Journal of Islamic Law on Digital Economy and Business
2025, 1(2), 121-138

Constitutionalizing cybersecurity: Indonesia–Malaysia regulatory convergence through a maqasid al Sharia framework

Farid Al Hadana[1], Tashekal Tashekal[2], Sukarman Sukarman[3], Farhan Margono[4]

[1]Constitutional Law, Sharia Faculty and Islamic Law, Institut Agama Islam Negeri Bone, Watampone, Indonesia
[2]Political Science, Faculty of Usuluddin and Philosophy, Universitas Islam Negeri Alauddin Makassar, Gowa, Indonesia
[3]Constitutional Law, Graduate School, Institut Agama Islam Negeri Bone, Watampone, Indonesia
[4]Islamic Family Law, Graduate School, Institut Agama Islam Negeri Bone, Watampone, Indonesia

Article Info

Article history
Received : 2026-01-11
Revised : 2026-02-17
Accepted : 2026-02-26
Published : 2026-02-27

Keywords:
Cybersecurity law, Regulatory harmonization; Maqasid al-Sharia

DOI:
10.20885/JILDEB.vol1.iss2.art2

JEL classification:
K23, L86, O33, K20, F13

Corresponding author:
Farid Al Hadana
faridhadana171@gmail.com

Author's email:
tashekal67@gmail.com
sukarman.m.h@gmail.com
farhanmargono19@gmail.com.

Paper type:
Research paper

Abstract

Purpose – This article examines the evolving regulatory architectures of cybersecurity and cyber resilience in Indonesia and Malaysia and proposes harmonization strategies that are both responsive to escalating cyber risks and normatively fair, using maqasid al-Sharia as an evaluative lens.

Methodology – This study employs a qualitative doctrinal approach combined with a comparative legal analysis. Primary materials (statutes, regulations, policy documents, and case law where available) are systematically interpreted and contrasted, and are triangulated with recent high-impact international scholarship on cyber security law, digital constitutionalism, and Islamic legal theory.

Findings – The analysis shows that Indonesia is moving towards cyber resilience through incremental institutional strengthening and the coordination of fragmented sectoral regimes, while Malaysia adopts a more centralized model via dedicated cybersecurity legislation focused on the National Critical Information Infrastructure. These divergent trajectories shape risk allocation, incident reporting and accountability mechanisms. This study identifies a set of functionally equivalent harmonization strategies: baseline obligations, mutual recognition of standards and certification, interoperable incident reporting, and institutional interoperability, and demonstrates how maqasid al-Sharia reframes these as instruments to protect life, intellect, property, dignity, and social order.

Implications – The findings offer concrete guidance for regulators and policymakers in designing cybersecurity frameworks that enhance resilience without legitimizing disproportionate state power in the digital domain and provide a normative benchmark for Muslim-majority jurisdictions.

Originality – This study is among the first to integrate digital constitutionalism, comparative public law, and maqasid al-Sharia into a single analytical framework to assess and harmonize cybersecurity regulations in Indonesia and Malaysia.

Cite this article:
Al Hadana, F., Tashekal, T., Sukarman, S., & Margono, F. (2025). Constitutionalizing cybersecurity: Indonesia–Malaysia regulatory convergence through a maqasid al-Sharia framework *Journal of Islamic Law on Digital Economy and Business*, *1*(2), 121-138. https://doi.org/10.20885/JILDEB.vol1.iss2.art2.

Centre for Islamic Economics Studies and Development, Faculty of Business and Economics, Universitas Islam Indonesia

Introduction

The digital transformation in Indonesia and Malaysia over the past decade has increased their dependence on ICT-based infrastructure and service. This encompasses various sectors, such as population, fiscal, health, transportation, and payment systems. Thus, cyberspace is no longer

merely a technical aspect but also a constitutional space that shapes the fulfilment of rights, legitimacy of policies, and government effectiveness.

In the context of a state governed by the rule of law, this change requires a reconsideration of the relationship between sovereignty, rights protection, and regulatory functions, particularly as cyber threats increase and states respond with regulations on cybersecurity, resilience, and safety. This paper on digital constitutionalism demonstrates that digital regimes are driving a shift from a market-liberal approach to a constitutional approach that places greater emphasis on democratic values and fundamental rights (De Gregorio, 2021; De Gregorio & Radu, 2022). At this point, cybersecurity and resilience issues cannot be relegated solely to the sectoral policy level, as the design of norms, attribution of authority, accountability mechanisms, and limitations on state actions (e.g., surveillance, data processing, or the establishment of security obligations) directly intersect with constitutional principles such as the rule of law, proportionality, limitations on power, and the protection of civil liberties.

Conceptually, the comparison between Indonesia and Malaysia is interesting to examine because both countries are developing nations with aggressive digitalization agendas, yet they have followed different institutional and normative paths in this regard. Indonesia has developed a narrative on cybersecurity and resilience that is closely linked to strengthening cybersecurity institutions and umbrella legislative efforts. Conversely, Malaysia places greater emphasis on cybersecurity safety/security and the management of the Critical National Information Infrastructure (CNII), with a more centralized approach. The difference in the use of the terms resilience versus safety/security is not merely a matter of semantics. However, it reflects a paradigm in risk governance: whether the primary focus is on systemic resilience (the ability to survive and recover) or prevention and compliance through standards and oversight. The critical infrastructure protection framework emphasizes that effective regulatory design requires a clear definition of objectives (what is considered critical), a measurable model of obligations, and inter-sectoral coordination. Otherwise, fragmented norms and overlapping authorities can emerge, which can become shortcomings that reduce the state's capacity to address threats (Markopoulou & Papakonstantinou, 2021). At this stage, an analysis of constitutional law is crucial, examining how design variations (such as establishing a single authority versus a multi-actor authority) will impact the division of responsibilities, the exercise of discretion, and the manner in which disputes are resolved through constitutional oversight mechanisms (judicial review, parliamentary control, and administrative oversight).

In the digital business landscape, personal data protection is not only a legal obligation but also a tool for building trust and a prerequisite for the sustainability of digital commerce. Data collection and processing strategies influence platform revenue models while generating privacy costs and leakage risks that can harm welfare and trigger intervention from regulators (Galeotti et al., 2023). From a market behavior perspective, research in marketing and consumer behavior shows that concerns about privacy and security guarantees play a role in building trust and purchase intent in e-commerce services (Alzaidi & Agag, 2022). Meanwhile, the tension between privacy and data has shaken the relationship between consumers and companies, prompting changes in data management strategies and regulatory designs (Martin et al., 2022). In the context of international trade, privacy regulations significantly impact cross-border e-commerce flows through web traffic channels, data collection, advertising, and data sharing, ultimately creating strategic compliance consequences for multinational companies (Yan, 2024). Therefore, this study highlights the intersection of cybersecurity and personal data protection as a constitutional and economic issue, determining the legitimacy of rights protection, competitiveness, and the architecture of trust for an increasingly integrated digital ecosystem between Indonesia and Malaysia.

Cyber incidents increasingly generate systemic economic externalities that extend to supply chains, platform markets and public services. Economic research on ransomware and large-scale cyber risks shows that attack dynamics can reshape market equilibrium and cause welfare losses that are insufficiently internalized by private actors, thereby strengthening the argument for robust and enforceable regulations rather than voluntary best practices. In parallel, interdisciplinary privacy studies emphasize that privacy and cybersecurity management are now core requirements

of the digital economy, as data-intensive business models, platform intermediaries, and cross-border services make trust and resilience functional inputs for growth, rather than mere legal add-ons. In this view, the key legal question is how states design credible obligations (prevention, response, remediation, and verification) while preventing regulatory overreach that erodes market rights and fairness.

