

TOWARDS MAQASID SHARIAH-ALIGNED ICT GOVERNANCE: A SYSTEMATIC REVIEW OF DATA SOVEREIGNTY AND DATA SAFETY IN MALAYSIA

¹ Nurafifah Mohd Nor, ^{2,3*} Nur Ilyana Ismarau Tajuddin, ^{1,3} Norita Md Norwawi, ⁴ Nur Aina Abdulah

¹ Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, Malaysia

² Tamhidi Centre, Universiti Sains Islam Malaysia, Nilai, Malaysia

³ AI and Safety for Human Development Research Group, Universiti Sains Islam Malaysia, Nilai, Malaysia

⁴ Faculty of Syariah and Law, Universiti Sains Islam Malaysia, Nilai, Malaysia

*Correspondence:

Nur Ilyana Ismarau Tajuddin, e-mail: nur_ilyana@usim.edu.my

History:

Received : 14.5.2026

Revised : 10.8.2026

Accepted : 17.8.2026

Published: 30.9.2026

Cite as:

Mohd Nor, N., Tajuddin, N. I. I., Md Norwawi, N., & Abdulah, N. A. (2026). Towards Maqasid Shariah-aligned ICT governance: A systematic review of data sovereignty and data safety in Malaysia. *Journal of Fatwa Management and Research*, 31(3), 210–235. <https://doi.org/10.33102/jfatwa.vol.31no3.891>

Funding

No funding was received for this study.

Abstract

Rapid digital transformation has accelerated innovation, economic development, and public service delivery across many countries, including Malaysia. Yet, this shift poses serious threats to data safety and data sovereignty. Following the PRISMA guideline, this study implements a Systematic Literature Review (SLR) to synthesize the evidence on data sovereignty and data safety in Malaysia's ICT governance. Following a standard screening process, 71 relevant studies published between 2021 and 2026 were selected and analyzed to examine their relevance to ethical ICT governance in Malaysia. The selected articles were further categorized based on quality assessment criteria with a goal to deliver a complete summary of the present research landscape. This study examines existing frameworks related to ICT governance, data sovereignty, data safety, and Islamic ethical perspectives, particularly Maqasid Shariah. The findings highlight the need for a unified governance model that synthesizes regulatory governance, technical safeguards, ethical principles, and public trust. This study contributes to the development of a Maqasid Shariah-aligned ICT governance framework for Malaysia's digital transformation agenda.

Keywords: *Maqasid Shariah; ICT governance; Data sovereignty; Data safety; Digital ethics*



© The Author(s). This article is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0). Reuse and adaptation are permitted, provided appropriate credit is given to the author(s) and source, a licence link is provided, and any changes made are indicated.

INTRODUCTION

The unprecedented growth of cloud computing, large-scale datasets, and artificial intelligence (AI) has optimized public service delivery but introduced critical challenges in data sovereignty and data safety (Hummel et al., 2021; Williamson, 2022). While data sovereignty ensures data remains subject to domestic laws (Hippelainen et al., 2017), data safety involves protecting information from cyber threats and misuse through a combination of technological, legal, and governance safeguards. As data becomes a strategic national asset, reliance on foreign digital infrastructure has intensified concerns over jurisdictional control (Jansen et al., 2023).

In Malaysia, initiatives like MyDIGITAL and RMKe-12 drive digital adoption but increase cybersecurity exposure (Huawei Technologies Malaysia & MDEC, 2022). A significant regulatory gap persists as the Personal Data Protection Act 2010 excludes government-held data, leaving public sector records vulnerable to breaches and foreign jurisdiction (Alibeigi et al., 2020; Harun, 2025). This vulnerability is reflected in an average of 15 data breaches per week in 2023 (CyberSecurity Malaysia, 2023), with AI further complicating accountability and privacy through opaque algorithms (Bernama, 2025).

Acknowledging these vulnerabilities, the Malaysian authorities introduced the AIGE (National Guidelines on Artificial Intelligence Governance and Ethics (MOSTI, 2024). However, integrating these into a framework that includes religious-ethical considerations remains a challenge. Maqasid Shariah, representing the fundamental tenets of the Islamic legal tradition, provides a crucial analytical framework for mitigating risks (Al-Shatibi, 1996; Sawari et al., 2025). This study assesses three pivotal domains: *Hifz al-Mal*, *Hifz al-Aql*, and *Hifz al-Nafs*, with further details provided in Table 1.

Table 1: Selected Maqasid Shariah Principles in Digital Governance

Maqasid Shariah Principles	Findings
<i>Securing Wealth and Assets (Hifz al-Mal)</i>	Protecting data as a strategic asset against financial harm from fraud, ransomware, and data breaches.
<i>Upholding Intellectual Integrity (Hifz al-‘Aql)</i>	Preserving rational thinking and knowledge integrity against algorithmic bias, misinformation, and disinformation.
<i>Safeguarding Life (Hifz al-Nafs)</i>	Safeguarding individuals from physical or dignity-based harm, such as cyberattacks on healthcare or digital harassment.

Current governance practices invoking Maqasid Shariah are fragmented and inconsistently applied across sectors (Bashori et al., 2024), despite evidence that cyber threats directly compromise the realization of Maqasid Shariah objectives (Mohadi et al., 2023). These gaps hinder Malaysia’s RMKe-12 goals. Therefore, a holistic, Shariah-aligned ICT framework is essential to ensure a secure and ethically sustainable digital transformation. An SLR-based synthesis of data sovereignty, safety, and Maqasid Shariah is conducted in this study to inform a tailored governance framework. This study addresses the following core inquiries:

RQ1: What are the existing frameworks and practices related to data sovereignty and data safety in ICT governance?

RQ2: How have Maqasid Shariah principles been operationalized in ICT ethics, cybersecurity, or digital governance?

RQ3: What theoretical or practical gaps exist in integrating Maqasid Shariah with data sovereignty and data safety frameworks?

RQ4: How can insights from the literature inform the design of an ethical ICT governance model suitable for Malaysia?

LITERATURE REVIEW

Data Sovereignty

Data sovereignty dictates that data is regulated by its physical or jurisdictional location (Hippelainen et al., 2017). As a strategic asset, controlling data flows is essential for national digital authority (Pierucci, 2025), yet cross-border cloud computing creates conflicting international laws and privacy risks (Micheal, 2024). To mitigate foreign dependence and safeguard security, nations adopt diverse frameworks: privacy-centric models emphasizing adequacy and safeguards (EU, Australia); strict localization prioritizing state control and national security (China, Saudi Arabia); and flexible sectoral approaches favoring innovation and digital growth (USA, Singapore).

Data Sovereignty in Malaysia

Malaysia's sovereignty framework is anchored by the Personal Data Protection Act (PDPA), which regulate commercial data processing. However, a "regulatory blind spot" persists as the Act excludes government-held data (Alibeigi et al., 2020). This lack of public-sector oversight for sensitive biometric hinders Malaysia's pursuit of international "adequacy status" (Daud, 2024; Pool et al., 2024).

Malaysia has strengthened its digital ecosystem by implementing the PDPA 2024 Amendments which focus on biometric data and protocols for security incidents. Furthermore, the passing of the 2024 Cyber Security Act serves to protect National Critical Information Infrastructure (NCII), while the commencement of the 2025 Data Sharing Act facilitates more efficient data transfers between government bodies. To address external legal threats, such as the US CLOUD Act, the Sovereign Cloud Policy was developed to minimize risks from foreign jurisdictions. However, Malaysian tort law remains untested against AI-driven negligence in healthcare and finance, highlighting a need for global best practices in liability frameworks (Bernama, 2025).

Data Safety in Malaysia

Malaysia manages cybersecurity by combining the strategic oversight of NACSA (National Cyber Security Agency) with the technical expertise of CyberSecurity Malaysia. Despite the Cyber Security Act 2024, the nation's threat landscape remains volatile. In 2023, Malaysia ranked among the top ten most affected countries for leaked accounts, with fraud (71%) and data breaches (10%) dominating the reported incidents (MyCERT, 2025; Yeoh, 2023). Three high-profile incidents highlight the policy-practice gap:

- PADU (2024): A federal-state conflict where Sarawak halted participation over data control and sovereignty concerns (New Straits Times, 2024).

- SOCSO (2023): A deep intrusion leaking internal data, exposing vulnerabilities in social welfare systems. (Malay Mail, 2023).
- NRD/MyIdentity (2021-2022): The alleged leak of 22.5 million records via APIs, proving state susceptibility to attack (The Straits Times, 2022).

These breaches fuel debate over Section 3(1) of the PDPA 2010, which exempts government agencies from penalties and mandatory notifications (Malaysian Bar, 2025). This exemption creates a "trust deficit," as the state bypasses the security standards required of the private sector.

Cybersecurity is now widely recognized as a societal and moral issue, moving beyond a strictly technological focus (Hoong, 2024). By integrating Maqasid Shariah tenets, specifically the preservation of wealth (*Hifz al-Mal*), intellect (*Hifz al-Aql*) and human life (*Hifz al-Nafs*), governance can prioritize human wellbeing within the digital ecosystem (Darus et al., 2024). This holistic approach is vital for a secure, inclusive, and ethically sustainable digital transformation (Bernama, 2025).

Artificial Intelligence and Data Governance

The Artificial Intelligence (AI) integration exacerbates Malaysia's sovereignty and safety challenges, as reliance on foreign cloud services and opaque algorithms risks compromising national jurisdiction and public trust (Othman, 2025). Malaysia's AI evolution has progressed through three phases:

1. Strategic Foundation (2021–2022): National 4IR Policy and AI Roadmap established development frameworks.
2. Ecosystem Activation (2024): Digital literacy initiatives (AI untuk Rakyat) and significant investments from Microsoft and Google.
3. Governance & Sovereignty (2025–2026): Enforcement via the National AI Office (NAIO) and AIGE (MOSTI, 2024).

