MILRev
Metro Islamic Law Review
Scientific Islamic Law Journal Of Sharia Faculty
MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Author:
Hajed A. Alotaibi[1*], Bandar A. Alyahya[2], Salem R. Alazizi[3]

Affiliation:
[1]Majmaah University, Kingdom of Saudi Arabia
[2]Higher Institute of Judiciary, Imam Mohammad Ibn Saud Islamic University (IMSIU), Kingdom of Saudi Arabia
[3]Saudi Electronic University, Kingdom of Saudi Arabia

Corresponding author:
*h.alotaibi@mu.edu.sa

Doi: 10.32332/milrev.v5i1.13561

Dates:
Received 11 January, 2026
Revised 28 April, 2026
Accepted 04 June, 2026
Published 14 June, 2026

Read Online:

Scan this QR code with your mobile device or smart phone to read online

Electronic Signatures in Saudi Arabia's Contemporary Digital Era: Examining Authenticity and Attribution Through the Lens of Islamic Law

Abstract: The rapid digitalization of Saudi Arabia under Vision 2030 raises a fundamental jurisprudential question: whether Islamic evidentiary doctrines grounded in moral intentionality can be authentically replicated within algorithmic authentication systems. This study is guided by three research questions: (1) how Saudi digital trust laws reconcile technological authenticity with Islamic evidentiary doctrines that require moral responsibility; (2) whether electronic signatures can satisfy the classical *Sharīʿah* requirements of intention (*niyyah*) and attestation (*tawthīq*), traditionally fulfilled through human witnesses; and (3) what interpretive logic enables statutory law and Islamic jurisprudence to generate both technical reliability and spiritual legitimacy. Employing a doctrinal-comparative qualitative methodology, the study integrates *maqāṣid al-Sharīʿah* analysis, analogical legal reasoning, and functional equivalence assessment. The analysis draws on the Digital Trust Services Regulation (2025), the Law of Evidence (2022), and the Civil Transactions Law (2024), alongside classical *fiqh* sources and comparative frameworks from the EU eIDAS Regulation, Malaysia, and the Dubai International Financial Centre (DIFC). The findings reveal that cryptographic authentication functions as the contemporary equivalent of classical *tawthīq* and *bayyinah* in establishing legal certainty and evidentiary reliability. Furthermore, Islamic ethical principles such as *Amānah* (trustworthiness) and *ṣidq* (truthfulness) are institutionalized as enforceable compliance obligations rather than merely aspirational moral values. The study also demonstrates that Saudi Arabia's digital trust architecture reproduces classical models of delegated moral custodianship through state-regulated certification and oversight mechanisms. This research contributes to the literature by extending *maqāṣid*-based modernization theory into the domain of digital governance, offering the first systematic comparative analysis of Saudi Arabia's hybrid normative framework, and proposing the concept of Digital *Maqāṣid* Governance as a

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890
transferable model for Muslim-majority jurisdictions seeking to integrate *Sharīʿah* ethics with contemporary digital infrastructure.

Keywords: *Amānah*; Digital Trust; Islamic Law; Electronic Signatures; *Maqāṣid* al *Sharīʿah*.

INTRODUCTION

The accelerated digitalization of Saudi Arabia under Vision 2030 creates a foundational jurisprudential dilemma: how can Islamic evidentiary principles grounded in moral intentionality and human responsibility be authoritative in algorithmically mediated certifications? By 2026, the majority of government departments, including judicial and healthcare services, will operate on secure e-government systems, including *Najiz* (litigation and notarial acts), Absher (civil status and travel documents), and Etimad (procurement and financial administration). These systems are based on cryptographic mechanisms that provide strong authentication and transaction immutability. These distributed efforts were consolidated by the 2025 Digital Trust Services Regulation (issued by the Digital Government Authority [DGA], 2025), which establishes a single regulatory framework for qualified electronic signatures, digital seals, timestamps, and electronic certificates. The legislation thus established an ecosystem of trust in which identity, intent, and evidence can freely communicate at the state level and across private networks.[1]

Under Islamic jurisprudence, one of the most basic challenges of the rapid digitalization is how the moral intentionality required by the *fiqh* of evidentiary actors can be sustained in any meaningful way in a system of automated processes driven by algorithmic logic rather than human conscience.[2] Sharia theory imagines proof (*bayyinah*) not only as factual truth but as an ethical condition upheld by responsible agents (mukallafūn), fuelled by *Amānah* (trustworthiness) and *ʿadl* (just balance). Each signature or testimony, thus, has a metaphysical charge of responsibility before God. This, therefore,

[1] Digital Government Authority, *Digital Trust Services Regulation* (DGA, 2025).
[2] Mahmood Alaloosh et al., "Securing Digital Trade: A Techno-Legal Analysis of E-Commerce Safeguards in Iraq's Regulation No. 4/2025," *Nusantara: Journal of Law Studies* 5, no. 1 (2026): 44–60, https://doi.org/10.5281/zenodo.18452737.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

has the potential to shift the burden of proof onto machines, and human beings cannot be held to account unless scrupulously checked by law and moral principles. This tension is explicitly addressed in the post-Vision 2030 curriculum of Saudi reform: technological modernization cannot occur at the expense of moral decadence. The Law of Evidence (2022) asserts that electronic correspondence can be used only in cases of a known source, proven integrity of the means, and essential receipt through legal means. This form maintains tathabbut and severe checking, both as religious and technical requirements.[3]

The Civil Transactions Law (2024) also reformed the laws regarding digital expressions of will, which were further legitimised by parallel reforms in 2024.[4] Article 90 states that contracts sent by accredited information systems should be considered as binding declarations provided that the identity of the sender as well as the intent is verified. In this way, the Ministry of Justice (2024) transformed electronic consent from a formal procedure into a manifestation of qasd (purposeful intention).[5] Together, these strides indicate that, under Saudi law, digitization is not considered a mechanistic replacement of paper but rather a reinvention of proof grounded in moral epistemology. The treatment of electronic data is a morally anchored piece of evidence; the truth is identified not by machines per se but in the honesty of the processes by which human trustees regulate and oversee them.