The urgency of this research stems from the fact that cybersecurity and data protection regimes now operate in a global context characterized by regulatory fragmentation, proliferation of obligations, and increasing tensions between digital sovereignty interests, rights protection, and the need for smooth data flows for digital trade. The development of digital trade law shows rapid growth in the formulation of norms and agreements related to data flows and digital economic agreements; however, their substantive convergence is uneven because of differences in domestic approaches to privacy and security (Burri et al., 2024). In fact, the legal framework for trade can "move too fast and too far" compared to the evolution of domestic privacy laws, creating a lack of synchronization that strains the regulatory capacity of countries and gives rise to the need for a more legitimate reconciliation design (Burri, 2023). In the Indonesia-Malaysia context, this situation makes the issue of "regulatory convergence" not merely an academic choice, but a governance necessity: without principled convergence, the protection of rights and certainty of business compliance will remain vulnerable as data, services, and threats move across borders.

The link between personal data protection and the digital economy and business landscape is fundamental. On the one hand, data serve as the foundation for innovation, personalization, and market efficiency; on the other hand, without adequate protection, the incentives to collect data can lead to privacy costs that negatively impact welfare and pose reputational and litigation risks for companies (Galeotti et al., 2023). Legal-technology research also shows that data protection regulations can influence the direction of global digital economic development and not only protect consumers but also impact competition and innovation through extraterritorial effects and standard setting (Niebel, 2021). At the micro level, empirical evidence shows that trust and privacy concerns are important factors influencing shopping behavior and the adoption of digital retail services, such that "strong data protection" serves as an asset of trust in the marketplace rather than mere administrative compliance (Alzaidi & Agag, 2022). Furthermore, the tension between privacy and data has altered the relationship between consumers and companies and necessitated more responsible data management strategies, which in turn require consistent normative certainty (Martin et al., 2022). Thus, the strategic value of this research lies in the development of a convergence framework that not only complies with laws and constitutions but also enhances the trust infrastructure for sustainable digital commerce.

Previous studies on cyber regulation have generally emphasized (1) the design of critical infrastructure protection frameworks (Markopoulou & Papakonstantinou, 2021), (2) the relationship between regulation and national cybersecurity maturity (AlDaajeh et al., 2022), (3) the direction of regulatory hardening through product and supply chain security obligations (Chiara, 2025; Shaffique, 2024), and (4) the constitutional dimensions of digital governance and the limitation of power (De Gregorio, 2021; De Gregorio & Radu, 2022). However, a significant gap exists: studies that combine doctrinal and comparative legal approaches in depth to map the normative architecture (hierarchy, consistency, and coherence), institutional architecture (attribution of authority, coordination, and accountability), and constitutional architecture (limitations on rights and control of power) in the context of Indonesia and Malaysia are still rare, especially with a focus on the differences in the cybersecurity and digital economic resilience paradigms in Indonesia and Malaysia.

Therefore, this study not only compares the lists of regulations but also evaluates the constitutional-regulatory models underlying both, whether they are moving towards a centralized regulatory state model, a fragmented multi-actor model, or a hybrid model, as well as their normative consequences for security effectiveness, rights protection, and governance legitimacy in the digital economy.

Literature Review

Recent international literature on cybersecurity/resilience regulation demonstrates a shift from security as a technical control to security as constitutionalized governance, in which cybersecurity is understood as a legal regime that regulates power relations among the state, digital corporations, and citizens through rights, due diligence, and accountability mechanisms. This shift is strongly evident in the current trend of digital constitutionalism, which positions the protection of fundamental rights as a legal parameter for assessing regulatory design and administrative actions in the digital space. De Gregorio (2021) asserts that the modern constitutional logic of limiting power and guaranteeing rights is shifting to address the private power of platforms and the complexities of digital governance. Cyber policy is no longer technocratic and neutral but rather fraught with normative choices about who bears the risk, who receives protection, and how the legitimacy of state action is constructed.

Within the field of cybersecurity law, works based on a risk regulation approach map regulation as systemic risk management rather than simply criminalizing incidents. Markopoulou and Papakonstantinou's (2021) paper on critical infrastructure protection (particularly in the healthcare sector) identifies classic weaknesses in the cybersecurity regime, including fragmentation of authority, weak standardisation of baseline security obligations, and implementation problems that hinge on institutional capacity and cross-sector coordination. This study is relevant in the comparative context of Indonesia and Malaysia because both countries face the challenge of multi-agency governance involving numerous institutions. However, legal design often fails to establish a transparent chain of accountability (who is obligated to do what, what sanctions are in place, and what evidence is required). At this point, the discourse on cyber resilience demands a doctrinal reading of the norms of prevention, detection, response, recovery, and compliance rather than simply a policy reading.

However, the literature on risk management obligations and incident reporting emphasizes the relationship between norm design and effectiveness against actual attack tactics. Ferguson's (2023) paper uses a legislative interpretation approach and a cyber kill chain model to demonstrate the limited effectiveness of risk management obligations if regulations do not cover the initial phases of an attack, so that formal compliance does not always correlate with substantive resilience. This discourse provides an evaluative lens for comparison: do the Indonesian and Malaysian regimes mandate outcome-oriented controls (to reduce the likelihood and impact) or simply require procedures? To emphasize the dynamic evolution of the regime, institutional information indicates that the NIS2 has been in effect since January 16, 2023, demonstrating the acceleration of compliance standards and oversight in a globally benchmarked jurisdiction.

The cybersecurity certification literature adds an important dimension: standard harmonization and compliance verification. Ferguson (2022) critiques the adequacy of minimum security objectives in certification schemes, asserting that certification can be a powerful tool for market governance. However, risks become symbolic if the minimum security objectives are not aligned with dominant threats and do not strengthen post-incident recovery or forensic capacity. For Indonesia and Malaysia, this issue is relevant because cybersecurity regimes often overlap with obligations related to certification, accreditation, audits and technical standards. Comparative doctrinal methods can examine whether compliance verification mechanisms have a clear normative basis and proportionate legal consequences.

Some studies link cyber resilience to international law and collective security, particularly in the context of critical infrastructure and attack attribution. Kouloufakos' (2023) paper shows that norms for protecting critical infrastructure in cyberspace have developed through soft law and the practices of international organizations. However, they still face challenges related to terminology and legal status. At the high political level, Poli and Sommario's (2023a) paper highlights the dilemma of state accountability and cyber sanctions regimes: on the one hand, states need deterrence; On the other hand, attribution uncertainty and diplomatic caution foster ambiguity that can erode legal certainty. This literature is important for the Indonesia-Malaysia comparison because resilience is not only about technical safeguards but also about a country's

position on attribution norms, cross-border cooperation, and response tools (administrative, criminal, and diplomatic sanctions).

The literature on rights, privacy, and governance of automated decision-making shows that cybersecurity/safety is increasingly tied to rights-based compliance. Papakonstantinou (2022) even proposed a conceptual path towards recognizing a "right to cybersecurity" in European Union law that would compel states and businesses to justify cybersecurity policies against standards of rights protection and proportionality. In the realm of implementation, discourses on the GDPR and AI (e.g., administrative decision automation and HRIA for data-intensive systems) shift the focus from simply what is safe to who is safe and with what impact. Therefore, the literature calls for the integration of security, safety, and administrative accountability. For Indonesia–Malaysia research, this opens up a gap: existing studies often separate cybersecurity from rights protection, whereas modern regimes tend to combine the two through design obligations, audits, reporting, and complaints and oversight mechanisms.