With the objective of securing digital sovereignty, the government allocated RM 2 billion in the 2026 Budget for a Sovereign AI Cloud. Managed by the NAIO, this infrastructure keeps sensitive data within domestic jurisdiction while enabling ethical modelling (Ministry of Digital Malaysia, 2025).

However, an "innovation-security paradox" has emerged: while fostering growth, the same foreign-owned infrastructures are exploited for AI-powered scams. In early 2025, Malaysians lost RM 2.11 billion to deepfakes and voice cloning, highlighting the urgent need for enforceable regulatory frameworks (New Straits Times, 2025; Sharif et al., 2025).

Maqasid Shariah in Technology Governance

Beyond technical metrics, Malaysia's socio-religious landscape positions Maqasid Shariah, the core principles of Islamic law, as an analytical framework to guide ICT governance. Al-Ghazali and Al-Shatibi, characterized the essence of Islamic jurisprudence as the preservation of five fundamental pillars: progeny (*hifz al-nasl*), life (*hifz al-nafs*), religion (*hifz al-din*), material assets (*hifz al-mal*), and intellect (*hifz al-'aql*) (Al-Shatibi, 1996; Dusuki & Bouheraoua, 2021). While traditionally applied to finance and classical governance, this framework is now essential for evaluating digital domains where cyber threats directly

compromise these core values (Ali, 2025; Sawari et al., 2025). Integrating Maqasid Shariah ensures that technological innovation remains anchored in ethical responsibility. Three dimensions are pivotal for this study:

Safeguarding Assets (Hifz al-Mal)

Within the realm of the digital economy, data is a strategic economic asset. Cyber fraud, ransomware, and identity theft constitute modern "unjust consumption" of property. This preservation is rooted in the Quranic command:

“Do not consume one another’s wealth unjustly, nor deliberately bribe authorities in order to devour a portion of others’ property, knowing that it is a sin” (Surah Al-Baqarah, 2:188).

Strengthening data sovereignty and safety measures contributes directly to *Hifz al-Mal* by safeguarding financial systems and maintaining public trust in digital transactions.

Safeguarding the Intellect (Hifz al-’Aql)

The core of this principle lies in maintaining the soundness and reliability of information. AI systems, through algorithmic bias and opaque decision-making, can distort knowledge and undermine rational thought. This digital danger is addressed by the Prophetic caution regarding uncritical dissemination:

The Prophet (peace be upon him) stated, “It is enough for a man to prove himself a liar when he goes on narrating whatever he hears” (Sahih Muslim).

Ethical AI frameworks emphasizing transparency and accountability are therefore essential to protecting the intellect by ensuring technologies support informed, responsible decision-making.

Safeguarding Life (Hifz al-Nafs)

Digital safety has become an essential prerequisite for physical safety. Cyberattacks on healthcare, transportation, or critical infrastructure endanger public life (*nafs*). Furthermore, the objective extends to protecting individual dignity against unauthorized surveillance, as warned in the Quranic verse:

“O believers! Avoid many suspicions, for indeed, some suspicions are sinful. And do not spy, nor backbite one another. Would any of you like to eat the flesh of their dead brother? You would despise that! And fear Allah. Surely Allah is the Acceptor of Repentance, Most Merciful” (Surah Al-Hujurat, 49:12).

By aligning cybersecurity with *Hifz al-Nafs*, governance models prioritize the protection of individuals and societal stability over mere technical efficiency.

Recent scholars like as Zafar and Ali (2025) proposed the development of a Shariah governance standard for generative AI, focusing on accountability, fairness, and compliance with Islamic ethical norms. Such proposals signal that Maqasid principles can be systematically translated into digital policies rather than treated as abstract ideals.

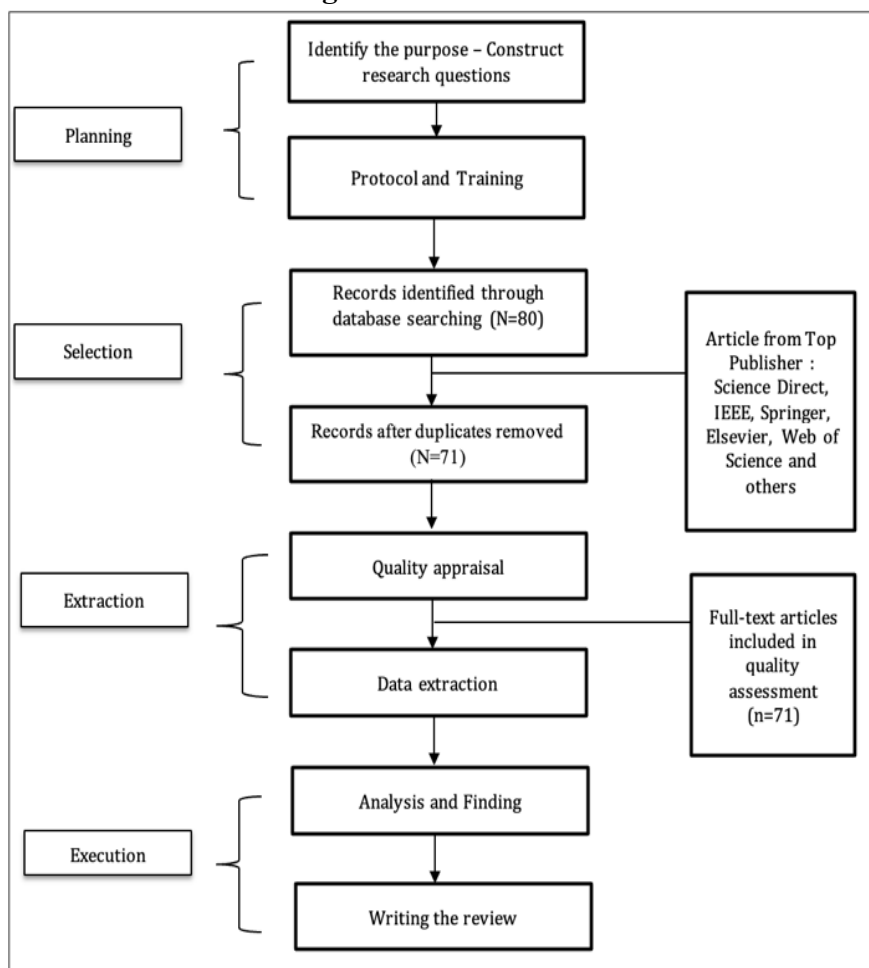
However, current research remains fragmented: legal experts focus on PDPA compliance, technical experts on security tools, and Islamic scholars on abstract theory. There is a pressing need for an ICT governance model that integrates legal compliance, technical safeguards, and Shariah-aligned ethics. This study addresses this by positioning Maqasid Shariah as the ethical foundation for Malaysia's digital sovereignty and safety.

METHODOLOGY

Research Design

An SLR was executed in compliance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) standards, ensuring that the reporting of results remains consistent and thorough. The complete methodological workflow for the SLR is visualized in Figure 1:

Figure 1: SLR Process



Planning

The research prioritizes delineating the research context, establishing formal review protocols, and constructing the core research questions.

Selection

Using Boolean searches across five databases (Scopus, IEEE Xplore, Web of Science, Elsevier and Google Scholar, last searched on 6 May 2026, this review identified English-language studies (2021–2026) addressing data sovereignty, cybersecurity, AI governance, and Maqasid Shariah. The search string combined three concept blocks: (“data sovereignty” OR “data localisation” OR “data residency”) AND (“data safety” OR “data security” OR cybersecurity OR “AI governance”) AND (“Maqasid Shariah” OR “Islamic ethics” OR “digital ethics”), applied to title, abstract, and keyword fields.

Studies were eligible if they (i) were published between 2021 and 2026, (ii) were written in English, (iii) appeared as peer-reviewed journal articles or conference papers, and (iv) substantively addressed at least one of data sovereignty, data safety, ICT or AI governance, or Maqasid Shariah in a digital context. Book chapters, dissertations, editorials, non-peer-reviewed reports, and non-English texts were excluded.

A set of criteria for literature filtration was devised. This study utilised literature exclusively from high-quality sources, as indicated in Table 2, based on established criteria. Screening followed the PRISMA flow shown in Figure 1. Of the 80 records identified, 9 were excluded during screening (e.g., duplicates, no substantive treatment of the review concepts, inaccessible full text), yielding 71 studies for final analysis.

Table 2: Criteria of article

No	Criteria	Inclusion	Exclusion
1	Focus on the article	Article that focus on: — ICT — Data Safety, Data security, Data sovereignty — Maqasid Shariah — Islamic and Digital Ethic	Articles that did not focus on: — ICT — Data Safety, Data security, Data sovereignty — Maqasid Shariah — Islamic and Digital Ethic
2	Journal published	Top publisher/source: Scopus, IEEE, Elsevier, WoS, Google Scholar	Journal and conference paper outside of the top publisher/source
3	Publication date	2021 onwards	Before 2021
4	Publication type	Journal, conference paper, technical report	Book chapters, dissertations
5	Language	Journal article, conference paper was written in English	Other languages were not included

Extraction and Execution

Data were extracted from each included study using a standardized form capturing: citation details (author, year, publisher); study type (conceptual, review, or empirical, coded C, R, and E respectively in Table 4); publication type (journal article or conference paper, coded J and P); geographic or jurisdictional focus; the governance domain addressed; and whether and how Maqasid Shariah was invoked.

A quality assessment of the shortlisted articles was then performed against the four criteria (Q1–Q4) listed in Table 3. Each question targets a distinct dimension of study quality.