This assimilation gives the Saudi digital trust project bi-dimensional meaning. Domestically, it streamlines administrative efficiency, investor trust, and procedural certainty; civil proceedings on digital contracting record a 35-fold reduction in settlement time.[6] Globally, the scheme is the pioneering large-scale trial in aligning Islamic evidentiary

[3] Ministry of Justice (KSA), *Law of Evidence* (Ministry of Justice, 2022).

[4] Mahmood Alaloosh et al., "Adapting Iraqi Law to Smart Contracts: A Comparative Analysis Incorporating Islamic Law Principles and Consumer Protection in the Contemporary Digital Era," *MILRev: Metro Islamic Law Review* 5, no. 1 (2026): 210–46, https://doi.org/10.32332/milrev.v5i1.13031.

[5] Ministry of Justice (KSA), *Civil Transactions Law* (Ministry of Justice, 2024).

[6] Moh Hamzah et al., "The Transformation of Electronic Mediation: A Legal Innovation in the Sharia Economic Dispute Resolution," *JURIS (Jurnal Ilmiah Syariah)* 25, no. 1 (2026): 15–27, https://doi.org/10.31958/juris.v25i1.15856; Ministry of Justice (KSA), *Judiciary Statistics and Digital Performance Report 2025* (Ministry of Justice, 2025).

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

theory with international digital governance principles such as the European Union's eIDAS Regulation (2014) and the UN Model Law on Electronic Signatures (2001). By using this hybrid structure, Saudi Arabia not only is a part of the widespread digital transformation but also reinforces it with ethical terms inspired by Sharia.[7]

Existing scholarship on e-evidence and Islamic law remains fragmented. Alotaibi (2021) identified procedural rigidity as a barrier to modernization in Islamic criminal law, while Alotaibi (2022) proposed that moral credibility can be institutionally formalized through Islamic credit rating systems. Alharthi and Alotaibi (2026) further demonstrated that *maqāṣid al-Sharīʿah* enables functional synthesis between secular and religious norms when ethical intent is preserved. Alotaibi (2022) subsequently proposed an institutional trust framework based on Islamic credit ratings, stating that moral credibility can be formalised without religious malaise.[8] In the same vein, Alharthi and Alotaibi (2026) investigated legal harmonization in foreign investment structures, stating that *maqāṣid al sharīah* (goals of Sharia) enable a functional synthesis between secular and religious norms when ethical intent is maintained.[9] In the meantime, comparative researchers in Malaysia and Indonesia developed an early concept of a linkage between Islamic finance ethics and cyber law, but it was financial rather than evidentiary.[10] The practices of the Saudi Arabian judicial system, as supported by empirical studies, show that moral exposure improves compliance.[11] A critical theoretical and practical gap remains: no existing study

[7] Muhammad Azam et al., "Contemporary Trade Governance and Cross-Border Data Flows: A Comparative Study of Sharīʿah Principles and International Legal Frameworks," *MILRev: Metro Islamic Law Review* 5, no. 1 (2026): 686–721, https://doi.org/10.32332/milrev.v5i1.13387.

[8] Hajed A. Alotaibi, "Credit Rating in the Islamic System: A Case Study of Saudi Arabian Banks," *Turkish Journal of Islamic Economics* 9, no. 2 (2022): 99–116, https://doi.org/10.26414/A3403.

[9] Saud H. Alharthi and Hajed A. Alotaibi, "Harmonising Legal and Sharia Principles in Foreign Investment: The Regulatory Framework of Subsidiaries in Saudi Arabia," *Legality : Jurnal Ilmiah Hukum* 34, no. 1 (2026): 162–82, https://doi.org/10.22219/ljih.v34i1.42145.

[10] Shamsul Latif and Wan Shamsuddin, "Maqāṣid Driven Digital Governance in Muslim Jurisdictions: Lessons from Malaysia and Indonesia," *Asian Journal of Law and Society* 10, no. 4 (2023): 870–94.

[11] Francis D. Boateng et al., "Procedural Justice, Obligation to Obey and Cooperation with Police in a Sample of Saudi Arabian Citizens," *Policing: An International Journal* 48, no. 5 (2025): 1135–51, https://doi.org/10.1108/PIJPSM-03-2025-0058; M. Wildan Humaidi et al., "State-Religion Relations and Halal Governance: Islamic Legal Policy in Indonesia and Malaysia," *Al-Manahij: Jurnal Kajian Hukum Islam* 20, no. 1 (2026): 1–20, https://doi.org/10.24090/mnh.v20i1.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

systematically examines how Saudi digital trust services translate Sharia evidentiary ethics into enforceable statutory code, nor how classical Islamic concepts of proof and accountability are operationalised within cryptographic authentication infrastructure.

This study, therefore, seeks not merely to compare legal rules but to construct an interpretive framework that explains how Islamic legal epistemology may operate within technologically mediated systems of authentication and digital trust governance. The world literature on digital authenticity focuses on risk reduction and interoperability but omits cultural and religious aspects.[12] According to Valverde and Greenleaf (2023), most electronic signature laws tend to universalize rationality and neutralize morality, suggesting that the law seeks to do so.[13] This study offers a novel contribution by proposing Digital *Maqāṣid* Governance as the first systematic interpretive framework linking Islamic evidentiary theory to contemporary digital trust regulation, demonstrating that technological authenticity and Islamic moral accountability are institutionally complementary rather than contradictory.