The perspective of maqāṣid al-sharīʿah can deepen the normative evaluative framework in this literature review, not as a "replacement" for modern regulatory theory, but rather as a tool for assessing objectives (teleology) that are compatible with the notion of public interest and the protection of human dignity. The Islamic framework-based AI ethics literature shows that maqāṣid, in this case the protection of life (ḥifẓ al-nafs), reason (ḥifẓ al-ʿaql), property (ḥifẓ al-māl), honour/dignity (ḥifẓ al-ʿirḍ), and religion/moral order (ḥifẓ al-dīn), can be mapped to contemporary cyber risks: attacks on healthcare and energy services threaten lives; disinformation, deepfakes, and algorithmic manipulation threaten reason and dignity; data theft and ransomware attack property; and systemic privacy violations undermine human dignity. Ali et al. (2025) demonstrate that Islamic approaches to technology ethics often utilize maqāṣid but also seek to develop a more comprehensive ethical model for technology governance, thereby opening a conceptual space to assess "resilience" as the maintenance of benefits and the prevention of cross-sectoral harms. Similarly, Raquib et al. (2022) emphasize an Islamic virtue ethics framework for AI, rooted in maqāṣid, as an alternative to global ethical standards that often take the form of soft law. This integration offers theoretical novelty: a comparative study of Indonesia–Malaysia cyber regulations can assess not only the adequacy of norms (obligations, sanctions, and authorities) but also the alignment of regulatory objectives with the protection of fundamental values widely recognized in Muslim societies in the region.

Research Methods

This study applies a qualitative-doctrinal approach combined with comparative legal analysis to describe the cybersecurity regulatory architecture of Indonesia and Malaysia as a public legal regime that regulates the distribution of authority, compliance obligations, and limits on state intervention in the digital space. Primary and secondary legal sources were systematically collected from various laws, derivative regulations, strategy/policy documents, government publications, reports from international organizations, and relevant court decisions, if available, and then interpreted doctrinally to test the coherence of norms (hierarchy, consistency, and enforceability) and the institutional logic developed by each country. This doctrinal framework is further strengthened through triangulation with influential international literature in the fields of cyber security law, digital constitutionalism, and Islamic legal theory, so that the analysis of regulatory texts does not stop at policy description, but is also able to evaluate the rationality of the design of obligations, accountability patterns, and their constitutional impact on rights and legitimacy in governance (De Gregorio & Radu, 2022; Markopoulou & Papakonstantinou, 2021; Papakonstantinou, 2022; Raquib et al., 2022).

In the analysis phase, this study uses thematic and interpretive content analysis to identify and code key themes such as legal certainty, justice, maslahah, state control, and digital ethics. It then links these themes to an evaluative framework to assess whether regulations in each jurisdiction are truly adaptive to the dynamics of threats, sufficiently inclusive, and have adequate channels for participation in the process of rule formation and implementation. Indonesia and

Malaysia were selected as a comparative design based on contextual variations: differences in legal ideology, institutional character, and policy configuration provide an opportunity to test the functional equivalence between instruments, namely whether variations in the form of norms still produce equivalent governance functions in reducing systemic risk and creating accountability mechanisms, as well as opening up opportunities for the formulation of convergence recommendations that are aligned in their objectives (Thomas, 2021). In this context, maqāṣid al-sharīʿah is used as a teleological lens to examine whether the convergence design truly protects fundamental interests (protection of life, intellect, property, dignity, and social order) without sacrificing the principles of proportionality and limitation of power (Ahmed, 2025). Thus, its methodological contribution goes beyond a simple comparison of regulatory lists to a comprehensive evaluation of the existing normative-institutional architecture and constitutional legitimacy.

Results and Discussion

The dynamics of cybersecurity regulation development in Indonesia and Malaysia

The development of cybersecurity and resilience regulations in Indonesia and cyber safety/security regulations in Malaysia over the past five years shows an interesting convergence pattern. Both countries have shifted from a paradigm of data protection and the criminalization of cybercrime to a paradigm of systemic resilience that emphasizes risk management, incident reporting obligations, strengthening critical infrastructure, standardization and certification, and authority structuring. In the context of public law, this dynamic can be understood as a form of administrative change in cybersecurity, where the state is no longer only present through criminal law and enforcement after an incident occurs but also through ex ante risk-based regulations, compliance obligations, auditability, and the ability to coordinate across sectors (Mirzaei & De Busser, 2024; Buckley et al., 2024). The perspective of digital constitutionalism asserts that when digital space becomes an arena for state functions and citizens' rights, cybersecurity becomes a constitutional requirement to protect rights, ensure the continuity of public services, and safeguard the legitimacy of the government (De Gregorio, 2021). Therefore, cybersecurity regulations are not neutral; they regulate the distribution of authority (who has the right to command, conduct inspections, and enforce compliance) while also setting the limits of proportionality of state intervention in freedom, privacy, and freedom of enterprise (De Gregorio & Radu, 2022).

In Indonesia, the dynamics of cybersecurity development tend to be characterized by gradual institutionalization, with a regulatory landscape spanning various regimes, including electronic system governance, personal data protection, sectoral regulations (finance, telecommunications, and health), and national security policies. This fragmentation enriches the instruments but also raises problems of coordination, overlapping mandates, and variations in compliance standards across sectors. Theoretically, modern cybersecurity requires polycentric governance: multiple actors (states, operators, service providers, CERT/CIRT, and security communities) interact within a regulatory network, so that the quality of response is determined not only by written norms, but also by institutional design, crisis command flows, and economic-compliance incentives (Kettemann et al., 2021). However, when polycentricity is not supported by binding minimum standards and effective crisis coordination mechanisms, it turns into a governance gap, a condition in which systemic risks increase because of governance inconsistencies.

The public service disruption caused by a ransomware attack on the National Data Centre (PDN) in 2024 became an empirical highlight, revealing the limits of governance that remain optional in crucial areas such as backup, business continuity, and cross-agency risk management. Reuters reported that the attack disrupted immigration services and airport operations, affecting hundreds of agencies nationwide. They included a highly problematic fact: 98% of the affected data was not backed up, and a data center governance audit was part of the state's response (Reuters, June 28, 2024). Regulatory-wise, events like this shift the discourse from administrative compliance to objectively testable resilience obligations, such as minimum standards for data backup, network segmentation, disaster recovery plans, and enforceable reporting obligations. In the cybersecurity

law literature, this shift is consistent with the argument that policy and law must force a transformation from security as the best effort to security as a duty, especially for systems that perform essential public functions (Kouloufakos, 2023; Markopoulou & Papakonstantinou, 2021).

In the Indonesian context, institutional responses also demonstrate the strengthening of the role of national cybersecurity authorities through strategies and governance tools that emphasize coordination, preparedness, and the formation and operationalization of incident response teams. The BSSN positions cybersecurity as a national priority issue and emphasizes the urgency of strengthening capacity across all aspects of state life, including law and organization. At the implementation level, the establishment and strengthening of CIRTs and cyber crisis management guidelines are understood as efforts to close the response gap that has arisen due to procedural unpreparedness and weak cross-agency orchestration, which is consistent with the view that "resilience" is not only technology, but also a governance architecture that enables a rapid, accountable, and coordinated response (Ferguson, 2022). However, Indonesia's challenge lies in consolidation: translating strategy into binding norms, harmonizing minimum standards across sectors, and establishing an accountability regime that goes beyond policy.

This contrasts with Malaysia, which exhibits a relatively more centralized dynamic through specific legislation that explicitly regulates the critical information infrastructure and incident management. The Cyber Security Act 2024 (Act 854) introduces key features regarding the formation of a national cyber security committee, the structuring of the authority of the Chief Executive of NACSA, the affirmation of the role of sector leads and NCII (National Critical Information Infrastructure) entities, the management of threats and incidents related to NCII, and licensing provisions for cyber security service providers (Cyber Security Act 2024 (Act 854), 2024). Practitioner summaries state that this law will take effect on August 26, 2024, and will set clearer NCII protection standards and compliance mechanisms (Kennedy et al., 2024). Theoretically, this model approaches the idea of a central cyber authority and command-and-coordination, whereby the state determines who leads and what the minimum obligations are to prevent coordination failure during a crisis, while still delegating technical implementation to operators (Poetranto et al., 2021; Collett, 2021).