- Q1 Conceptual Clarity and Relevance: Does the study clearly define and discuss concepts related to data sovereignty, data safety, ICT governance, or Maqasid Shariah principles?
- Q2 Methodological Rigor: Is the research methodology (e.g., empirical, conceptual, framework-based) clearly described and appropriate for addressing issues of data governance or ethical principles?
- Q3 Evidence Strength and Practical Insight: Does the study provide explicit evidence, frameworks, or empirical findings related to data sovereignty/safety or ethical ICT governance?
- Q4 Integration with Ethical or Theoretical Principles: Does the study incorporate, discuss, or align with ethical principles, Islamic digital ethics, or Maqasid Shariah in ICT governance?

Each question presents three response options:

- 0 = Not addressed, or unrelated to the review scope (No)
- 0.5 = Mentioned but not clearly defined (Partially)
- 1 = Clearly addressed and directly relevant to the review scope (Yes)

Scores were summed across the four criteria to give a total of 0 to 4 per study. Studies scoring below [THRESHOLD - Poor (1 - < 2)] were excluded from synthesis; the 71 studies meeting the threshold were retained, and each study's score is reported in Table 5. The reporting phase follows this evaluation, detailing the literature characteristics and synthesis outcomes in the subsequent sections.

Table 3: Quality Assessment Criteria

No.	Item	Answer
Q1	Does the study clearly define and discuss concepts related to data sovereignty, data safety, ICT governance, or Maqasid Shariah principles?	Yes/No/ Partially
Q2	Is the research methodology (e.g., empirical, conceptual, framework-based) clearly described and appropriate for addressing issues of data governance or ethical principles?	Yes/No/ Partially
Q3	Does the study provide explicit evidence, frameworks, or empirical findings related to data sovereignty/safety or ethical ICT governance?	Yes/No/ Partially
Q4	Does the study incorporate, discuss, or align with ethical principles, Islamic digital ethics, or Maqasid Shariah in ICT governance?	Yes/No/ Partially

Findings

The selected 71 articles were analyzed to establish their relevance to ethical ICT governance in Malaysia. With the quality assessment complete, the final set of selected articles was categorized to provide an in-depth view of the current research landscape. Table 4 provides a comprehensive overview of the 71 selected article.

Table 4: Final Selection of Articles

ID	Author(s)	Title	Study Type	Paper Type	Publisher
MS-01	Osman et al. (2021)	Cyber Security and Maqasid Al-Shariah: A Case of Facebook Application	C	J	GAE
MS-02	Uddoh et al. (2021)	Cross-Border Data Compliance and Sovereignty: A Review of Policy and Technical Frameworks	R	J	APH
MS-03	Yusif et al. (2021)	A Conceptual Model for Cybersecurity Governance	C	J	T&F
MS-04	Formosa et al. (2021)	A principlist framework for cybersecurity ethics	C	J	Elsevier
MS-05	Verstraete et al. (2021)	Optimizing Breach Notification	C	J	UOI
MS-06	Gonzalez et al. (2021)	Automated Cyber and Privacy Risk Management Toolkit	C	J	MDPI
MS-07	Raquist et al. (2022)	Islamic virtue-based ethics for artificial intelligence	C	J	Springer
MS-08	Nugraha et al. (2022)	Cybersecurity service level agreements: understanding government data confidentiality requirements	E	J	OUP
MS-09	Wexler (2022)	Life, Liberty, and Data Privacy: The Global CLOUD, the Criminally Accused, and Executive Versus Judicial Compulsory Process Powers	E	J	-
MS-10	Thomas et al. (2022)	A framework for data privacy and security accountability in data breach communications	E	J	Elsevier
MS-11	Skopik et al. (2022)	From scattered data to actionable knowledge: flexible cyber security reporting in the military domain	E	J	Springer
MS-12	Dash et al. (2022)	Threats And Opportunities with Ai-Based Cyber Security Intrusion Detection: A Review	E	J	Elsevier
MS-13	Mohiqi (2023)	Data's Nature and Its Prevailing Right under Islamic Law	C	J	IJMMU
MS-14	Mohadi et al. (2023)	Maqasid Al-Shari'ah and the Ethics of Artificial Intelligence: Contemporary Challenges	C	J	Maqasid Institute
MS-15	Lam et al. (2023)	Regulating Data Privacy and Cybersecurity	E	J	Elsevier
MS-16	Porcedda (2023)	Cybersecurity, Privacy and Data Protection in EU Law	E	B	BP
MS-17	Krotov et al. (2023)	Big web data: Challenges related to data, technology, legality, and ethics	C	J	Elsevier
MS-18	Molitor et al. (2023)	Exploring Key Issues in Cybersecurity Data Breaches: Analyzing Data Breach Litigation with ML-Based Text Analytics	E	J	MDPI
MS-19	Vostoupal et al. (2023)	The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond	C	J	Elsevier
MS-20	Asgarinia et al. (2023)	"Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies	C	J	MDPI
MS-21	Solaiman et al. (2024)	Regulating AI in Health in the Middle East: Case Studies from Qatar, Saudi Arabia and the United Arab Emirates	C	B	Frontiers Media SA

MS-22	Gorian et al. (2024)	Digital Ethics of Artificial Intelligence (AI) in Saudi Arabia and United Arab Emirates	C	J	USIM
MS-23	De Colle (2024)	Towards an ontology of data sovereignty and ownership in cyberspace	C	P	Springer
MS-24	Abbas et al. (2024)	Beyond control over data: Conceptualizing data sovereignty	C	J	Springer
MS-25	Del Re (2024)	Technologies of Data Protection and Institutional Decisions for Data Sovereignty	E	J	MDPI
MS-26	Zhou et al. (2024)	Cybersecurity data breaches and internal control	E	J	Elsevier
MS-27	Pestana et al. (2024)	Data Governance to Counter Hybrid Threats against Critical Infrastructures	C	J	MDPI
MS-28	Bobbert et al. (2024)	Overcoming the Fear of Missing Out on Data	E	P	Springer
MS-29	Agarwal et al. (2024)	Addressing AI Risks in Critical Infrastructure: Formalising the AI Incident Reporting Process	C	P	IEEE
MS-30	Ababneh et al. (2024)	Role of Artificial Intelligence in Data Protection for Digital Asset Systems: A Review of Recent Development	E	J	UIKTEN
MS-31	Samonte et al. (2024)	Building a Privacy-Centric Systems Integration and Architecture	C	P	ACM
MS-32	Bandaru et al. (2024)	Enhancing Privacy Measures in Healthcare within Cyber-Physical Systems through Cryptographic Solutions	C	J	EAI
MS-33	Leicht et al. (2024)	Creating Privacy Policies from Data-FlowDiagrams	C	P	Springer
MS-34	Durango et al. (2024)	Human Data Interaction Framework: A Comprehensive Model for a Future Driven by Data and Humans	C	J	Cornell University
MS-35	Schubert et al. (2024)	Data Governance, Privacy, and Ethics	C	J	Springer
MS-36	Waseem et al. (2025)	Islamic Ethical Perspectives on AI and Digital Transformation in the 21st Century	C	J	Wah Academia
MS-37	Azizli et al. (2025)	Artificial Intelligence and Islamic Jurisprudence: A Critical Analysis of Legal and Ethical Challenges in Automated Decision-Making	C	J	AHS-EDU
MS-38	Hamza (2025)	An AI-Driven Blockchain Framework for Intelligent Halal Data Governance and Digital Evidence Integrity Across the Halal Supply Chain	C	J	Indus University
MS-39	Zafar et al. (2025)	Shariah Governance Standard on Generative AI for Islamic Financial Institutions	C	J	-
MS-40	Elgujja et al. (2025)	Ethical and Legal Implications of Artificial Intelligence in Infection Prevention and Control: A Saudi Arabian Perspective	C	J	JMIR Publishing
MS-41	Elgujja et al. (2025)	Privacy-by-Design, Digital Dignity, and Algorithmic Justice in Healthcare AI: A Comparative Legal, Ethical, and Technical Analysis of Saudi Arabia and Nigeria	C	J	-
MS-42	Aloufi et al. (2025)	Legal Gaps, Islamic Ethics, and Digital Trust: Building a Regulatory Framework for Saudi E-Commerce Under Vision 2030	C	J	Lectito Publishing
MS-43	Aljawi et al. (2025)	Harmonization of National and International Law in the Utilization of AI for the Organization of Hajj: A Collaborative Study Between Indonesia and Saudi Arabia	E	J	Greenation Publisher
MS-44	Fatarib et al. (2025)	Qiyas as a Method of Digital Ijtihad for Social Sustainability in ASEAN in the Era of Technological Disruption	C	P	UINSK