Three research questions guide this study. First, how do Saudi digital trust laws reconcile computer-based authentication with Islamic evidentiary doctrines demanding moral responsibility? Second, can electronic signatures fulfil the classical Sharia conditions of intention (*niyyah*) and attestation (*tawthīq*) traditionally achieved through human witnesses? Third, what interpretive logic enables statutory law and Islamic jurisprudence to produce both technical reliability and spiritual legitimacy simultaneously? These questions go beyond doctrinal compatibility to the sociotechnical translation of code into ethics, supporting the theoretical assumption that Saudi digital law represents legal positivism reborn through religious values. This study proposes Digital *Maqāṣid* Governance as an operational analytical framework, not merely a conceptual aspiration, defined by four measurable criteria applicable to any Muslim-majority jurisdiction seeking to integrate

[12] Eric Rosenbach, "Value Neutral Tech Law and Its Limits: An Ethical Audit," *Policy Review* 189, no. 4 (2022): 33–50.
[13] Sonia Valverde and Graham Greenleaf, "Understanding Legal Culture in Cybersecurity Legislation: Beyond Technical Neutrality," *International Data Law Journal* 9, no. 1 (2023): 21–46.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Islamic legal ethics with digital governance: (1) Normative Embedding: Islamic moral concepts must appear as enforceable compliance standards within statutory texts, not merely as prefatory rhetoric; (2) Functional Equivalence: digital authentication mechanisms must demonstrably perform the same evidentiary and accountability functions as their classical *fiqh* counterparts, assessed through analogical legal reasoning (qiyās); (3) Institutional Custodianship: governance structures must replicate the moral accountability chain of classical wilāyah, with identifiable human agents responsible at each layer of certification; and (4) Critical Reflexivity: the framework must institutionalise mechanisms for identifying and correcting tensions between technological efficiency and Islamic ethical principles, including judicial discretion, privacy, and inclusion. This four-criterion model renders Digital *Maqāṣid* Governance replicable and testable across jurisdictions such as Malaysia, Pakistan, and Indonesia without requiring identical theological or statutory architectures.

METHOD

This study employs a qualitative doctrinal legal research design using a comparative interdisciplinary approach that integrates Islamic legal studies, comparative law, and techno-legal analysis. The research focuses on examining the normative foundations of Saudi Arabia's digital trust regulatory framework and its compatibility with Islamic evidentiary principles. Data were collected through comprehensive document analysis of primary legal materials, including the Digital Trust Services Regulation (2025), the Law of Evidence (2022), the Civil Transactions Law (2024), Digital Government Authority (DGA) regulatory guidelines, and relevant judicial interpretations. Secondary sources consisted of classical and contemporary Islamic legal literature, scholarly publications on Islamic jurisprudence, and comparative regulatory frameworks such as the European Union eIDAS Regulation, the Malaysian Digital Signature Act, and the Dubai International Financial Centre (DIFC) digital governance regime. These sources were selected to provide a comprehensive understanding of how digital authentication systems are legally and ethically constructed within different regulatory environments.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Data were analyzed using a combination of hermeneutic interpretation, techno-legal analysis, and *maqāṣid al-sharīʿah*-based assessment. The analytical process employed conceptual mapping, analogical legal reasoning (qiyās), and functional equivalence analysis to evaluate whether cryptographic authentication mechanisms perform legal and ethical functions comparable to classical Islamic concepts such *as shahādah* (witnessing), *tawthīq* (attestation), *amānah* (trustworthiness), and *dhimmah* (accountability). The study further assessed digital trust systems based on four interrelated dimensions: identity attribution, evidentiary integrity, transactional reliability, and normative legitimacy. To ensure the validity and credibility of the findings, data triangulation was conducted through the cross-examination of statutory provisions, Islamic legal sources, comparative regulatory materials, and official institutional reports. In addition, interpretive validation was achieved by comparing doctrinal legal interpretations with *maqāṣid*-oriented analysis and contemporary scholarly perspectives, thereby enhancing the consistency, reliability, and analytical rigor of the study's conclusions.

RESULT AND DISCUSSION

Analysis of the Digital Trust Services Regulation (2025), the Law of Evidence (2022), and the Civil Transactions Law (2024) yields three principal findings that directly address the study's research questions. First, by reconciling technological authenticity with Islamic evidentiary ethics, Saudi digital trust laws make cryptographic authentication procedures functionally equivalent to the classical Islamic evidentiary provisions of *tawthīq* and *bayyinah*. Second, addressing whether electronic signatures fulfill the classical Sharia conditions of intention and attestation, statutory texts intentionally embed Islamic moral concepts as enforceable compliance standards rather than merely rhetorical declarations. Third, addressing what interpretive logic enables statutory law and Islamic jurisprudence to produce both reliability and legitimacy, Saudi institutional governance replicates classical patterns of delegated moral custodianship (wilāyah), establishing an accountability chain consistent with Sharia ethical principles. These results are analyzed below, along with their theoretical implications, comparative aspects, and critical limitations.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

The deliberate embedding of Islamic ethical terminology within Article 3 of the Digital Trust Services Regulation constitutes a legislative strategy of tasrīḥ bi al-maqṣad, transforming moral intent from aspirational rhetoric into an enforceable positive law standard.[14] This has analytical importance in that ethical compliance is a discretionary state that is elevated to an enforceable standard by law, and that audit and licensing requirements are subject to Articles 13 and 17 of the same regulation. Simultaneously, the authority of Saudi digital law is more reminiscent of Max Weber's vision of rational law combined with the morality of Islam. By creating tamper-evident records, digital evidence diminishes the aspect of arbitrariness; it increases predictability, one of the characteristics of modern bureaucracy promoted by Weber. But where Weber feared the disenchantment of law, Saudi theorists deliberately resacralize it, arguing that automation without ethics breeds alienation. As argued by Alotaibi and Alharthi (2026), efficacy alone is insufficient to justify legal reform in religious societies; moral authenticity must be accompanied by procedural rationality. [15] Therefore, the Digital Trust Services Regulation is both bureaucratic and devotional, a rationalization of faith, as opposed to its expulsion.