Malaysia's dynamics can also be supported by a relatively well-established incident-reporting ecosystem, as reflected in the response center statistics from Cyber999 and MyCERT. CyberSecurity Malaysia regularly releases quarterly incident summaries that describe the categories and numbers of incidents reported/handled (CyberSecurity Malaysia, Q4 2023). In addition, MyCERT periodically provides classified incident statistics that show the scale and typology of threats (e.g., fraud, malicious code, and intrusion) (MyCERT, 2023–2025). The advantage of this type of data, although it does not always reflect the entire threat ecosystem, is that it can create regulatory feedback: regulators and policymakers can adjust minimum requirements based on the most common attack patterns rather than simply on assumptions. In the literature, feedback based on reporting and data is considered a prerequisite for effective risk regulation because, without it, compliance obligations can easily become mere formalities (Mantelero & Esposito, 2020).

In comparison, Indonesia appears to be moving forward with a strategy of institutional strengthening and operational guidelines while continuing to pursue comprehensive legislation to unify cross-sector cyber resilience regimes. This need is also recognized in regulatory updates that mention plans to strengthen the cybersecurity and cross-sector compliance framework. Malaysia, on the other hand, already has a complex law that explicitly structures the NCII, entity obligations, and service-provider licensing. Within the framework of digital constitutionalism, this difference can be seen as a variation in how countries constitutionalize cyberspace (Mohamed Noor et al., 2025). Indonesia is still in the phase of harmonizing regimes (integrating multiple instruments), while Malaysia prioritizes codifying minimum authorities and obligations for critical sectors. At this point, the question is no longer who is more advanced, but rather what trade-offs are chosen, such as a fragmented model that risks weak coordination but is adaptive to the sectoral context, or a centralized model that risks rigidity but provides certainty in the chain of command and minimum standards (Algamar et al., 2024).

These dynamics must also be read in the context of global trends that reinforce cybersecurity obligations through standardization, certification, and digital product/service security requirements. For example, the European Union is developing a cybersecurity certification framework as an internal market instrument (Ferguson, 2022), strengthening risk management and reporting obligations in NIS2 (Teichmann, 2025), and promoting a product security approach through the Cyber Resilience Act, which tightens security requirements for IoT devices and ecosystems (Shaffique, 2024; Tridgell, 2025). At the conceptual level, the push towards the right to cybersecurity is beginning to emerge, signalling that cybersecurity is increasingly seen as a prerequisite for the effective enjoyment of digital rights (Chiara, 2024). If this trend is projected to Southeast Asia, the Indonesia–Malaysia dynamic can be understood as part of regulatory convergence driven by cross-border risks, digital economic integration, and the need to ensure the reliability of public services.

The empirical urgency is even stronger when linked to the costs and patterns of such attacks. International Business Machines (IBM) reports that the average cost of a data breach in 2024 will reach USD 4.88 million, indicating increasing economic pressure on organizations to invest in prevention, detection, and recovery (International Business Machines, 2024). Meanwhile, Verizon's 2024 DBIR emphasizes ransomware and extortion as dominant patterns in many modern data breaches (Verizon 2024). In other words, regulatory strengthening is not merely a normative response but a rational response to escalating risks and costs. The case of Indonesia's PDN shows how the impact of attacks can quickly shift from private losses to public service disruptions that touch on the legitimacy of state administration (Beaman et al., 2021; Saccone et al., 2025).

Ultimately, the dynamics of cybersecurity development in Indonesia and Malaysia can be formulated as a shift from reactive compliance to resilient governance, with two different institutional paths. Indonesia affirms the role of national authorities and strategies while consolidating disseminated norms, while Malaysia pursues a specific legislative path that structures the NCII, entity obligations, and service provider governance (De Gregorio & Papakonstantinou, 2021; De Gregorio & Radu, 2022). This comparison is important not only to map substantive legal differences but also to examine how institutional design affects effectiveness: whether minimum standards actually reduce systemic risk, how incident reporting shapes the learning system, and how states maintain proportionality so that security does not become a justification for expanding authority that reduces rights.

Reading the dynamics of indonesian cybersecurity regulations through the lens of maqāṣid al-sharīʿa

In the treasury of usul al-fiqh, classical maqāṣid, such as hifẓ al-dīn, al-nafs, al-'aql, al-nasl, and al-māl, were originally developed to organize social and political relations in an analog context. However, recent developments show serious efforts to transform maqāṣid into the realm of the digital economy, artificial intelligence, and data governance as a form of maintaining public interest in the cyber era (Bashori et al., 2024; Chaudhary, 2020). In the context of Indonesia, a Muslim-majority country with a legal system that recognizes religious law as one of its sources of values, maqāṣid can serve a dual function: first, as a substantive source of values for assessing whether cybersecurity regulations truly protect the basic interests of citizens; second, as a normative argument of legitimacy that can strengthen social acceptance of cybersecurity regimes and personal data protection.

Several recent publications on Islam-based digital ethics and artificial intelligence show that maqāṣid can be mapped to specific issues in technology governance, such as privacy, accountability, algorithmic justice, and the prevention of harm (*dar' al-mafsadah*) in cyberspace (Chaudhary, 2020; Ali et al., 2025; Raquib et al., 2022). The trusteeship ethics approach developed by Ali et al. emphasizes that state and corporate actors are mustakhlaf who bear the trust of public data and digital infrastructure, so that failure to protect data, allowing security breaches, or ignoring risks are forms of betrayal of trust (khiyānah) that are normatively reprehensible (Ali et al., 2025). In this context, hifẓ al-māl is no longer limited to physical assets but also includes digital assets, government databases, national data center infrastructure, and public service ecosystems that

depend on state information systems (Bashori et al., 2024; Saputra et al., 2022). The data leak and major ransomware attack on the Temporary National Data Center (PDNS) in June 2024, which affected immigration and other public services, can be normatively interpreted as a failure of hifẓ al-māl and the state's mandate to protect the collective digital wealth of Indonesian citizens.

Maqāṣid also places the protection of life (*hifẓ al-nafs*) and reason (*hifẓ al-'aql*) as the primary objectives. In the context of cybersecurity, this dimension is relevant when cyberattacks target critical infrastructure related to health, transportation, or energy services, which, if disrupted, can threaten life safety, and when regulations are inadequate in dealing with disinformation, information manipulation, and harmful content that impacts public mental health and reasoning (Bou Sleiman & Gerdemann, 2021; He 2022). From the perspective of maqāṣid, this fact shows that the risks to hifẓ al-nafs and hifẓ al-'aql are no longer hypothetical, but actual; cybersecurity policies and the implementation of PDP Law No. 27 of 2022 must not only regulate administrative compliance procedures, but also ensure the continuity of essential public services and information security as part of protecting citizens' lives and minds. In the Sharia-based digital ethics literature, privacy is understood as an extension of the protection of honor (*hifẓ al-'ird*) and, to a certain degree, is attached to hifẓ al-nafs and hifẓ al-'aql, because privacy violations can have an impact on an individual's psychological well-being, social reputation, and economic opportunities (Komaruddin et al., 2023; Saputra et al., 2022).