MS-45	Mujahid et al. (2025)	Islamic Ethical Values as The Foundation for The Use of Artificial Intelligence in Islamic Boarding School Education	C	P	UMS
MS-46	Maman et al. (2025)	Artificial Intelligence and Machine Learning in Financial Industry Transformation: A Comparative Analysis of Conventional and Sharia Fintech in Indonesia	E	J	UINRMSS
MS-47	Albous et al. (2025)	AI Governance in the GCC States: A Comparative Analysis of National AI Strategies	E	J	-
MS-48	Hadi et al. (2025)	Artificial Intelligence and Dispute Resolution in Brunei: Assessing Readiness, Legal Reform, and the Way Forward	E	J	UMM
MS-49	Albaroudi et al. (2025)	Empowering Data Sovereignty through Artificial Intelligence: A Framework for Sustainable Smart Energy Systems in Saudi	E	J	SI
MS-50	Mustapha et al. (2025)	Islamic Perspectives on AI And Cybersecurity: Developing Ethical Frameworks for Autonomous Security Systems	E	J	GAE
MS-51	Ali et al. (2025)	Islamic Ethics and AI: An Evaluation of Existing Approaches to AI using Trusteeship Ethics	C	J	Springer
MS-52	Kannike et al.	Exploring The Ethical Governance of Artificial Intelligence from An Islamic Ethical Perspective	C	J	Universiti Malaya
MS-53	Farid et al. (2025)	Maqasid Sharia Analysis on Personal Data Protection from the Dangers of Artificial Intelligence Misuse	E	J	UMS
MS-54	Dahlan et al. (2025)	Modeling AI-Generated Misinformation: Shariah, Ethical and Forensic Perspectives from Malaysia	E	J	USIM
MS-55	Wahab et al. (2025)	Digital Shariah Governance and the Future of Islamic Finance: A Framework for AI-Driven Shariah Compliance in a Global Regulatory Environment	C	J	UINSK
MS-56	Pierucci (2025)	Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace	C	J	Springer
MS-57	Sorrentino et al. (2025)	Towards Semantic Coherence: Understanding Cybersecurity and Digital Sovereignty in the Automotive Landscape	C	P	IEEE
MS-58	Figuerola et al. (2025)	Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals	E	J	Springer
MS-59	Pahune et al. (2025)	The Importance of AI Data Governance in Large Language Models	E	J	MDPI
MS-60	Fouad et al. (2025)	Failing better in the infosphere: ontological uncertainties and the essence of security in cyberspace	C	J	RJ
MS-61	Wang et al. (2025)	Privacy-enhanced deep learning inference acceleration towards third-party cloud based on trusted execution environment	E	J	Springer
MS-62	Awais et al. (2025)	Managing Cyber Security Risks in Islamic Fintech: A Shariah Perspective	C	J	PARE
MS-63	Misra et al. (2025)	Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges	E	J	Springer
MS-64	Qiu et al. (2025)	Progress and recommendations in data ethics governance: a transnational analysis based on data ethics frameworks	E	J	Springer
MS-65	Batool et al. (2025)	AI governance: a systematic literature review	E	J	Springer
MS-66	Rofiq et al. (2025)	Online Data Privacy Ethical Guidelines based on Islamic Perspectives	C	J	DSR

MS-67	Mia et al. (2026)	Designing Ethical AI-Integrated Cybersecurity Education: A Qur'anic Values Informed Framework for Responsible Digital Learning	E	J	-
MS-68	Nugroho et al. (2026)	Institutionalizing Artificial Intelligence within Indonesia's Zakat Architecture: Navigating Regulatory Challenges and Sharia Compliant Implementation	E	J	UMS
MS-69	Smolo (2026)	Islamic Finance in the Digital Age: Fintech as a Civilizational Tool	C	J	MDPI
MS-70	Saqib et al. (2026)	Comparative Analysis of AI Regulation for Fintech Cybersecurity and Privacy in the European Union and Qatar	E	J	Springer
MS-71	Rizk (2026)	Integrating Artificial Intelligence into Credit Risk Assessment (A Comparative Study of Islamic and Conventional Banks)	C	J	AJRSP

Note: C = Conceptual; E = Empirical; R = Review; B = Book; J = Journal; P = Proceeding; AJRSP = Academic Journal of Research and Scientific Publishing; APH = Anfo Publication House; BP = Bloomsbury Publishing Plc; DSR = Design for Scientific Renaissance; EAI = European Alliance for Innovation; GAE = Global Academic Excellence; IJJMU = IJMMU Foundation; T&F = Taylor & Francis; SI = SCIENCEDOMAIN International; UINSK = UIN Sunan Kudus; UINRMSS = UIN Raden Mas Said Surakarta; UMM = Universitas Muhammadiyah Malang; UMS = Universitas Muhammadiyah Surakarta; UOI = University of Illinois; USIM = Universiti Sains Islam Malaysia; OUP = Oxford University Pres; ICS = Inst Computer Sciences; RJ = Routledge Journals; PARE = Pinnacle Academia Research & Education;

The bibliometric analysis reveals a dominance of journal articles (86%) over proceedings (11%) and book (3%), reflecting a strong reliance on mature, peer-reviewed sources within AI governance and Islamic ethics. Publication trends show a sharp increase from the foundational phase (2021–2022) to a peak in 2025 (31 papers), underscoring the rising global urgency of data sovereignty.

However, the landscape remains primarily theory-driven: conceptual studies (58%) and reviews (21%) far outweigh empirical investigations (21%), highlighting a critical need for data-driven validation. The field is anchored by Springer (11 papers) and Elsevier (7 papers), ensuring high academic rigor, while increasingly diversifying through regional institutional publishers and specialized Islamic academic venues. This shift, particularly visible from 2024 to 2026, highlights a transition from global theoretical frameworks to localized, context-specific research led by institutions like USIM, UINSK, and UMS.

The distribution of quality scores across sources and questions is displayed in Table 5. Every selected study clearly defined its research aims and objectives. Specifically, all 71 papers demonstrated clear research objectives and provided pertinent, adequate explanations of their analytical methods.

Table 5: Quality assessment result

Article Ref.	Q1	Q2	Q3	Q4	Cumulative Score
MS-01	1	0.5	0.5	1	3
MS-02	1	1	1	0.5	3.5
MS-03	1	0.5	0.5	0	2
MS-04	1	0.5	1	0.5	3
MS-05	1	0.5	1	0.5	3
MS-06	1	1	1	0.5	3.5
MS-07	1	0.5	0.5	1	3
MS-08	1	1	1	0.5	3.5

MS-09	1	0.5	1	1	3.5
MS-10	1	1	1	0.5	3.5
MS-11	1	1	1	0	3
MS-12	0.5	0	0.5	0	1
MS-13	1	0.5	0.5	1	3
MS-14	1	0.5	0.5	1	3
MS-15	1	1	1	0.5	3.5
MS-16	1	1	0.5	0.5	3
MS-17	1	0.5	1	0.5	3
MS-18	1	1	1	0	3
MS-19	1	0.5	1	0	2.5
MS-20	1	0.5	1	0.5	3
MS-21	1	0.5	1	0.5	3
MS-22	1	0.5	1	1	3.5
MS-23	1	1	0.5	0	2.5
MS-24	1	1	1	0.5	3.5
MS-25	1	0.5	0.5	0.5	2.5
MS-26	1	1	1	0.5	3.5
MS-27	1	0.5	1	0.5	3
MS-28	1	0.5	1	0.5	3
MS-29	1	0.5	1	0.5	3
MS-30	1	1	0.5	0.5	3
MS-31	1	0.5	1	0.5	3
MS-32	1	0.5	1	0.5	3
MS-33	1	1	1	0.5	3.5
MS-34	1	1	1	0.5	3.5
MS-35	1	0.5	1	0.5	3
MS-36	1	1	1	1	4
MS-37	1	1	0.5	1	3.5
MS-38	1	1	1	0.5	3.5
MS-39	1	1	1	1	4
MS-40	1	0.5	1	1	3.5
MS-41	1	0.5	1	0.5	3
MS-42	1	1	1	1	4
MS-43	1	0.5	1	0.5	3
MS-44	1	0.5	0.5	1	3
MS-45	1	0.5	0.5	1	3
MS-46	1	1	1	1	4
MS-47	1	1	1	0.5	3.5
MS-48	1	1	1	0.5	3.5
MS-49	1	0.5	1	1	3.5
MS-50	1	1	0.5	1	3.5
MS-51	1	1	0.5	1	3.5
MS-52	1	0.5	1	1	3.5
MS-53	1	1	1	1	4
MS-54	1	1	1	1	4
MS-55	1	0.5	0.5	1	3
MS-56	1	0.5	0.5	0	2
MS-57	1	0.5	0.5	0	2
MS-58	1	1	1	0	3

MS-59	1	0.5	1	0.5	3
MS-60	1	0	0.5	0.5	2
MS-61	1	1	1	0.5	3.5
MS-62	1	1	1	1	4
MS-63	1	1	1	0.5	3.5
MS-64	1	0.5	0.5	0.5	2.5
MS-65	1	1	1	0.5	3.5
MS-66	1	0.5	0.5	0.5	2.5
MS-67	1	1	1	1	4
MS-68	1	0.5	1	1	3.5
MS-69	1	0.5	1	1	3.5
MS-70	1	1	1	0.5	3.5
MS-71	1	1	0.5	1	3.5

As summarized in Table 6, the quality assessment confirms a robust evidence base, with 86% of the studies rated as "Very Good" (3–4). These papers demonstrated high conceptual clarity, well-structured frameworks, and strong alignment with contemporary AI and cybersecurity discourse. Approximately 13% were categorized as "Good" (2–<3), offering valuable interdisciplinary insights despite minor methodological or empirical limitations. Only 1% were rated as "Poor". Crucially, no studies were rated "Very Poor" (<1), ensuring all selected literature meets the minimum academic threshold.

While conceptually strong, the evidence base reveals a critical need for improved methodological rigor and consistent integration of ethical frameworks, specifically Maqasid Shariah, within AI governance and data sovereignty. Future research should prioritize empirical approaches and interdisciplinary methodologies to enhance the practical applicability of Shariah-aligned digital governance.

Table 6: Quality assessment result summary

Quality Grading Range	Very poor (<1)	Poor (1 - <2)	Good (2 – <3)	Very good (3 – 4)	Aggregate
No. of papers	0	1	9	61	71
Percentages (%)	0	1	13	86	100

FINDINGS AND DISCUSSION

Existing Frameworks and Practices in Data Sovereignty and Data Safety (RQ1)

Existing governance frameworks address data sovereignty and safety through three primary pillars: legal regulation, technological safeguards, and institutional mechanisms.

- **Legal:** Regulations like the GDPR and various national data protection laws enhance transparency and accountability for data processors (Verstraete et al., 2021). In Malaysia the legal pillar is layered rather than unified, comprising the Personal Data Protection Act 2010 (Act 709), the Communications and Multimedia Act 1998, the Computer Crimes Act 1997 and, most recently, the Cyber Security Act 2024 (Act 854), each administered by a different authority.