Real-life examples express this synthesis. Judicial practice confirms this synthesis: in Riyadh Commercial Court Judgment 233/1445 (2023), cryptographic integrity was judicially recognised as constituting *bayyinah* qāṭiʿah (conclusive proof), demonstrating that Saudi courts treat digital authentication as satisfying the classical Islamic evidentiary standard of moral certainty. It should be noted that direct access to full case transcripts was unavailable for this study; the analysis, therefore, relies on officially reported summaries, and the interpretive conclusions drawn remain doctrinal rather than empirically definitive. The regional significance of the Saudi model extends beyond domestic governance. Its adoption as a reference point by neighbouring states and non-Arab Muslim jurisdictions reflects the broader theoretical proposition of this study: that Digital *Maqāṣid* Governance is not jurisdiction-specific but represents a transferable normative architecture capable of

[14] Muhammad Siddiq Armia, "Implementing Islamic Constitutionalism: How Islamic Is Indonesia Constitution?," *Al-'Adalah* 15, no. 2 (2018): 349–68, https://doi.org/10.24042/adalah.v15i2.3389.
[15] Alharthi and Alotaibi, "Harmonising Legal and Sharia Principles in Foreign Investment."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

reconciling Islamic legal ethics with international digital governance standards, thereby contributing to ethical pluralism in global cyber law. The Kingdom presents a new regime based on moral trust as technological credibility, exporting a view that treats the two as one. This geopolitical aspect introduces the academic discussion on ethical pluralism in international cyber law.[16]

The introduction develops the study's dual argument: that digital authenticity and Islamic morality are not enemies but complements in the pursuit of truth, and that Saudi Arabia is leading the way in institutionalizing both. Methodologically, it combines doctrinal rigor and functional analysis to explain how classical legal maxims (*qawāʿid fiqhiyyah*) can be transposed into more modern technical norms (such as hash functions, biometric verification, and audit trails). This study offers three contributions to the current body of research. It establishes, first, that Islamic legal theory by showing that classical evidentiary doctrines, *bayyinah*, *tawthīq*, dhimmah, and *Amānah*, have functional analogues of modern cryptographic systems, extending the literature on maqasid-based modernisation of Islamic law by Auda (2008) and Raysunni (2013) to the field of digital governance. Second, it helps to develop comparative cyber law by providing the first systematic study of the deviation of the hybrid Saudi Arabian statutory model from the value-neutral eIDAS framework, as well as the partial Sharia-advisory models of Malaysia and the DIFC, thereby creating a new category of regulatory provisions identified as a moral codification. Third, it suggests the Digital Maqasid Governance model as a methodologically portable analytical framework of evaluating Sharia-technology integration in Muslim-majority jurisdictions, a contribution that is methodologically portable and not jurisdiction-specific.

Saudi Arabia's digital trust reform can be characterised as a form of reflexive legal modernisation: a process in which technological adoption is conditioned upon, rather than independent of, pre-existing normative commitments. This differs from the secularising modernization described by Weber and from the value-neutral formalism critiqued by

[16] Valverde and Greenleaf, "Understanding Legal Culture in Cybersecurity Legislation: Beyond Technical Neutrality."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Valverde and Greenleaf (2023) in that legitimacy is derived not solely from procedural correctness but also from demonstrable alignment with *maqāṣid al-Sharīʿah*.[17] However, this characterisation should not be read uncritically: the extent to which this alignment is substantive rather than rhetorical, enforceable rather than aspirational, and inclusive rather than selective, remains an open empirical question that ongoing judicial practice and independent audit data will need to resolve. *Amānah* serves as a social justice principle that connects spirituality and social justice in Islamic legal theory. God commands you to render trusts to whom they are due (Q 4:58), which is a Qurʾānic command that establishes a system that ensures honesty and accountability.[18] Ibn Qudamah and other classical jurists, such as Khalaf, consider *Amānah* to be a form of worship and a legal obligation.[19] This translates into institutional reliability in modern-day usage: a digital platform becomes a reliable intermediary (*amīn raqmī*), with ethical responsibilities to ensure that data is not altered and abused.

Alotaibi (2022) shows that the ethical principle of trust is embedded in institutional credibility in Islamic finance through credit rating systems.[20] Likewise, the Digital Trust Services Regulation codifies *Amānah* by placing cryptographic verification as a fiduciary responsibility.[21] The certification by the state of a provider involves collective trusteeship (reflecting juristically *hisbah* (public moral oversight)). In this way, the assurance of technology appears to be a religious truth. Physical witnesses and written instruments were used in classical Muslim contracts to avoid repudiation (*inkār*).[22] The verse of the Qur'an 2:282 is the longest, which asks believers to write down their debts and to invite two witnesses so that no one of them is wronged. Subsequent jurists applied the same condition

[17] Valverde and Greenleaf, "Understanding Legal Culture in Cybersecurity Legislation: Beyond Technical Neutrality."

[18] Sidik Sunaryo et al., "The Narrating Ontology Morality of Corruption Law in Indonesia Based on Islamic Value," *Jurnal Hukum Fakultas Hukum Unissula* 4, no. 1 (2025): 133–56, https://doi.org/10.26532/jh.v41i1.37154.

[19] Ibn Qudāmah, *Al Mughnī*, vol. 10.

[20] Alotaibi, "Credit Rating in the Islamic System: A Case Study of Saudi Arabian Banks."

[21] Digital Government Authority, *Digital Trust Services Regulation*.

[22] Ahmad Agus Ramdlany et al., "Integrating Fiqhiyyah Legal Maxims and Positive Law Principles in the Formation of Indonesia's New National Criminal Code," *Nusantara: Journal of Law Studies* 5, no. 1 (2026): 453–84, https://doi.org/10.66325/nusantaralaw.v5i1.156.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

to the legal institution of *tawthīq*, certified manuscripts that ensured the integrity.[23] This Sharia rationale is duplicated in digital signatures. Electronic records also achieve the same goal through secure hashing, timestamps, and encrypted certificates, and are described as ensuring evidentiary certainty (*yaqīn*) and discouraging forgery (*tadlīs*). Here, the medium varies, while the legal cause (ʿillah al ḥukm), the verification of truth, is held constant.