Contemporary maqāṣid literature focusing on the digital economy emphasizes that the objectives of Sharia are not only to protect individual interests but also the governance structure and sustainability of the digital ecosystem as a space for the production and distribution of benefits (Bashori et al., 2024; Mohamad Puad & Hamdi, 2025). In this framework, cybersecurity is not merely a technical issue but also part of protecting al-naẓm al-ijtimā'ī (social order), which is a prerequisite for achieving distributive justice and digital economic stability in Indonesia. Mohamad Puad and Hamdi, in the context of e-commerce consumer protection in Indonesia, show that the application of maqāṣid requires legal certainty, effective compensation mechanisms, and strict transaction security standards as conditions for the validity of digital business practices. If this logic is applied at the macro level, then the design of national cybersecurity regulations should ideally ensure that businesses and public institutions not only comply with minimum security standards but also actively mitigate risks and provide adequate recovery mechanisms when cyber incidents harm users. The concept of maslahah mursalah here justifies the imposition of new technical obligations and security certification standards for critical infrastructure operators, as long as this is proven to prevent greater damage and does not conflict with qath'i texts (Ferguson, 2022; Bygrave, 2025).

The dimensions of justice (al-'adl) and participation (al-syūrā) also occupy an important place in the maqāṣid reading of cybersecurity governance. Recent studies on AI and data governance highlight a shift towards participatory models that involve affected groups in the regulation and oversight process to correct the power asymmetry between the state, technology corporations, and citizens (Kaminski & Malgieri, 2023; Tridgell, 2025). This perspective aligns with the principle of syūrā, whereby public decision-making on matters affecting citizens' basic rights should ideally not be carried out in a top-down manner without meaningful consultation mechanisms. In the Indonesian context, the formulation of policies related to the PDP Law, the Cyber Security Bill, and the management of PDNS is still relatively elitist, and civil society and the cybersecurity community often participate as technical consultants rather than deliberative partners. From a maqāṣid perspective, this condition can lead to risks of substantive injustice, for example, in the form of overregulation of citizens' digital expression, but under-enforcement of security violations by large actors, which is normatively contrary to the objectives of justice and protection of vulnerable groups.

Normatively, maqāṣid also offers a way to assess the balance between the demands of digital sovereignty and the principles of openness and of global justice. From a maqāṣid perspective, it is legitimate for a country to assert digital sovereignty to protect the public interest (maslahah 'āmmah), but it must not neglect its obligation of international solidarity (ta'āwun) in

dealing with transnational cybercrime, especially when its impact affects the basic rights of citizens in various jurisdictions (Shukri & Azalan, 2023). Therefore, when Indonesia develops a national cybersecurity architecture and local data policy (data localization) for the PDNS, the maqāṣid framework can be used to assess whether the policy actually increases public interest (for example, by strengthening control over strategic data) or increases the risk of incidents due to weak domestic infrastructure capacity and minimal integration with global standards.

Ultimately, the integration of maqāṣid al-syarī'ah in the interpretation of Indonesian cybersecurity regulations shifts the focus of the analysis from mere formal compliance with positive legal norms to a substantive evaluation of the extent to which the legal regime protects and promotes the fundamental objectives of sharia in the digital space. Hifẓ al-dīn demands a cyberspace that is free from hate speech and religious exploitation without becoming a pretext for silencing legitimate criticism; hifẓ al-nafs and al-'aql require the protection of critical infrastructure and public information ecosystems; hifẓ al-nasl demands special protection for children and vulnerable groups in the digital space; and hifẓ al-māl requires comprehensive protection of citizens' digital assets and personal data. Islamic-based digital ethics literature and contemporary cybersecurity law studies provide a conceptual foundation for operationalizing these values into stronger and more equitable regulatory, institutional, and law enforcement practices (Chaudhary, 2020; Ali et al., 2025; Saputra et al., 2022; Komaruddin et al., 2023). Thus, maqāṣid functions not only as symbolic legitimacy but also as a concrete evaluative framework to test whether the regulatory harmonization strategies proposed in the previous section are truly responsive and fair in the face of escalating cyber threats in Indonesia and the region.

Regulatory harmonization strategy: recommendations for responsive and fair adaptation

Strategies to harmonize responsive and fair cybersecurity regulations, particularly in the context of a comparison between Indonesia and Malaysia, must begin with the recognition that regulatory fragmentation is not only a matter of the number of regulations but also relates to the coherence of objectives, distribution of authority, and consistency of compliance standards across the ecosystem (Schmitz-Berndt, 2023; Chiara, 2025). Cybersecurity dynamics show differences in emphasis: Indonesia faces challenges in cross-sectoral coordination and overlapping authorities, while Malaysia is relatively more integrated within a specific institutional architecture, although it still faces risks of sectoral silos and tensions between national security and data protection. Therefore, responsive harmonization does not mean standardizing all instruments, but creating functional equivalence: uniform minimum standards for comparable risks, with proportional room for adaptation to the institutional context and capacity of each jurisdiction (Savaş & Karataş, 2021).

Based on these findings, the recommended strategy includes establishing an adaptive national legal framework that involves various stakeholders in its development; the involvement of BSSN, Kominfo, and other sectors in a legal manner to reduce overlap and governance gaps; designing a national cybersecurity literacy strategy that is integrated into formal curricula, ASN training, and public campaigns; and integrating maqāṣid al-syarī'ah (hifẓ al-nafs, al-'aql, al-māl, al-'irḍ) and the principles of the rule of law (legality, proportionality, due process) into academic texts and the consideration of cybersecurity regulations (Shukri & Azalan, 2023).

In addition to the recommendations we put forward in Table 1, we recommend a strategy for both countries that includes the following: First, the development of a baseline layer of uniform cross-sector cybersecurity obligations in both countries, while still allowing for sectoral delegated regulation. This baseline should include (1) definitions and classifications of compatible critical/essential services, (2) top-level governance obligations, (3) minimum controls, and (4) incident reporting obligations based on significant thresholds. The critical infrastructure protection paper emphasizes the need for dynamic definitions, as criticality changes with digital dependence and supply chain interconnectivity (Markopoulou & Papakonstantinou, 2021; Rogalski, 2021). Thus, the Indonesia–Malaysia baseline should ideally include equivalent supply chain risk management obligations so that transnational companies do not face two conflicting audit regimes.

The next strategy is harmonization through mutual recognition of standards and certification schemes, not merely the harmonization of legal texts. Studies on cyber certification

schemes in internal markets show that certification can serve as a bridge between security interests and legal certainty for the industry, provided that its design avoids duplication, has clear assurance levels, and does not stifle innovation (Ferguson, 2022; Kohler, 2020). In Southeast Asia, the most realistic strategy is to establish a mutual recognition mechanism for ISO/IEC 27001/27002-based standards, digital product security standards, and specific security evaluation criteria for key sectors. However, several studies underscore the importance of distributive justice: the burden of compliance must be proportional to the actor's risk and capacity, especially for MSMEs and certain software developers, to avoid creating market imbalances (Chiara, 2022).