- Technical: Encryption, secure cloud infrastructure, and cybersecurity monitoring mechanisms are vital for maintaining data confidentiality, integrity, and availability (Micheal, 2024).
- Institutional: National agencies, such as CyberSecurity Malaysia and NACSA coordinate threat responses and manage critical infrastructure. NACSA's mandate was placed on a statutory footing by the Cyber Security Act 2024 (Act 854), which came into operation on 26 August 2024 and designates eleven National Critical Information Infrastructure (NCII) sectors. Among them are government, banking and finance, healthcare, energy, water and defence, whose sector leads may issue binding codes of practice.

Despite these efforts, current frameworks often prioritize commercial transactions, leaving government data and cross-border flows insufficiently protected (Harun et al., 2025). This regulatory gap necessitates more comprehensive models that secure jurisdictional control over national data assets.

Most of the reviewed studies focus on the legal pillar. Laws such as the GDPR and the PDPA 2010 dominate this literature, largely because statutory text is the easiest object of study to locate and analyse. Technical and institutional measures, by contrast, are usually asserted rather than tested. Studies mention encryption, secure cloud infrastructure, and national coordinating agencies, but few show that these controls actually reduce breaches or shorten response times. The three-pillar model therefore looks more complete on paper than it is in practice.

Existing frameworks lean towards commercial concerns because of how they were created, not because of an oversight. Most data protection laws were written to support trade and build consumer confidence in e-commerce. They therefore place duties on commercial data processors and give remedies to individuals. Government data, national registries, and cross-border processing by foreign cloud providers fall outside this design. The exclusion is explicit rather than inferred: section 3(1) of the PDPA 2010 provides that the Act "shall not apply to the Federal Government and State Governments", and section 3(2) removes personal data processed outside Malaysia unless it is intended for further processing in the country. These are drafting choices about scope, not judgements about risk; government-held data was never the intended object of the statute. The gap identified by Harun et al. (2025) is therefore structural, not accidental. This matters for reform: simply extending consent-based commercial rules to state data is unlikely to close it.

Malaysian practice appears to bear this out. Rather than widening the PDPA, the legislature enacted a separate public-sector regime, the Data Sharing Act 2025 (Act 864), in force on 28 April 2025, which establishes the National Data Sharing Committee, obliges public agencies to maintain security safeguards and report unauthorised disclosures, and carries penalties of up to RM1 million or five years' imprisonment. The structural reading advanced here therefore has legislative support, although the Act is too recent for the reviewed studies to have assessed its effectiveness.

One further tension runs through the literature, and few studies acknowledge it. Data sovereignty, understood as keeping data within national borders, can work against data safety. Keeping national data inside domestic infrastructure reduces exposure to foreign jurisdictions, but it also creates a single point of failure and gives up the stronger security capabilities of

global providers. The literature tends to assume that sovereignty and safety reinforce each other. The evidence reviewed here suggests otherwise: they are competing objectives that must be traded off deliberately. That trade-off is precisely where an ethical framework becomes necessary rather than decorative.

Operationalization of Maqasid Shariah in Digital Governance (RQ2)

Maqasid Shariah provides a substantive ethical framework for ICT governance, transposing classical protections into the digital age through three primary objectives:

- *Hifz al-Mal* (Protection of Wealth): Beyond personal asset safety, this principle addresses systemic digital vulnerabilities. In Malaysia, where online scam losses reached RM2.97 billion in 2025, up from RM1.57 billion in 2024 (Bernama, 2026), *Hifz al-Mal* necessitates robust data sovereignty and anti-fraud mechanisms to prevent "unjust appropriation" (*akl al-mal bi al-batil*) and preserve the integrity of the national financial ecosystem.
- *Hifz al-Aql* (Protection of Intellect): This objective shifts from classical reasoning to contemporary "epistemic integrity." It counters harms from algorithmic bias and disinformation that distort public cognition. Operationalizing *Hifz al-Aql* requires algorithmic transparency and ethical AI oversight to safeguard intellectual autonomy and informed judgment.
- *Hifz al-Nafs* (Protection of Life): This links cybersecurity directly to human safety. Cyberattacks on healthcare or critical infrastructure are viewed not merely as technical failures but as ethical threats to life. Thus, critical infrastructure protection and cyber-resilience become moral imperatives within the *Nafs* framework.

Taken together, these three objectives do more than give existing security goals an Islamic vocabulary. Their real value is that they reorder priorities. A conventional risk-based framework ranks harms by expected financial loss. A Maqasid-based reading, by contrast, treats threats to life and to the integrity of knowledge as more serious than an equivalent loss of money. A probabilistic risk matrix would treat the RM2.97 billion in scam losses and an attack on hospital systems in much the same way. *Hifz al-Nafs* ranks them differently. This gives a defensible reason to protect critical infrastructure first, rather than simply minimising total losses.

Even so, the mapping faces two objections that the reviewed studies largely leave unanswered. The first is post-hoc rationalisation. If a Maqasid category is invoked only after a technical control has been chosen, the framework justifies decisions instead of guiding them, and almost any governance measure can be fitted to some objective. The second is that the framework gives no clear answer when objectives conflict. *Hifz al-Aql* supports algorithmic transparency and access to information, while *Hifz al-Mal* and *Hifz al-Nafs* may support restricting and localising the same data. Classical Islamic legal theory (*usul al-fiqh*) does offer established principles for ranking such competing objectives, but no study reviewed here applies them to an actual ICT trade-off. In this literature, therefore, Maqasid Shariah works as a normative orientation rather than as a decision procedure. That distinction explains the deficit documented below.

The Implementation Gap:

Despite these conceptual links, the SLR reveals an operationalization deficit. Only 25% (18/71) of the studies explicitly utilize Maqasid Shariah, and even fewer provide actionable governance models or policy mechanisms. While the relevance of Maqasid is established theoretically, its translation into functional ICT regulatory environments remains underdeveloped, marking a significant gap this research aims to bridge.

Three factors plausibly explain this 25% figure. The first is disciplinary separation. Cybersecurity and data governance research appears in technical and policy journals that do not draw on Shariah expertise, while Islamic studies journals rarely require technical validation. Few authors are therefore equipped to write across both fields. The second is methodological difficulty. Maqasid objectives are qualitative ends, and turning them into auditable indicators, thresholds, or compliance tests takes design work that a conceptual paper is not required to do. The third is the incentive structure. Conceptual alignment papers are publishable, while operational models need institutional access and evaluation data that most researchers do not have.

The figure also has limits as evidence. It counts only studies that name Maqasid explicitly, so it understates real alignment. Several studies use duty-of-care, public-interest, or *maslahah*-like reasoning without naming the framework. At the same time, naming the framework is not a measure of rigour, and some of the 18 studies use Maqasid terminology only decoratively. The stronger claim is therefore not that Maqasid is under-cited. It is that the studies which do cite it assert far more than they specify in operational terms, and that is the deficit this study addresses.

Gaps in Integrating Maqasid Shariah with ICT Governance (RQ3)

The literature review reveals a fragmented landscape where data sovereignty, cybersecurity, AI ethics, and Islamic frameworks remain isolated. This leads to three critical gaps: ethical-technical decoupling, where ICT frameworks lack engagement with Islamic traditions; a lack of operationalization, as Maqasid Shariah remains conceptual rather than functional; and contextual deficiency, with a scarcity of research on integrating these principles into national frameworks like Malaysia's.

These three gaps are not separate weaknesses. They form a cycle in which each one reinforces the next. The ethical-technical decoupling comes first. ICT governance research and Islamic ethical research appear in separate journals and follow different standards of evidence, so neither is obliged to engage the other. That separation then produces the operationalization gap. A framework that is never tested against technical constraints is never forced to specify indicators, thresholds, or the institutions responsible. The lack of operational detail in turn produces the contextual gap, because policymakers cannot adopt what cannot be implemented or audited. Without national case studies, the empirical material that would otherwise draw the two literatures together is missing. Seeing the gaps as a cycle changes what an adequate response looks like. More conceptual mapping addresses only the weakest link. An operational model applied to a real national setting, by contrast, intervenes at the point where the cycle can be broken.

This points to an urgent need for interdisciplinary research that brings technological governance, regulation, and Maqasid-based ethics together into a single, coherent model.

Implications for Developing an Ethical ICT Governance Model for Malaysia (RQ4)

The synthesis of literature informs the development of a Shariah-aligned ICT governance model for Malaysia through three essential shifts:

- **Integrated Architecture:** Effective governance must move beyond isolated policies toward a synchronization of legal frameworks, technological safeguards, and institutional coordination. Robust infrastructures must be structurally linked to regulatory mandates like the Cyber Security Act 2024.
- **Cultural-Ethical Localization:** While global standards (e.g., OECD, UNESCO) offer a foundation, incorporating Maqasid Shariah ensures that digital transformation aligns with the values of Muslim-majority societies. This localization strengthens public trust and ensures technological innovation serves societal wellbeing.
- **Holistic Ecosystem Management:** Data sovereignty, data safety, and AI ethics are not separate issues but interconnected components of a single governance ecosystem.

Consequently, the literature advocates for a unified ICT governance framework for Malaysia. By integrating legal compliance and technological resilience with Shariah-aligned ethical principles, Malaysia can establish a digital environment that meets global standards while remaining anchored in local societal values.