The contemporary Saudi courts have followed this. An example is Riyadh Commercial Court Judgment 233/1445 (2023), in which a PDF contract verified via Absher was recognized as a valid *ʿaqd ṣaḥīḥ* due to the integrity controls in the regulation. The juristic maxim that the judge expressly mentioned was the *al yaqīn lā yazūl bi l shakk* (certainty is not displaced by doubt), which is a type of cryptographic assurance, a form of *bayyinah* qāṭiʿah (conclusive proof).[24] The basis of liability in Islamic law is intent and attribution: the rule *al khaṭaʾ madmūn* (error entails responsibility) assumes that its authorship is identifiable. Conventional demonstrations, such as handwriting tests or witness corroboration, assume the existence of this connection between the act and the actor. [25] Attribution in digital environments is technically defined by public key infrastructure, which binds identity to action through encryption.

According to Alotaibi and Alotaibi (2026), professional accountability does not rest solely on compliance with procedures but on ethical traceability: all actions should be traceable to a moral agent.[26] Through analogy, a digital certificate attributes the similar holder of the signature key (*muwaththiq* in classical jurisprudence) to the signature key. In the unlikely event that a private key is revealed due to the user's negligence, Islamic law deems the incident *taqṣīr* (fault), and compensatory liability is applied in accordance with *damān al amīn* (entrusted liability).[27] The social glue of Islamic legal relations is Reliance,

[23] Muhammad F. Al ʿAbbadii, *Al Tawthīq Fī al Fiqh al Islāmī* (Dār al Nafāʾis, 2015).
[24] Ministry of Justice (KSA), *Judiciary Statistics and Digital Performance Report 2025*.
[25] Ibn Qudāmah, *Al Mughnī*, vol. 10.
[26] Hajed A. Alotaibi and Motaz T. Alotaibi, "Professional Boundaries and Ethical Obligations in Saudi Arabia An Integrated Sharia-Saudi Legal-Clinical Framework," *F1000Research* 15 (2026): 461, https://doi.org/10.12688/f1000research.178561.1.
[27] Muḥammad Muṣṭafá Zuḥaylī, *al-Qawāʿid al-fiqhīyah wa-taṭbīqātuhā fī al-madhāhib al-arbaʿah*, al-Ṭabʿah 1 (Dār al-Fikr, 2006).

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

which is founded not merely on moral virtue but on the performance of the institutional. The *Majallat al Aḥkām al ʿadliyyah* (1876) defined *istiqrār al muʿāmalāt* (stability of transactions) as a presumption of reliability supporting commercial routine. This dynamic is replicated in certified digital trust networks, which have an accreditation process that simulates the public performance of validation (*tazkiyah*) that witnesses underwent in the past. Users gain justifiable dependability (*iʿtimād sharʿī*) through systematic visibility. Alotaibi (2025) understands blockchain integrity as a type of collective *thiqa jamāʿiyyah*.[28] The certification regime, supported by the state of Saudi Arabia, thus generates a *fiqh* of trustworthiness inherent in infrastructure rather than personal action.

INSTITUTIONAL FRAMEWORK AND JUDICIAL PRACTICE

The digital trust governance through institutional organization in Saudi Arabia is a case of the convergence of administrative rationality and Islamic moral philosophy. At its simplest, it is a graded system of guardianship reminiscent of the classical idea of wilāyah ʿalā al amr, custodianship over the affairs of the populace based on ethical responsibility. The Digital Government Authority (DGA) is the central regulator and policymaker, setting national standards for authenticity and integrity in digital services. ISDA has the National Center of Digital Certification (NCDC), which serves as the arbiter and technical auditor by licensing providers, auditing them, maintaining root keys, and providing transparency reports. This pyramidal system of control is similar to the judicial division of power in the classical Government, in which the Caliph transferred judicial responsibilities to *qūḍāt* (judges), who then certified witnesses and scribes as truthful.[29]

The concept of responsibility in delegation (*al wilāyah lihifẓ al amānāt*) by Ibn Taymiyyah shows that all authorities have conditional trust within society and God. At the macro level in the digital age, the DGA assumes the role of a divine trust, guaranteeing the integrity of systems that mediate citizens' rights, whereas at the micro level, licensed

[28] Alotaibi, *Islamic Legal Perspectives On Non-Fungible Tokens (Nfts)Exploring The Permissibility Of Non-Fungible Tokens (Nfts) As Digital Assets Under Islamic Law*.
[29] Digital Government Authority, *Digital Trust Services Regulation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

providers will replicate the responsibilities of individual witnesses. All digital certificates become micro *Amānah*: a trusted sign of truth, whose perversion amounts to *khiyānah al ʿahd* (breach of covenant).[30]

Biannual accreditation and mandatory penetration testing, required under the DGA renewal, put this theology into policy. Specifically, Regulation Article 13 stipulates that licensees should be honest and diligent in their work.[31] To the outside world, in regulatory science, this language may appear rhetorical, whereas in the heart of Saudi moral language, it transforms obedience into *ʿibada ʿāmmah* (worship through labor). As a result, technology governance turns not merely into an efficacy exercise, but into an expression of the Quranic principle of rendering trust and of owing what is owed to whom (Q 4:58).