Table 1. Synthesis of regulatory harmonisation strategies based on national contexts and bilateral relations

Strategic Dimension	Recommendations for Indonesia	Bilateral recommendation with Malaysia
Legal Framework	Developing a national cybersecurity framework that integrates sectoral laws (PDP, ITE, telecommunications, finance, health) into a single cross-sector cybersecurity baseline: definition of essential services, minimum requirements (risk management, incident reporting, business continuity), certification/standards, and proportional sanctions. Clarifying the legal division of authority between BSSN, Kominfo, and other sectors to reduce overlap and governance gaps.	Developing an Indonesia–Malaysia MoU and/or bilateral protocol on minimum equivalent baseline: equivalence of critical information infrastructure definitions, categories of incidents that must be reported, and shared principles of due diligence so that cross-border companies face a compatible regime, rather than conflicting ones.
Actor Involvement	Configure a clear multi-actor architecture: BSSN as the lead technical authority, Kominfo as the digital services regulator, PDP authorities as privacy supervisors, and sector regulators as those responsible for sectoral compliance. Require the establishment and accreditation of CSIRT/CIRTs within strategic agencies and sectors, with standardized escalation channels.	Establish a permanent Indonesia–Malaysia Cyber Governance Forum that brings together regulators, national CSIRTs, PDP authorities, and representatives from critical sectors to coordinate policy, conduct tabletop exercises, and share best practices. Develop CSIRT interoperability protocols for cross-border incident handling and threat indicator sharing.
Ethical and Sharia Principles	Integrating maqāṣid al-syarīʿah (hifẓ al-nafs, al-ʿaql, al-māl, al-ʿirḍ) and the principles of the rule of law (legality, proportionality, due process) into academic papers and considerations of cybersecurity regulations. Establishing ethical guardrails on the authority to monitor and use offensive tools (e.g., strict permits, independent audits, public accountability) so that security does not become a pretext for expanding power that infringes on citizens' rights.	Develop a joint Indonesia–Malaysia code of ethics for government cybersecurity practices (e.g., the use of surveillance tools and cross-border data access) that explicitly references the principles of maslahah, prevention of mafsadat, and human rights. Agree on minimum standards of transparency and accountability when major incidents occur that affect citizens of both countries.
Literacy and Participation	Designing a national cybersecurity literacy strategy that is integrated into formal curricula, civil servant training, and public campaigns (focusing on privacy, phishing, device security, and data rights). Opening channels for public and security community participation (consultation on draft legislation, targeted bug bounty programs, public comment on derivative regulations) as a manifestation of the participatory principle and the principle of shura.	Organizing joint literacy programs and awareness campaigns between Indonesia and Malaysia, including bilingual materials, regional incident simulations, and best practice sharing on digital consumer protection. Establishing a regional policy consultation platform involving academics, industry, and civil society from both countries to provide input on regulatory harmonization initiatives.

Source: Results of qualitative data analysis, 2026

The third recommendation, as the core of responsiveness, is to design incident reporting obligations that encourage systemic learning rather than mere administrative compliance. The literature on incident reporting in the Asia-Pacific region emphasizes the wide variation in the definitions of reportable incidents, time frames, recipients of reports, and report content. This variation complicates cross-border coordination and burdens regional companies (Seng, 2023). Therefore, Indonesia–Malaysia harmonization can use a three-tier model: (1) early warning (initial notification), (2) incident notification (initial report with minimum indicators), and (3) final report (root cause analysis and mitigation measures) (Ebert et al., 2025).

The fourth recommendation relates to fairness and constitutional legitimacy: harmonization must control the risk of state overreach and ensure the proportionality of restrictions on rights (Rojszczak, 2021). In cybersecurity, justice regulation focuses on the government's use of surveillance technology and hacking tools. Public procurement analysis shows that this invisible market requires legal protection to prevent security interests from compromising accountability and citizen rights (Anstis 2021). Therefore, fair harmonization requires rule-of-law safeguards: strict licensing mechanisms, independent audits, sunset clauses for extraordinary powers, and minimum transparency that is compatible with national security.

The fifth recommendation is to build institutional interoperability that standardizes norms and how institutions work across borders. At the Indonesia-Malaysia bilateral level, interoperability can be operationalized through (1) standardized information-sharing protocols between CSIRTs/CERTs (Haque & Krishnan, 2021) (2) joint incident response and essential service recovery exercises (Yamin & Katt, 2022) (3) digital forensic assistance request templates (Abraha, 2021) and (4) joint maturity assessment schemes. Responsive harmonization of regulations must include institutional feedback loops, such as periodic evaluations of reporting thresholds, lists of critical sectors, and minimum control standards, so that the system can adapt to evolving threats (Schmitz-Berndt, 2023).

The sixth recommendation is to align approaches to digital sovereignty and cross-border data realistically. Harmonization between Indonesia and Malaysia requires policies that support the digital economy while protecting security and data privacy. This can be achieved by agreeing on data transfer standards that cover basic security, auditing, and cross-border breach notifications, as well as creating dispute resolution and digital evidence exchange mechanisms to reduce procedural barriers. In the context of digital evidence and security, existing privacy and human rights impact assessment methodologies can be integrated as mandatory into high-risk security monitoring systems, making rights protection part of the design rather than just a response to disputes (Georgiadis & Poels, 2022; Mantelero & Esposito, 2021).

The seventh recommendation is to ensure that harmonization does not merely add norms but also improves governance incentives. The literature on cyber norms and the interpretation of international law emphasizes that the boundaries of acceptable behavior are often fluid, and that states often exploit ambiguities for political flexibility (Broeders et al., 2022). In the regional context, a fair response does not mean equalizing all enforcement actions, but equalizing principles: minimum attribution standards for administrative actions with significant impact, accountability for the use of sanctions, and cross-border coordination of responses to attacks targeting essential services. The literature on cyber sanctions at the EU level highlights the dilemma of attribution and state responsibility, as well as the importance of legal certainty to ensure that retaliatory actions do not become arbitrary (Poli & Sommario, 2023). For Indonesia and Malaysia, this can be translated into a joint protocol on incident classification, minimum technical indicators, and escalation thresholds.

Ultimately, responsive and equitable Indonesia–Malaysia harmonization must be understood as a project of "cybersecurity constitutionalization" at the policy level: states recognize security as a prerequisite for rights but also acknowledge that legitimate cybersecurity requires limits, accountability, and protection against excesses. The argument for cybersecurity as a state praxis has even been advanced as a path toward the legal recognition of a new right to cybersecurity (Papakonstantinou, 2022). However, if the right to cybersecurity is read too broadly without the principle of proportionality, it risks becoming a generic justification for state control. Therefore,

the most operational harmonization recommendations are (1) a compatible cross-sector baseline, (2) mutual recognition of standards/certification, (3) learning-oriented incident reporting, (4) rights and oversight controls, and (5) institutional interoperability with adaptive evaluation mechanisms.

Conclusion

The development of cybersecurity and security regulations in Indonesia and Malaysia is moving towards a resilient governance model in the digital economy, but through different institutional and architectural paths. Indonesia tends to rely on institutional strengthening and harmonization of various sectoral regulations, which still leaves issues of fragmentation of authority and standards. Meanwhile, Malaysia pursues a more centralized path through specific legislation with an emphasis on the protection of critical information infrastructure and a clearer chain of command. A comparative analysis shows that these differences affect how each country manages risk, regulates technical obligations, and enforces accountability mechanisms. The proposed harmonization strategy does not aim to standardize legal texts but rather to achieve functional equivalence through cross-sectoral cybersecurity foundations, incident reporting that encourages systemic learning, mutual recognition of standards/certifications, and institutional interoperability. The integration of the maqāṣid al-syarī'ah perspective affirms that cybersecurity must be understood as a tool to protect life, intellect, property, honor, and social order. Therefore, regulatory design and law enforcement practices are tested not only in terms of formal compliance but also in terms of the extent to which they truly protect the public interest and limit the potential for abuse of state authority in the digital economy.

The theoretical implication of this article is to broaden the discussion on digital constitutionalism by emphasizing that it is carried out through the engineering of authority and obligations and accountability mechanisms. In addition, the maqāṣid al-sharī'ah framework can serve as a practical teleological lens for evaluating whether strengthening security truly supports the public interest without neglecting the principles of legality, proportionality, and due process of law. From a practical standpoint, Indonesia needs to strengthen binding minimum standards in various sectors and design an effective incident reporting system to create a learning environment. Meanwhile, Malaysia must ensure that the centralization of authority remains within the limits of regulated discretion and effective oversight so that legal certainty does not justify excessive control. The limitations of this study lie in its doctrinal-comparative nature: although strong in mapping the normative-institutional architecture and trade-off logic, this study has not empirically tested the quality of implementation and is highly sensitive to rapid changes in regulations. Therefore, further research needs to integrate a socio-legal/empirical approach, deepen sectoral analysis, particularly in the field of digital business, and develop maqāṣid-based proportionality metrics to accurately assess when cybersecurity policies are still within the bounds of legitimacy and when they have the potential to become a tool for expanding authority that reduces rights.

