org/10.2139/ssrn.5906354>.

Okoro, Daniel Chibuike. 'An Evaluation of Cybersecurity Frameworks and Privacy Regulations for Companies in the Digital Age: A Legal Approach'. *Asian Journal of Economics, Business and Accounting* 25, no. 4 (April 2025): 431–440. <https://doi.org/10.9734/ajeaba/2025/v25i41761>.

Rohid, Nibrosu, Rahma Sugihartati, Bagong Suyanto, Oleksandr Gotin, Nabrisi Rohid, and Sukisno. 'Reconstructing the Legal Enforcement Framework for Digital Activism in an Era of Technological Disruption'. *Nusantara: Journal of Law Studies* 5, no. 2 (July 2026): 881–901. <https://doi.org/10.66325/nusantaralaw.v5i2.236>.

Shevchenko, Andrii Volodymyrovych. 'International Trade, Investment Flows, and Economic Integration between Asia-Pacific and Europe'. *Journal of Nusantara Economy* 4, no. 2 (December 2025): 135–159. <https://doi.org/10.66325/nusantaraeconomy.v4i2.383>.

Suheryadi, Bambang, Hariyanto, Bambang Sugeng Ariadi Subagyono, Agus Yudha Hernoko, and Hd Djunaedi. 'Bridging Legal Traditions in Consumer Protection: Criminal Liability in Comparative Jurisprudence and Contemporary Islamic Law'. *MILRev: Metro Islamic Law Review* 5, no. 1 (April 2026): 492–532. <https://doi.org/10.32332/milrev.v5i1.12863>.

Sumartono, Eddy, Rois Harliyanto, Sahat Maruli Tua Situmeang, Darwin Steven Siagian, and Ema Septaria. 'The Legal Implications of Data Privacy Laws, Cybersecurity Regulations, and AI Ethics in a Digital Society'. *The Journal*

<https://doi.org/10.66325/nusantaralaw.v5i2.367>

of Academic Science 1, no. 2 (July 2024): 103–110.
<https://doi.org/10.59613/29qypw51>.

Suwondo, Denny, Arpangi, Umar Ma'ruf, Rakhmat Bowo Suharto, and Mamoon Suliman Alsmadi. 'Consumer Legal Protection Against Standard Clauses in Contemporary Peer-To-Peer Lending: An Islamic Economic Law Perspective'. *MILRev: Metro Islamic Law Review* 5, no. 2 (August 2026): 1296–1329. <https://doi.org/10.32332/milrev.v5i2.12643>.

Thomas, Louise, Iqbal Gondal, Taiwo Oseni, and Selena (Sally) Firmin. 'A Framework for Data Privacy and Security Accountability in Data Breach Communications'. *Computers & Security* 116 (May 2022): 102657. <https://doi.org/10.1016/j.cose.2022.102657>.

Tsimachidis, Konstantinos. 'Self-Regulation in Digital Exercise: Perceived Service Quality and Connectivity as Predictors of Autonomous Motivation'. *International Journal of Physical Education, Sports and Health* 12, no. 6 (2025): 620–626. <https://doi.org/10.22271/kheljournal.2025.v12.i6i.4154>.