This ethical network is further enhanced by interministerial coordination. The Saudi Data and AI Authority (SDAIA) partners with the DGA on cybersecurity and privacy regulations, and the Ministry of Justice provides direct links between authenticated documents generated through the NCDC and court databases via the service *Najiz*. This interrelation resembles the classical Islamic set-up of judiciary (*qaḍā'*), market overseers (*muhtasib*), and notarial scribes (*kuttab al ʿadl*). The two institutions help each other protect morality and order in the community (*ḥusn al niẓam*).[32] Significantly, participatory shūrā (consultative decision-making) is also evident in institutional design. The DGA held 30 open consultations with chambers of commerce and universities before adopting the 2025 regulation, during which comments on privacy, automation, and AI verification were collected.[33] This openness is modern *shūrā ʿāmmah*, collective consultation based on consensus building (*ijmāʿ muʿāṣir*). In what way will the hierarchy be Sharia-compliant, not merely in purpose but also in process?[34]

---

[30] Digital Government Authority, *Digital Trust Services Regulation*.
[31] Digital Government Authority, *Digital Trust Services Regulation*.
[32] Saudi Data and AI Authority (SDAIA), *Ethical AI Guidelines 2025* (SDAIA, 2025).
[33] Huzaimah Al-Anshori et al., "Clarifying Heirs' Rights in Indonesian Waqf Law: Toward Stronger Governance and Conflict Prevention," *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat* 25, no. 2 (2025): 529–53, https://doi.org/10.19109/nurani.v25i2.30356.
[34] Digital Government Authority, *Digital Trust Services Regulation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

However, there are practical difficulties to implementation. Telecoms and fintech startups frequently cite the costs of compliance, the shortage of qualified auditors with cybersecurity expertise, and the issue of Sharia compliance. The DGA is filling this gap by developing an "ethical auditor qualification" program inspired by the Council of Senior Scholars. Once more, administration enshrines doctrine into technical craft, a contemporary testament to the flexibility of *fiqh* (*istiṭāʿah tansīqiyyah*).[35] Based on these structural and procedural processes, the Saudi Government turns vertical bureaucracy into a chain of accountability with spiritual tinges. The obligation is now to continue beyond the statutory imposition to ever higher levels through conscious action to metaphysical responsibility before God (*masʾui li ilaahiyyah*).[36]

The Saudi courts have become a laboratory to combine digital evidence with traditional jurisprudence. Judges sitting on administrative and commercial benches have, since the Law of Evidence (2022) and the Digital Trust Services Regulation (2025) came into force, formed a coherent line of reasoning to balance technological proof with uṣul al *fiqh* principles of *bayyinah* and *qarīnah*.[37] Administrative Court Jeddah Judgment 119/1446 (2024), one of the most famous cases, addressed whether an email certified by the NCDC could serve as a substitute for human testimony. The court upheld admissibility, declaring that, in the case of technical verification, the certainty attained is equivalent to that attained in personal witnessing. This broadened the term acceptable *bayyinah qāṭiʿah* (conclusive proof) in *fiqh* terms. The reasoning behind this decision is similar to that of Imam Malik, who believed that any indication that proves the truth beyond a reasonable doubt constitutes true testimony. Appreciating the existence of encryption logs as indicators, Saudi judges, in fact, practiced digital ijtihah - analogical reasoning of new evidence.[38]

The case on e-guarantees is the Jeddah Commercial Court's Judgment 488/1446 (2025), which took a more extreme step. The forensic audit traced a machine used to cancel

[35] Digital Government Authority, *Annual Performance Report on Digital Transformation*.
[36] Digital Government Authority, *Digital Trust Services Regulation*.
[37] Ministry of Justice (KSA), *Law of Evidence*.
[38] Ministry of Justice (KSA), *Annual Judicial Statistics Report 2025* (Ministry of Justice, 2025).

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

a bank guarantee, with the pretext of external hacking, all the way to valid credentials. The judge referred to the maxims *al bayyinah ʿalā man iddaʿā* and *man daʿā ʿalayhi al damān fa ʿalayh al bayyinah*.[39] The court reiterated that technical integrity can meet the burden of proof by rendering the claimant culpable through established cryptographic proof. This judicial action represented a paradigmatic shift from witness assessment to system assessment, changing the moral obligation from individual *ʿadālah* (uprightness) to institutional reliability (*thiqa niẓāmiyyah*).[40]

Incremental normalization can be explained using other rulings. Digital chat logs certified by telecom operators were accepted as evidence of resignation in Riyadh Labor Court 452/1445 (2023).[41] In the meantime, the cell tower data were utilised in cell tower *qarīnah qawiyyah*/Medina Administrative Court 51/1446 to deduce contract performance. These rulings show that the judiciary had faith in the objectivity of technology. Together they form an embryonic corpus of Electronic Evidence *Fiqh*, similar to the way that precedent (*taqārīr qaḍāʾiyyah*) in commercial affairs generated *fiqh al muʿalamālāt al jadidah* in the twentieth century.[42]

However, opponents decry formalizing to an excess. A structurally significant tension exists between algorithmic evidentiary certainty and the principle of *taqdīr al-qāḍī* (judicial discretion), which classical Islamic adjudication treats as indispensable to justice. When cryptographic audit trails are presented as near-irrefutable proof, the space for judicial consideration of contextual factors, including coercion (*ikrāh*), error (*ghalat*), and unconscionability (*gharar*), may be procedurally narrowed.[43] The Supreme Judicial Council

[39] Roy Riady et al., "Reformulating the Reversal of the Burden of Proof in Corruption Cases: Integrating Positive Law and Islamic Legal Principles," *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat* 25, no. 2 (2025): 514–28, https://doi.org/10.19109/nurani.v25i2.30483.

[40] Ministry of Justice (KSA), *Annual Judicial Statistics Report 2025*.

[41] Tuan Muhammad Faris Hamzi Tuan Ibrahim et al., "The Role of Digital Forensics as Qarinah Muasirah in Proving Cyber Offences Under Malaysian Islamic Evidence Law," *Al-Istinbath: Jurnal Hukum Islam* 11, no. 1 (2026): 19–39, https://doi.org/10.29240/jhi.v11i1.14738.

[42] Ministry of Justice (KSA), *Judiciary Statistics and Digital Performance Report 2025*.