References

Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: Mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology, 29*(2), 118–153. https://doi.org/10.1093/ijlit/eaab001

Ahmed, H. (2025). Islamic normative legal theory: Framework and applications. *Journal of Law and Religion, 40*(1), 28–58. https://doi.org/10.1017/jlr.2025.10056

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*, Article 102754. https://doi.org/10.1016/j.cose.2022.102754

Algamar, M. D., Munir, A. B., & Hendro. (2024). Managing Indonesian data breach notification in the financial services sector: A case for one-stop notification model. *Journal of Central Banking Law and Institutions*, *3*(3), 547–584. https://doi.org/10.21098/jcli.v3i3.271

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), Article 120. https://doi.org/10.1007/s13347-025-00922-4

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services*, *68*, Article 103042. https://doi.org/10.1016/j.jretconser.2022.103042

Anstis, S. (2021). Government procurement law and hacking technology: The role of public contracting in regulating an invisible market. *Computer Law & Security Review*, *41*, Article 105536. https://doi.org/10.1016/j.clsr.2021.105536

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/mjsl.vol12no2.647

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, Article 102490. https://doi.org/10.1016/j.cose.2021.102490

Bou Sleiman, M., & Gerdemann, S. (2021). Covid-19: A catalyst for cybercrime? *International Cybersecurity Law Review*, *2*(1), 37–45. https://doi.org/10.1365/s43439-021-00024-9

Broeders, D., de Busser, E., Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: Inching towards lines in the sand? *Journal of Cyber Policy*, *7*(1), 97–135. https://doi.org/10.1080/23738871.2022.2041061

Broeders, D. W. J., & Sukumar, A. M. (2024). Core concerns: The need for a governance framework to protect global Internet infrastructure. *Policy & Internet*, *16*(2), 411–427. https://doi.org/10.1002/poi3.382

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity, 10*(1), tyae017. https://doi.org/10.1093/cybsec/tyae017

Burri, M. (2023). Cross-border data flows and privacy in global trade law: Has trade trumped data protection? *Oxford Review of Economic Policy*, *39*(1), 85–97. https://doi.org/10.1093/oxrep/grac042

Burri, M., Vásquez Callo-Müller, M., & Kugler, K. (2024). The evolution of digital trade law: Insights from TAPED. *World Trade Review*, *23*(2), 190–207. https://doi.org/10.1017/S1474745623000472

Bygrave, L. A. (2025). The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. *Computer Law & Security Review, 56*, 106071. https://doi.org/10.1016/j.clsr.2024.106071

Celeste, E., & Formici, G. (2024). Constitutionalizing mass surveillance in the EU: Civil society demands, judicial activism, and legislative inertia. *German Law Journal*, *25*(3), 427–446. https://doi.org/10.1017/glj.2023.105

Chaudhary, M. Y. (2020). Initial considerations for Islamic digital ethics. *Philosophy & Technology*, *33*(4), 639–657. https://doi.org/10.1007/s13347-020-00418-3

Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, *53*, Article 105961. https://doi.org/10.1016/j.clsr.2024.105961

Chiara, P. G. (2025). Understanding the regulatory approach of the Cyber Resilience Act: Protection of fundamental rights in disguise? *European Journal of Risk Regulation*, *16*(2), 469–484. https://doi.org/10.1017/err.2025.9

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures. *Journal of Cyber Policy, 6*(3), 298–317. https://doi.org/10.1080/23738871.2021.1948582

Cyber Security Act 2024 (Act 854) (Malay.). (2024). https://www.nacsa.gov.my/act854.php [Accessed December 25, 2025]

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001

De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, *30*(1), 68–87. https://doi.org/10.1093/ijlit/eaac004

De Hert, P., & Bouchagiar, G. (2022). Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices? *Information Polity*, *27*(2), 193–217. https://doi.org/10.3233/IP-211525

Ebert, N., Schaltegger, T., Ambuehl, B., Geppert, T., Trammell, A., Knieps, M., & Zimmermann, V. (2025). Learning from safety science: Designing incident reporting systems in cybersecurity. *Journal of Cybersecurity*, *11*(1), Article tyaf019. https://doi.org/10.1093/cybsec/tyaf019

Erdos, D. (2022). Identification in personal data: Authenticating the meaning and reach of another broad concept in EU data protection law. *Computer Law & Security Review*, *46*, Article 105721. https://doi.org/10.1016/j.clsr.2022.105721

Ferguson, D. D. S. (2022). European cybersecurity certification schemes and cybersecurity in the EU internal market. *International Cybersecurity Law Review*, *3*(1), 51–114. https://doi.org/10.1365/s43439-021-00044-5

Galeotti, A., Hoffman, M., & Squintani, F. (2023). Digital privacy. *Management Science*, *69*(6), 3157–3173. https://doi.org/10.1287/mnsc.2022.4513

Georgiadis, G., & Poels, G. (2022a). Towards a privacy impact assessment methodology to support the requirements of the GDPR in a big data analytics context: A systematic literature review. *Computer Law & Security Review*, *44*, Article 105640. https://doi.org/10.1016/j.clsr.2021.105640

Georgiadis, G., & Poels, G. (2022b). Towards a privacy impact assessment methodology to support the requirements of the GDPR in a big data analytics context. *Computer Law & Security Review*, *44*, Article 105640. https://doi.org/10.1016/j.clsr.2021.105640

Haque, M. F., & Krishnan, R. (2021). Toward automated cyber defense with secure sharing of structured cyber threat intelligence. *Information Systems Frontiers, 23*, 883–896. https://doi.org/10.1007/s10796-020-10103-7

He, Z. (2022). When data protection norms meet digital health technology: China's regulatory approaches to health data protection. *Computer Law & Security Review*, *47*, Article 105758. https://doi.org/10.1016/j.clsr.2022.105758

International Business Machines. (2024). *Cost of a data breach report 2024*. https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf [Accessed December 25, 2025]

Kaminski, M. E., & Malgieri, G. (2023). Stakeholder participation in AI and data governance. *Yale Journal on Regulation*, *40*(2), 247–312.

Kennedy, G., Haylock, A. K., & Lai, J. W. J. (2024, December). *Malaysia's new Cyber Security Act 2024 – A summary and brief comparative analysis*. Mayer Brown Insights. https://www.mayerbrown.com/en/insights/publications/2024/12/malaysias-new-

cyber-security-act-2024-a-summary-and-brief-comparative-analysis Accessed December 24, 2025]

Kettemann, M. C., Radu, R., Meyer, T., & Shahin, J. (2021). Normfare: Norm entrepreneurship in internet governance. *Telecommunications Policy*, *45*(6), Article 102148. https://doi.org/10.1016/j.telpol.2021.102148

Kohler, C. (2020). The EU Cybersecurity Act and European standards: An opportunity for global convergence? *International Cybersecurity Law Review, 1*, 15–32. https://doi.org/10.1365/s43439-020-00008-1

Komaruddin, K., Utama, A. S., Sudarmanto, E., & Sugiono, S. (2023). Islamic perspectives on cybersecurity and data privacy: Legal and ethical implications. *West Science Law and Human Rights*, *1*(04), 166–172. https://doi.org/10.58812/wslhr.v1i04.323

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, Article 105809. https://doi.org/10.1016/j.clsr.2023.105809

Mantelero, A., & Esposito, M. (2020). A common EU approach to personal data and cybersecurity regulation: The challenges ahead. *International Journal of Law and Information Technology*, *28*(4), 297–326. https://doi.org/10.1093/ijlit/eaaa021

Mantelero, A., & Esposito, M. S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, *41*, Article 105561. https://doi.org/10.1016/j.clsr.2021.105561

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review*, *41*, Article 105502. https://doi.org/10.1016/j.clsr.2020.105502

Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*. Advance online publication. https://doi.org/10.1007/s11747-022-00845-y

Mead, B., Goepel, J., Miller, J. P., & Flanagan, P. (2021). Defensibility: Changing the way organisations approach cybersecurity and data privacy. *Singapore Academy of Law Journal*, *33*, 127–166.