That conclusion holds only under three conditions, none of which the reviewed studies establish. Integrating the three pillars is an institutional problem before it is a design problem. The Cyber Security Act 2024, the PDPA 2010, and sectoral regulators spread authority across agencies with different mandates. Synchronising them therefore requires deciding which agency holds which powers, and no reviewed study sets this out. The overlap is already operational. A single incident exposing NCII personal data triggers two notifications: one to the Chief Executive of NACSA, with particulars due within six hours under the Cyber Security (Notification of Cyber Security Incident) Regulations 2024, and one to the Personal Data Protection Commissioner under the PDPA. Two regulators, two reporting clocks, one event, and none of the reviewed studies addresses how the duties should be sequenced or which takes precedence where they conflict.

Cultural and ethical localisation also carries a cost that the literature tends to omit. Departing from OECD or UNESCO instruments can raise compliance burdens for cross-border data flows and invite claims of protectionism. Localisation is therefore defensible only when the ethical gain is stated clearly and the loss of interoperability is kept limited. Finally, in a religiously plural society, a Maqasid-grounded framework earns broad legitimacy only if its objectives are justified in terms that non-Muslim citizens can also endorse. The three objectives already admit such a statement: Hifz al-Nafs as the protection of life, Hifz al-Mal as the protection of wealth, and Hifz al-Aql as the protection of intellect, understood as epistemic integrity.

Two limitations apply to these implications. The synthesis rests on published literature rather than on implementation data, so the proposed shifts are derived by analysis and have not been tested empirically. The reviewed studies are also weighted toward legal and conceptual work, which may tilt the model toward regulatory instruments at the expense of technical and operational controls. Testing the framework against Malaysian agency practice and developing measurable indicators for each Maqasid objective are necessary next steps, not conclusions that follow automatically from this review.

CONCLUSION

This research integrates the convergence of data sovereignty, safety, and ethical governance in Malaysia through three core themes. First, governance fragmentation persists despite regulatory progress, leaving critical gaps in cross-border data control and institutional coordination. Second, an ethical gap remains as predominant ICT models often fail to align with the cultural and religious values of Muslim-majority societies. Finally, the Maqasid Shariah solution offers a holistic foundation to anchor technological innovation in societal wellbeing and public trust. Ultimately, this research advocates for a unified governance model balancing economic growth with ethical sustainability to secure Malaysia’s digital future.

DECLARATIONS

Acknowledgements We gratefully acknowledge the financial support provided by Universiti Sains Islam Malaysia (USIM) for covering the journal publication fee. The contributions of all parties are deeply appreciated and have significantly enriched the quality and impact of this work.	Competing Interest The author(s) declare that they have no competing interests.
Authors' contributions Nurafifah Mohd Nor: Conceptualization, methodology, formal analysis, writing - original draft preparation, writing - review and editing. Nur Ilyana Ismarau Tajuddin: Supervision, conceptualization, methodology, writing - review and editing. Norita Md Norwawi: Supervision, conceptualization, methodology, writing - review and editing. Nur Aina Abdulah: Supervision, validation, writing - review and editing. All author(s) read and approved the final manuscript.	Ethics Approval This study did not require ethical approval as it involved only the analysis of previously published literature and did not involve human participants or the collection of primary data.
Data Availability All data generated or analysed during this study are included in this published article.	Use of Artificial Intelligence ChatGPT was used solely to assist with language editing and to improve the clarity of the manuscript. All content, analysis, arguments, and conclusions were reviewed, verified, and approved by the author(s), who remain fully responsible for the final manuscript.

REFERENCES

Ababneh, M., & Aljarrah, A. (2024). Role of artificial intelligence in data protection for digital asset systems: A review of recent development. *TEM Journal*, 13(4), 3431–3444. <https://doi.org/10.18421/TEM134-76>

Abbas, A. E., Van Velzen, T., Ofe, H., Van De Kaa, G., Zuiderwijk, A., & De Reuver, M. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. *Electron Markets*, 34(1), 20. <https://doi.org/10.1007/s12525-024-00695-2>

- Agarwal, A., & Nene, M. J. (2024, July). Addressing AI risks in critical infrastructure: formalising the AI incident reporting process. In *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)* (pp. 1-6). IEEE. <https://doi.org/10.1109/CONECCT62155.2024.10677312>
- Albaroudi, E., Elbehairy, M., Al Hinnawi, M. N. E., Hatamleh, M., Mansouri, T., & Alameer, A. (2025). Empowering Data Sovereignty through Artificial Intelligence: A Framework for Sustainable Smart Energy Systems. *Current Journal of Applied Science and Technology*, 44(9), 77-88. <https://doi.org/10.36227/techrxiv.175355730.00217604/v1>
- Albous, M., Al-Jayyousi, O. R., & Stephens, M. (2025). AI governance in the GCC states: a comparative analysis of national AI strategies. *Journal of Artificial Intelligence Research*, 82, 2389–2422. <https://doi.org/10.48550/arXiv.2505.02174>
- Ali, F., Bouzoubaa, K., Gelli, F., Hamzi, B., & Khan, S. (2025). Islamic Ethics And AI: An Evaluation of Existing Approaches to AI Using Trusteeship Ethics. *Philosophy & Technology*, 38(3), 120. <https://doi.org/10.1007/s13347-025-00922-4>
- Alibeigi, A., & Munir, A. (2020). Malaysian Personal Data Protection Act, a mysterious application. *University of Bologna Law Review*, 5, 362–374. <https://doi.org/10.6092/issn.2531-6133/12441>
- Aljawi, M. F., & Santiago, F. (2025). Harmonization of National and International Law in the Utilization of AI for the Organization of Hajj A Collaborative Study Between the Governments of Indonesia and Saudi Arabia in Hajj Technology Systems. *Jurnal Greenation Sosial dan Politik*, 3(2), 185-194. <https://doi.org/10.38035/jgsp.v3i2.356>
- Aloufi, A., Khan, M. A., & Hussain, B. (2025). Legal Gaps, Islamic Ethics, and Digital Trust: Building a Regulatory Framework for Saudi E-Commerce Under Vision 2030. *Journal of Cultural Analysis and Social Change*, 3860-3880. <https://doi.org/10.64753/jcasc.v10i4.3678>
- Al-Shatibi (1996) Al-Muwafaqat Fi Usul al-Syariah, Vol. 2. *Dar al-Ma'rifah*, Beirut.
- Asgarinia, H., Chomczyk Penedo, A., Esteves, B., & Lewis, D. (2023). “Who Should I Trust with My Data?” Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies. *Information*, 14(7), 351. <https://doi.org/10.3390/info14070351>
- Awais, A., Mehmood, M. U., & Goraya, M. M. (2025). Managing cyber security risks in Islamic fintech: A Shariah perspective. *Contemporary Journal of Social Science Review*, 3(4), 1674-1688. <https://doi.org/10.63878/cjssr.v3i4.1784>
- Azizli, K., Gargari, E. H., Muchtar, A. H., & Sahal, A. (2025). Artificial Intelligence and Islamic Jurisprudence: A Critical Analysis of Legal and Ethical Challenges in Automated Decision-Making. *Journal of Islamic Law and Legal Studies*, 2(2), 134-150. <https://doi.org/10.70063/jills.v2i2.117>
- Bandaru, V. N. R., Sumalatha, M., Rafee, S. M., Prasadraju, K., & Lakshmi, M. S. (2024). Enhancing privacy measures in healthcare within cyber-physical systems through cryptographic solutions. *EAI Endorsed Transactions on Scalable Information Systems*, 11(6). <https://doi.org/10.4108/eetsis.5732>
- Bashori, Y. A., Umami, K., & Wahid, S. H. (2024). Maqasid Shariah-based digital economy model: Integration, sustainability and transformation. *Malaysian Journal of Syariah and Law*, 12(2), 405–425. <https://doi.org/10.33102/mjssl.vol12no2.647>
- Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. *AI and Ethics*, 5(3), 3265-3279. <https://doi.org/10.21203/rs.3.rs-4784792/v1>
- Bernama. (2025, August 1). *AI without accountability? Why Malaysia needs new laws*. <https://www.bernama.com/en/thoughts/news.php?id=2452021>