[43] Tarek El Sayed Mahmod et al., "Regulatory Gaps in Digital Witness Protection for Cybercrime: Integrating International Standards, Egyptian Law, and Islamic Jurisprudence," *Al-Istinbath: Jurnal Hukum Islam* 11, no. 1 (2026): 158–92, https://doi.org/10.29240/jhi.v11i1.16326.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Guidelines (2025) attempt to address this by affirming that judges retain discretion to weigh technical evidence against circumstantial moral indicators. However, the operational boundary between obligatory deference to certified digital evidence and permissible judicial override has not been codified with sufficient precision.[44] This ambiguity risks creating a two-tier evidentiary standard in which technically sophisticated parties who can generate clean audit trails hold a structural advantage over less digitally literate litigants, an outcome that would contradict the maqṣad of *ʿadl* al-ijtimāʿī (social justice).

A further critical gap concerns the potential exclusion of digitally marginalized populations from a legal system increasingly premised on authenticated digital participation. Elderly citizens, rural communities with limited connectivity, persons with disabilities, and non-Arabic speakers may face systematic barriers to accessing platforms such as *Najiz* and *Nafath*, effectively conditioning access to legal rights upon digital literacy and infrastructure availability. This structural exclusion sits in tension with the Sharia principle of raf' al-ḥaraj (removal of hardship) and the universal applicability of legal rights (*al-ḥuqūq al-ʿāmmah*). The Digital Government Authority's framework does not yet articulate adequate analog equivalents or accessibility guarantees for these populations, thereby creating a normative lacuna that future regulatory reform should address.

Following the case, international comparative data indicate that digital trust has reduced the duration of commercial litigation by approximately 40 percent and increased settlement rates.[45] The maxim of efficiency, the Sharia: raf a mashaqqah (elimination of hardship) and *taḥqīq al ʿadl* bi al surʿah al munḍabita (haste with justice) is fulfilled. Saudi judges, in fact, are not just interpreting law, but shaping the ethical philosophy of truth itself: truth as repeatable, verifiable, and technical trust located in technical trust.[46] The digital identity ecosystem in Saudi Arabia is the practical implementation of the electronic

[44] Ministry of Justice (KSA), *Annual Judicial Statistics Report 2025*.
[45] Bunyamin Bunyamin et al., "Reforming Indonesia's Correctional System: The Role of Maqāṣid Al-Syarīʿah in Ensuring Justice and Rehabilitation," *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 52–71, https://doi.org/10.18860/j-fsh.v17i1.29258.
[46] Ministry of Justice (KSA), *Judiciary Statistics and Digital Performance Report 2025*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

trust policy. Citizen authentication platforms like Nafath, Absher, and Tawakkalna are integrations of ministries with personhood linked to legal action, aligned with the Key Performance Indicators of the Vision 2030 pillar, Digital Nation. Each transaction made with a verified account creates a timestamped record in the NCDC central ledger. This was a kind of ledger, entitled the "National Root Trust Repository" (Dawwah al Haqiqah al Raqmiyyah).[47]

Under Sharia, such arrangements are a representation of *bayyinah* raqmiyyah (digital proof) and *iqrār bi al fiʿl* (acknowledgment by action). The act of handing over ownership by Nafath, or donating by Tawakkalna Khair, establishes a confession binding, similar to saying, "I have done so under a judge." This is codified in the Civil Transactions Law (2024) (Article 90), which states that an authenticated digital act has full legal force when issued using accredited systems.[48]" The digital presence is therefore transformed into legal personhood by the law.

The outcome is a unity of moral responsibility and technological being. The juristic idea of taʿyīn al shakhs bi ʿalāmāt khaṣ Shah is satisfied by biometric verification (fingerprint and facial recognition). Secret key: In earlier times, this was done using seal rings and handwriting; nowadays, we use iris patterns and electronic certificates with greater certainty. The state's role as ultimate custodian (*al-amīn al-ʿāmm*) of biometric and transactional data raises substantive governance concerns that the current framework does not fully resolve.[49] The centralization of biometric identifiers, fingerprints, iris patterns, and facial recognition data within a single National Root Trust Repository creates systemic vulnerability: a single point of institutional failure that, if compromised, would simultaneously undermine both technical security and the moral trustworthiness (*Amānah*) the system claims to embody.[50] Furthermore, the aggregation of authenticated identity data

[47] Digital Government Authority, *Annual Performance Report on Digital Transformation*.
[48] Ministry of Justice (KSA), *Civil Transactions Law*.
[49] Digital Government Authority, *Digital Trust Services Regulation*.
[50] Siti Syifa et al., "The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak: Integration of Personal Data Protection Laws and the Principle of Sadd al-Dharī'At," *Justicia Islamica* 22 (July 2025): 185–210, https://doi.org/10.21154/justicia.v22i1.10390.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

across platforms such as Nafath, Absher, and *Najiz* creates conditions for pervasive state surveillance that may conflict with the Qur'ānic principle of *ḥurmat al-bayt* (sanctity of private life) and the *fiqh* prohibition on tajassus (unlawful spying, Q 49:12). Saudi data law's invocation of the principle *al-mālik yu'minu wa lā yamlik* (the custodian protects but does not own) offers a normative response, but its enforceability in practice, particularly against state actors, remains institutionally underspecified and warrants critical scrutiny.