Mirzaei, P., & De Busser, E. (2024). The New F-word: The case of fragmentation in Dutch cybersecurity governance. *Computer Law & Security Review, 55*, 106032. https://doi.org/10.1016/j.clsr.2024.106032

Mohamad Puad, N. A., & Hamdi, A. S. (2025). Maqasid Shariah and consumer protection in e-commerce: Strengthening legal safeguards in Indonesia's digital economy. *International Journal of Islamic Economics and Finance Research*, *Special Issue 2025*(1), 64–75. https://doi.org/10.53840/ijiefer222

Mohamed Noor, A. F., Moghavvemi, S., & Tajudeen, F. P. (2025). Identifying key factors of cybersecurity readiness in organizations: Insights from Malaysian critical infrastructure. *Computers & Security*, *159*, Article 104674. https://doi.org/10.1016/j.cose.2025.104674

Niebel, C. (2021). The impact of the general data protection regulation on innovation and the global political economy. *Computer Law & Security Review*, *40*, Article 105523. https://doi.org/10.1016/j.clsr.2020.105523

Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards the acknowledgement of a new right to cybersecurity? *Computer Law & Security Review*, *44*, Article 105653. https://doi.org/10.1016/j.clsr.2022.105653

Poetranto, I., Lau, J., & Gold, J. (2021). Look south: Challenges and opportunities for "rules of the road" for cyberspace in ASEAN and the AU. *Journal of Cyber Policy, 6*(3), 318–339. https://doi.org/10.1080/23738871.2021.2011937

Poli, S., & Sommario, E. (2023a). The rationale and the perils of failing to invoke state responsibility for cyber-attacks: The case of the EU cyber sanctions. *German Law Journal*, *24*(3), 522–536. https://doi.org/10.1017/glj.2023.25

Poli, S., & Sommario, E. (2023b). The rationale and the perils of failing to invoke state responsibility for cyber-attacks. *German Law Journal*, *24*, 522–536. https://doi.org/10.1017/glj.2023.25

Raquib, A., Channa, B., Zubair, T., & Qadir, J. (2022). *Islamic virtue-based ethics for artificial intelligence*. Discover Artificial Intelligence, 2, Article 11. https://doi.org/10.1007/s44163-022-00028-2

Redi, A. (2023). Responsive law enforcement in preventing and eradicating illegal mining in Indonesia. *Journal of Law and Sustainable Development*, *11*(8), Article e1436.

Reuters. (2024, June 28). *Indonesia data hit by cyberattack not backed up, officials say*. Reuters. https://economictimes.indiatimes.com/tech/technology/indonesia-data-hit-by-cyberattack-not-backed-up-officials-say/articleshow/111335886.cms [Accessed December 24, 2025]

Rogalski, M. (2021). Security assessment of suppliers of telecommunications infrastructure for the provision of services in 5G technology. *Computer Law & Security Review*, *41*, Article 105556. https://doi.org/10.1016/j.clsr.2021.105556

Rojszczak, M. (2021). The uncertain future of data retention laws in the EU. *Computer Law & Security Review*, *41*, 105572. https://doi.org/10.1016/j.clsr.2021.105572

Ryngaert, C. (2023). Extraterritorial enforcement jurisdiction in cyberspace: Normative shifts. *German Law Journal*, *24*(3), 537–550. https://doi.org/10.1017/glj.2023.24

Saccone, F., Melillo, P., Sgueglia, A., Di Sorbo, A., & Visaggio, C. A. (2025). The ransomware blueprint: Attack patterns and strategic variations across gangs. *Journal of Information Security and Applications*, *95*, Article 104264. https://doi.org/10.1016/j.jisa.2025.104264

Saputra, A. A., Fasa, M. I., & Ambarwati, D. (2022). Islamic-based digital ethics: The phenomenon of online consumer data security. *Share: Jurnal Ekonomi Dan Keuangan Islam*, *11*(1), 105–128. https://doi.org/10.22373/share.v11i1.11167

Sari, A. R. (2023, November 17). *BSSN records 361 million cyber attacks in Indonesia*. Asia Pacific Solidarity Network. https://www.asia-pacific-solidarity.net/index.php/news/2023-11-17/bssn-records-361-million-cyber-attacks-indonesia.html

Savaş, S., & Karataş, S. (2021). Cyber governance studies in ensuring cybersecurity: An overview of cybersecurity governance. *International Cybersecurity Law Review, 2*, 1–22. https://doi.org/10.1365/s43439-021-00045-4

Schmitz-Berndt, S. (2023). What makes incident reporting laws effective? *Journal of Cybersecurity*, *9*(1), Article tyad009. https://doi.org/10.1093/cybsec/tyad009

Seng, N. (2023). Cybersecurity incident reporting laws in the Asia Pacific. *International Cybersecurity Law Review*, *4*(3), 325–346. https://doi.org/10.1365/s43439-023-00088-9

Shaffique, M. R. (2024). Cyber Resilience Act 2022: A silver bullet for cybersecurity of IoT devices or a shot in the dark? *Computer Law & Security Review*, *54*, Article 106009. https://doi.org/10.1016/j.clsr.2024.106009

Shukri, S., & Azalan, M. A. M. (2023). The application of maqasid al-Sharia in multicultural Malaysia: Developing strong institutions for interethnic unity. *Contemporary Islam, 17*, 433–450. https://doi.org/10.1007/s11562-023-00528-7

Sukumar, A., Broeders, D., & Kello, L. (2024). The pervasive informality of the international cybersecurity regime. *Contemporary Security Policy*, *45*(1), 3–23. https://doi.org/10.1080/13523260.2023.2296739

Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 Directive and its role. *International Cybersecurity Law Review*, *6*, 207–220. https://doi.org/10.1365/s43439-025-00154-4

Thomas, C. G. (2021). *Research methodology and scientific writing* (2nd ed.). Springer. https://doi.org/10.1007/978-3-030-64865-7

Tridgell, J. (2025). Open or closing doors? The influence of 'digital sovereignty' in the EU's Cybersecurity Strategy on cybersecurity of open-source software. *Computer Law & Security Review*, 56, 106078. https://doi.org/10.1016/j.clsr.2024.106078

Verizon. (2024). *2024 data breach investigations report*. https://www.verizon.com/business/resources/T735/reports/2024-dbir-data-breach-investigations-report.pdf Accessed December 23, 2025]

Vionis, P., & Kotsilieris, T. (2024). The potential of blockchain technology and smart contracts in the energy sector: A review. *Applied Sciences*, *14*(1), Article 253. https://doi.org/10.3390/app14010253

Yan, J. (2024). Data privacy regulation and cross-border e-commerce. *Empirica*, *51*, 913–927. https://doi.org/10.1007/s10663-024-09624-0

Yamin, M. M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security, 116*, 102635. https://doi.org/10.1016/j.cose.2022.102635

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer. *Computer Law & Security Review*, *41*, Article 105610. https://doi.org/10.1016/j.clsr.2021.105610