- Bernama. (2025, August 12). *Malaysia to develop digital trust and data security strategy, establish data commission* – Gobind. <https://www.bernama.com/en/news.php?id=2455713>
- Bernama. (2026, June 24). *Trend kerugian penipuan dalam talian melonjak dalam tempoh tiga tahun - KDN*. <https://bernama.com/radio/news.php?id=2572388>
- Bobbert, Y., & Timmermans, T. (2024, November). Overcoming the Fear of Missing Out on Data. In *Proceedings of the Future Technologies Conference* (pp. 90-98). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-73128-0_7
- Cyber Security Act 2024 (Act 854) (Malaysia). <https://www.nacsa.gov.my/act854.php>
- Cyber Security (Notification of Cyber Security Incident) Regulations 2024, P.U. (A) 220/2024 (Malaysia). <https://www.nacsa.gov.my/act854.php>
- CyberSecurity Malaysia. (2023). *Cyber security incident statistics report*.
- Dahlan, H. A., Dahlan, H. A., & Dahlan, N. K. (2025). Modeling Ai-Generated Misinformation: Shariah, Ethical and Forensic Perspectives from Malaysia. *LexForensica: Journal of Forensic Justice and Socio-Legal Research*, 2(2), 74-84. <https://doi.org/10.33102/yy54vr91>
- Darus, M., Husin, N. K., Abidin, N. H., Khadzali, N. R., & Madan, M. (2024). Ethical governance through Maqasid Shariah perspective: A conceptual framework. *International Journal of Academic Research in Business and Social Sciences*, 14(10). <https://doi.org/10.6007/IJARBSS/v14-i10/23148>
- Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: a review. *International Journal of Software Engineering & Applications (IJSEA)*, 13(5). <https://doi.org/10.5121/ijsea.2022.13502>
- Data Sharing Act 2025 (Act 864) (Malaysia). <https://www.jdn.gov.my/en/data-sharing-act-2025-act-864/>
- Daud, M. (2025). A Legal Framework for Public Sector Data Sharing in Malaysia: The Clash Between Data Protection, Privacy and Public Interest. *IIUM Law Journal*, 33(2), 279-320. <https://doi.org/10.31436/iiumlj.v33i2.1072>
- De Colle, G. (2024, May). Towards an Ontology of Data Sovereignty and Ownership in Cyberspace. In *European Semantic Web Conference* (pp. 55-63). Cham: Springer Nature Switzerland. https://link.springer.com/chapter/10.1007/978-3-031-78955-7_6
- Del Re, E. (2024). Technologies of data protection and institutional decisions for data sovereignty. *Information*, 15(8), 444. <https://doi.org/10.3390/info15080444>
- Durango, I., Gallud, J. A., & Penichet, V. M. (2024). Human-data interaction framework: A comprehensive model for a future driven by data and humans. *arXiv preprint*. <https://doi.org/10.48550/arXiv.2407.21010>
- Dusuki, A. W., & Bouheraoua, S. (2021). The framework of Maqasid Shariah and its implication for governance and public policy. *Journal of Islamic Ethics*, 5(2), 173–190. <https://doi.org/10.52282/icr.v2i2.651>
- Elgujja, A., & Alkali, U. (2025). Privacy-by-Design, Digital Dignity, and Algorithmic Justice in Healthcare AI: A Comparative Legal, Ethical, and Technical Analysis of Saudi Arabia and Nigeria. <https://dx.doi.org/10.2139/ssrn.5979295>
- Elgujja, A. A., Alshahrani, F. S., Arimoro, A., Hersi, A., Musa, H., & Ezreqat, S. A. (2026). Ethical and Legal Implications of Artificial Intelligence in Infection Prevention and Control: A Saudi Arabian Perspective. *Journal of Nature and Science of Medicine*, 9(3), 291–299. https://doi.org/10.4103/jnsm.jnsm_239_25
- Farid, A. M., Pratama, F. A., & Sulistyowati, D. (2025). Maqashid Sharia Analysis on Personal Data Protection from the Dangers of Artificial Intelligence Misuse. *Jurnal Penelitian Ilmu-Ilmu Sosial*, 6(2), 179-192. <https://doi.org/10.23917/sosial.v6i2.12636>

- Fatarib, H., Ardhiansyah, M. F., Maulidini, A., & Riyandani, S. (2025, December). Qiyas As a Method of Digital Ijtihad for Social Sustainability in ASEAN In the Era of Technological Disruption. In *Proceeding of ICCoLaSS: International Collaboration Conference on Law, Sharia and Society* (Vol. 4, No. 1, pp. 26-45).
- Figuerola, V., Sanchez Crespo, L. E., Santos-Olmo, A., Rosado, D. G., & Fernandez-Medina, E. (2025). Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. *International Journal of Information Security*, 24(3), 121. <https://doi.org/10.1007/s10207-025-01024-0>
- Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, 109, 102382. <https://doi.org/10.1016/j.cose.2021.102382>
- Fouad, N. S. (2025). Failing better in the infosphere: ontological uncertainties and the essence of security in cyberspace. *Information, Communication & Society*, 1-18. <https://doi.org/10.1080/1369118X.2025.2492574>
- Gonzalez-Granadillo, G., Menesidou, S. A., Papamartzivanos, D., Romeu, R., Navarro-Llobet, D., Okoh, C., Nifakos, S., Xenakis, C., & Panaousis, E. (2021). Automated Cyber and Privacy Risk Management Toolkit. *Sensors*, 21(16), 5493. <https://doi.org/10.3390/s21165493>
- Gorian, E., & Osman, N. D. (2024). Digital ethics of artificial intelligence (AI) in Saudi Arabia and United Arab Emirates. *Malaysian Journal of Syariah and Law*, 12(3), 583-597. <https://doi.org/10.33102/mjssl.vol12no3.798>
- Hadi, A. S. A., Masum, A., & Arowosaiye, Y. I. (2025). The Artificial Intelligence and Dispute Resolution in Brunei: Assessing Readiness, Legal Reform, and the Way Forward. *Indonesia Law Reform Journal*, 5(2), 189-208. <https://doi.org/10.22219/ilrej.v5i2.40541>
- Hamza, S. M. An AI-Driven Blockchain Framework for Intelligent Halal Data Governance and Digital Evidence Integrity Across the Halal Supply Chain.
- Harun, Q. N. (2025). Menilai semula kedaulatan data Malaysia: Kritikan struktural terhadap Akta Perkongsian Data 2025: Reassessing Malaysia's data sovereignty: A structural critique of the Data Sharing Act 2025. *International Journal of Interdisciplinary and Strategic Studies*, 6(10), 631-657. <https://doi.org/10.47548/ijistra.2025.98>
- Hippelainen, L., Oliver, I., & Lal, S. (2017, July). Towards dependably detecting geolocation of cloud servers. In *International Conference on Network and System Security* (pp. 643-656). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-64701-2_51
- Hoong, Y., & Rezanian, D. (2024). Navigating cybersecurity governance: the influence of opportunity structures in socio-technical transitions for small and medium enterprises. *Computers & Security*, 142, 103852. <https://doi.org/10.1016/j.cose.2024.103852>
- Huawei Technologies Malaysia, & Malaysia Digital Economy Corporation (MDEC). (2022). Malaysia: Towards becoming ASEAN's digital capital: Value creation for ASEAN digital growth.
- Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1). <https://doi.org/10.1177/2053951720982012>
- Jansen, B., Kadenko, N., Broeders, D., Van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4). <https://doi.org/10.1016/j.giq.2023.101862>
- Kannike, U. M. M., & Fahm, A. O. (2025). Exploring the ethical governance of artificial intelligence from an Islamic ethical perspective. *Jurnal Fiqh*, 22(1), 134-161. <https://doi.org/10.22452/fiqh.vol22no1.5>

- Krotov, V., & Johnson, L. (2023). Big web data: Challenges related to data, technology, legality, and ethics. *Business Horizons*, 66(4), 481-491. <https://doi.org/10.1016/j.bushor.2022.10.001>
- Lam, W. M. W., & Seifert, J. (2023). Regulating data privacy and cybersecurity. *The Journal of Industrial Economics*, 71(1), 143-175. <https://doi.org/10.1111/joie.12316>
- Leicht, J., Wagner, M., & Heisel, M. (2023, September). Creating privacy policies from data-flow diagrams. In *European Symposium on Research in Computer Security* (pp. 433-453). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-54204-6_26
- Malay Mail. (2023, December 8). *Socso confirms cyberattack, claims leaked data is questionable and incomplete*. <https://www.malaymail.com/news/malaysia/2023/12/08/socso-confirms-cyberattack-claims-leaked-data-is-questionable-and-incomplete/106563>
- Malaysian Bar. (2025, June 25). *Press statement: Rebuilding the public trust deficit with regard to personal data collection* [Press release]. <https://www.malaysianbar.org.my/article/news/press-statements/press-statements/press-statement-rebuilding-the-public-trust-deficit-with-regard-to-personal-data-collection>
- Maman, N. E., & Susila, W. D. A. P. (2025). Artificial Intelligence and Machine Learning in Financial Industry Transformation: A Comparative Analysis of Conventional and Sharia Fintech in Indonesia. *Journal of Finance and Islamic Banking*, 8(2), 141-158. <https://doi.org/10.22515/jfib.v8i2.12901>
- Mia, M. H., Hossain, K. A., & Ali, M. M. (2026). Designing Ethical AI-Integrated Cybersecurity Education: A Qur'anic Values Informed Framework for Responsible Digital Learning. <https://doi.org/10.21203/rs.3.rs-9305391/v1>
- Micheal, Lee. (2024). Cross-Border Data Transfer Risks and Compliance Solutions for Cloud-Based Generative AI.
- Ministry of Digital Malaysia. (2025, October 11). *Allocations in Belanjawan MADANI 2026 set to spur Malaysia's digital transformation* [Press release]. <https://www.digital.gov.my/en-GB/siaran/Peruntukan-Dalam-Belanjawan-Madani-2026-Akan-Merangsang-Transformasi-Digital-Malaysia>
- Ministry of Science, Technology and Innovation (MOSTI). (2024). *The national guidelines on AI governance and ethics (AIGE)*. <https://mastic.mosti.gov.my/publication/the-national-guidelines-on-ai-governance-ethics/>
- Misra, S., Barik, K., & Kvalvik, P. (2025). Trust in Digital Sovereignty: A Review of Security, Privacy, and Governance Challenges. *Public Organization Review*, 1-23. <https://doi.org/10.1007/s11115-025-00968-0>
- Mohadi, M., & Tarshany, Y. M. A. (2023). Maqasid al-Shari'ah and the ethics of artificial intelligence: Contemporary challenges. *Journal of Contemporary Maqasid Studies*, 2(2), 79-102. <https://doi.org/10.52100/jcms.v2i2.107>
- Mohiqi, M. M. (2023). Data's nature and its prevailing right under Islamic law. *International Journal of Multicultural and Multireligious Understanding*, 10(3), 221-230. <https://doi.org/10.18415/ijmmu.v10i3.4559>
- Molitor, D., Raghupathi, W., Saharia, A., & Raghupathi, V. (2023). Exploring Key Issues in Cybersecurity Data Breaches: Analyzing Data Breach Litigation with ML-Based Text Analytics. *Information*, 14(11), 600. <https://doi.org/10.3390/info14110600>
- Mujahid, A. R., Mustofa, T. A., & Jinan, M. (2025). Islamic Ethical Values as The Foundation for The Use of Artificial Intelligence in Islamic Boarding School Education. *Proceeding ISETH (International Summit on Science, Technology, and Humanity)*, 1124-1132. <https://doi.org/10.23917/iseth.6916>

- Mustapha, R., Karim, S., Ibrahim, N., Burhan, N., & Hayati, N. (2025). Islamic perspectives on AI and cybersecurity: Developing ethical frameworks for autonomous security systems. *International Journal of Law Government and Communication*, 10(40), 590-604. <https://doi.org/10.35631/IJLGC.1040041>
- MyCERT. (2025, February 27). *Cyber incident quarterly summary report Q4 2024* (Report No. SR-029.022025). CyberSecurity Malaysia. <https://www.mycert.org.my/portal/advisory?id=SR-029.022025>
- New Straits Times. (2024, March 25). *Sarawak seeks clarification on security of information collected for PADU*. <https://www.nst.com.my/news/nation/2024/03/1030251/sarawak-seeks-clarification-security-information-collected-padu>
- New Straits Times. (2025, July 15). *AI deepfakes of PM, tycoons used in scams*. <https://www.nst.com.my/news/nation/2025/07/1240382/ai-deepfakes-pm-tycoons-used-scams>
- Nugraha, Y., & Martin, A. (2022). Cybersecurity service level agreements: understanding government data confidentiality requirements. *Journal of Cybersecurity*, 8(1), tyac004. <https://doi.org/10.1093/cybsec/tyac004>
- Nugroho, B. S., & Al-Giffari, H. A. (2026). Institutionalizing Artificial Intelligence within Indonesia's Zakat Architecture: Navigating Regulatory Challenges and Sharia Compliant Implementation. *Indonesian Journal of Islamic Economic Law*, 3(1), 113-143. <https://doi.org/10.23917/ijael.v3i1.13927>
- Osman, R. A. H., Zakariyah, L., Zakariyah, H., & Dahlan, A. R. A. (2021). Cyber security and Maqasid al-Shariah: A case of Facebook application. *International Research Journal of Shariah, Muamalat and Islam (IRJSMI)*, 3(6), 12-25. <https://gaexcellence.com/irjsmi/article/view/91>
- Othman, A. (2025). Data Sovereignty and National Cloud Strategy: The Case of Malaysia. <https://doi.org/10.13140/RG.2.2.33060.13442>
- Pahune, S., Akhtar, Z., Mandapati, V., & Siddique, K. (2025). The importance of AI data governance in large language models. *Big Data and Cognitive Computing*, 9(6), 147. <https://doi.org/10.3390/bdcc9060147>
- Personal Data Protection Act 2010 (Act 709) (Malaysia). <https://www.pdp.gov.my/ppdpv1/en/akta/pdp-act-2010-en/>
- Pestana, G., & Sofou, S. (2024). Data governance to counter hybrid threats against critical infrastructures. *Smart Cities*, 7(4), 1857-1877. <https://doi.org/10.3390/smartcities7040072>
- Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, 4(1), 1-19. <https://doi.org/10.1007/s44206-025-00189-4>
- Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, 74, 102719. <https://doi.org/10.1016/j.ijinfomgt.2023.102719>
- Porcedda, M. G. (2023). Cybersecurity, Privacy and Data Protection in EU Law.
- Qiu, Y., & Hu, Z. (2025). Progress and recommendations in data ethics governance: a transnational analysis based on data ethics frameworks. *Humanities and Social Sciences Communications*, 12(1), 1-11. <https://doi.org/10.1057/s41599-025-05664-4>
- Raquiab, A., Channa, B., Zubair, T., & Qadir, J. (2022). Islamic virtue-based ethics for artificial intelligence. *Discover Artificial Intelligence*, 2(1), 11. <https://doi.org/10.1007/s44163-022-00028-2>

- Rizk, A. M. (2026). Integrating Artificial Intelligence into Credit Risk Assessment (A Comparative Study of Islamic and Conventional Banks). *Ajrsp*, 7(82), 05-26. <https://doi.org/10.52132/Ajrsp.e.2026.82.1>
- Rofiq, A. F. N., Rahman, M. S., Shaikh, A. Y., Barry, M. B., & Zeki, A. M. (2025). Online Data Privacy Ethical Guidelines based on Islamic Perspectives. *International Journal on Islamic Applications in Computer Science and Technology*, 13(2).
- Samonte, M. J., Alvaran, R. M., Imutan, J., & Savellano, R. G. (2024, July). Building a privacy-centric systems integration and architecture. In *Proceedings of the 2024 12th International Conference on Computer and Communications Management* (pp. 121-131). <https://doi.org/10.1145/3688268.3688287>
- Saqib, H. M., & Amin, H. (2026). Comparative analysis of AI regulation for fintech cybersecurity and privacy in the European Union and Qatar. *Discover Artificial Intelligence*. <https://doi.org/10.1007/s44163-025-00736-5>
- Sawari, M. F. M., Shamsuddin, M. M. J., & Robbi, A. A. M. (2025). Integrating Maqāsid al-Sharī'ah and governance principles: a framework for SME Shariah financial compliance. *International Journal of Fiqh and Usul Al-Fiqh Studies*, 9(3), 97-116. <https://doi.org/10.31436/ijfus.v9i3.408>
- Schubert, K. D., & Barrett, D. (2024). Data governance, privacy, and ethics. In *Human Privacy in Virtual and Physical Worlds: Multidisciplinary Perspectives* (pp. 87-110). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-51063-2_5
- Sharif, A., & Badi, S. (2025). The Digital Evolution of Financial Crime: How Cross-Border Fraud is Reshaping Cybersecurity. <https://doi.org/10.13140/RG.2.2.21643.81443>
- Skopik, F., Bonitz, A., Grantz, V., & Gohler, G. (2022). From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. *International Journal of Information Security*, 21(6), 1323-1347. <https://doi.org/10.1007/s10207-022-00613-7>
- Smolo, E. (2026). Islamic Finance in the Digital Age: Fintech as a Civilizational Tool. *Religions*, 17(2), 218. <https://doi.org/10.3390/rel17020218>
- Solaiman, B., Bashir, A., & Dieng, F. (2024). Regulating AI in health in the Middle East: case studies from Qatar, Saudi Arabia and the United Arab Emirates. *Research handbook on health, AI and the law*, 332-354. <https://doi.org/10.4337/9781802205657.ch19>
- Sorrentino, E., Spagnuolo, A. F., Portaro, A., Taverniti, M., & Cardillo, E. (2025, July). Towards Semantic Coherence: Understanding Cybersecurity and Digital Sovereignty in the Automotive Landscape. In *2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS)* (pp. 1-5). IEEE. <https://doi.org/10.1109/IOLTS65288.2025.11116851>
- The Straits Times. (2022, May 18). *Data of 22.5 million Malaysians born 1940–2004 allegedly being sold for US\$10k*. <https://www.straitstimes.com/asia/se-asia/data-of-225-million-malaysians-born-1940-2004-allegedly-being-sold-for-us10k>
- Thomas, L., Gondal, I., Oseni, T., & Firmin, S. S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers & Security*, 116, 102657. <https://doi.org/10.1016/j.cose.2022.102657>
- Uddoh, J., Ajiga, D., Okare, B. P., & Aduloju, T. D. (2021). Cross-border data compliance and sovereignty: a review of policy and technical frameworks. *Journal of Frontiers in Multidisciplinary Research*, 2(2), 68-74. <https://doi.org/10.54660/.IJFMR.2021.2.2.68-74>
- Verstraete, M., & Zarsky, T. (2021). Optimizing breach notification. *U. Ill. L. Rev.*, 803.
- Vostoupal, J., Stupka, V., Harasta, J., Kasl, F., Loutocky, P., & Malinka, K. (2024). The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. *Computer Law & Security Review*, 53, 105988. <https://doi.org/10.1016/j.clsr.2024.105988>

- Wahab, A. W., & Mahdiya, I. (2025). Digital Shariah governance and the future of Islamic finance: A framework for AI-driven Shariah compliance in a global regulatory environment. *International Journal of Islamic Finance*, 3(2), 19-31. <https://doi.org/10.14421/ijif.v3i2.2777>
- Wang, Y., Duan, Y., Han, J., Chen, Z., Yin, M., & Zhong, G. (2025). Privacy-enhanced deep learning inference acceleration towards third-party cloud based on trusted execution environment. *Peer-to-Peer Networking and Applications*, 18(3), 162. <https://doi.org/10.1007/s12083-025-01978-x>
- Waseem, U., & Rahim, A. (2025). Islamic Ethical Perspectives on AI and Digital Transformation in the 21st Century. *Wah Academia Journal of Global Religions*, 1(3), 31-54. <https://doi.org/10.63954/4sz9d580>
- Wexler, R. (2022). Life, Liberty, and Data Privacy: The Global CLOUD, the Criminally Accused, and Executive versus Judicial Compulsory Process Powers. *101 Texas Law Review*, 1341. <https://dx.doi.org/10.2139/ssrn.4244186>
- Williamson, B. (2022). Governing Through Infrastructural Control: Artificial Intelligence and Cloud Computing in the Data-intensive State. *Digital Society*, 52(1). <https://doi.org/10.4135/9781529783193.n29>
- Yeoh, A. (2023, December 6). Cybersecurity report ranks Malaysia as eighth most breached country in Q3 2023. *The Star*. <https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity-report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023>
- Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of applied security research*, 16(4), 490-513. <https://doi.org/10.1080/19361610.2021.1918995>
- Zafar, M. B., & Ali, H. (2025). Shariah governance standard on generative AI for Islamic financial institutions. *SSRN Electronic Journal*. <https://dx.doi.org/10.1108/JIABR-03-2025-0141>
- Zhou, F., & Huang, J. (2024). Cybersecurity data breaches and internal control. *International Review of Financial Analysis*, 93, 103174. <https://doi.org/10.1016/j.irfa.2024.103174>