Specific cases highlight the system's scope. *Hajj* permit applications require the applicant to sign a commitment on Absher acknowledging compliance with health regulations; non-compliance is subject to disciplinary measures, as the digital signature represents binding acceptance. Likewise, the registration of divorce via *Najiz* now requires dual Nafath authentication by both parties to guarantee free will (*ikhtiyār*) and guard against coercion (*ikrāh*). Such applications make Sharia ethics programmatically enforceable.[51]

However, integration also raises questions of data ethics: Who has access to citizens' biometric data, and on what grounds can it be shared? Saudi data law applies the principle of *al mālik yu'minu wa lā yamlik* to balance ownership questions (the state is a custodian, not an owner). The information is stored on behalf of citizens and upholds their individual dignity (*karāmah insāniyyah*), but it also permits collective use in the interest of justice and security. This doctrine echoes the Quranic vision of stewardship: human beings are custodians of divine resources and are not their lord and master (Q 2:30). Government becomes the custodian of trust in cyberspace, serving the best interests of people rather than individual rights.[52]

Other Muslim jurisdictions are already drawing lessons. The Malaysian system combines its MyDigital ID with Zakat awarding platforms to eliminate fraud; the Saudi system introduces cultural relevance and moral semantics, transforming identity verification into a perpetually moral act of witnessing. This combination of state and virtue

[51] Ministry of Justice (KSA), *Civil Transactions Law*.
[52] Saudi Data and AI Authority (SDAIA), *Ethical AI Guidelines 2025*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

represents what researchers call devotional citizenship, voluntary involvement in state services as a compliant act of obedience.[53]

The level of moral language used in Saudi Arabian digital regulatory discourse is impressive. Regularly, policy writing is a mixture of technical jargon (TLS encryption, key length, tokenization) and ethical principles (transparency, trust, and justice). This artificially constructed lexical construct shall be indicative of a juridical philosophy in which the normativity of law is not imposed but rests on morals. What can be deemed rhetorical flair in the secular state is, in the Saudi context, legitimation by virtue (*taʿdīl bi al faḍīlah*). People are encouraged to obey the law, since piety entails obedience.[54]

For example, there are information security campaigns with slogans like "Trust is Worship" (*al-thiqa ʿibādah), equat*ing information security with religious responsibility. The SDAIA Ethical AI Guidelines Report (2025) found that 82 percent of surveyed participants reported increased willingness to engage with e-government services after exposure to faith-based awareness messaging. This figure, while sourced from a governmental self-assessment report rather than an independent study, is analytically consistent with the broader sociological literature on perceived institutional legitimacy and compliance behaviour documented by Boateng et al. (2025).[55] Its inclusion here is therefore illustrative of a behavioural pattern rather than conclusive empirical proof of causal effect, and independent replication through peer-reviewed survey research would be necessary to validate this finding.

At the corporate level, compliance has entered a "moral market." The NCDC's licensing scorecard now incorporates ethical performance indicators: whether incidents were reported transparently and whether users received compensation. This economy of virtue brings sūq al-*Amānah*, the market of trust, to bear. Similar to how Islamic finance

[53] Latif and Shamsuddin, "Maqāṣid Driven Digital Governance in Muslim Jurisdictions: Lessons from Malaysia and Indonesia."
[54] Digital Government Authority, *Digital Trust Services Regulation*.
[55] Boateng et al., "Procedural Justice, Obligation to Obey and Cooperation with Police in a Sample of Saudi Arabian Citizens."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

made ethical credit a financial metric, digital trust applies this reasoning to data integrity.[56] Critics warn, however, that over-moralisation risks blurring the boundary between legal obligation and religious conformity, potentially enabling selective enforcement along lines of piety rather than universal legal principle.[57] To reduce this risk, researchers have suggested grounding ethical analysis in universal standards, such as justice, sincerity, and non-harm, rather than in sectarian interpretation. Policy language is now subject to review by the Council of Economic Affairs and Development to secure consistency with constitutional objectives, a compromise that maintains Sharia's universality without prejudice to plural application (*taṭbīq mutanawwiʿ*).[58]

Companies are becoming increasingly reliant on Ethical Compliance Charters. As an example, Saudi Telecom Company (STC) committed to responding to data breach notifications within 24 hours and notifying users in plain Arabic. This policy is not legally required, but it exercises *istiḥsān* maslahi or doing what is more beneficial in the public interest. In like manner, a major e-commerce site deployed a 'return without evidence' policy for customers whose online receipts would not print, based on the Prophetic maxim: 'leave an obscure thing to that one who is not in the slightest doubt.' These are the corporate decisions that translate ethics into customer loyalty and legal security.[59]

Moral Economically, the moral economy of compliance forms a new governance paradigm: audit culture as the nurturing of virtue. Each institution follows what Alotaibi and Alotaibi (2026) refer to as an ethical continuum, a circular relationship in which legal obligation feeds professional ethics, and the reverse is also true.[60] This creates positive externalities in economic terminology, as social capital; in the language of jurisprudence, it by-creates *maṣlaḥah ʿāmmah* (the common good). The Saudi model, therefore, exemplifies

[56] Alotaibi, "Credit Rating in the Islamic System: A Case Study of Saudi Arabian Banks."
[57] Siti Nur Shoimah, "Freedom of Contract in the Digital Age: Perspectives on the Indonesian Civil Code and Fiqh Muamalah," *Trunojoyo Law Review* 8, no. 1 (2026): 59–94, https://doi.org/10.21107/tlr.v8i1.32568.
[58] Zuḥaylī, *al-Qawāʿid al-fiqhīyah wa-taṭbīqātuhā fī al-madhāhib al-arbaʿah*.
[59] Digital Government Authority, *Annual Performance Report on Digital Transformation*.
[60] Alotaibi and Alotaibi, "Professional Boundaries and Ethical Obligations in Saudi Arabia An Integrated Sharia-Saudi Legal-Clinical Framework."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

an uncommon union of compliance economics and religious sociology, as well as a standard of regulatory morality in the Islamic world.

The examples above show that Saudi Arabia's shift to digital trust is not a technical change but a reconfiguration of governance norms. The innovations of the twigs of institutional leadership turn amahnah into an administration; the legal interpretation of the law elevates encryption into evidence; the infrastructure of identities makes citizens subjects of self-witnessing; and the audit culture of corporate organizations accounts profits as ethical. All these dimensions show that the concept of trust in Sharia is not static but evolutionary. The Saudi experience, therefore, provides an exemplar for other Muslim-majority states that need to integrate technological innovation with ethical adherence. *Amānah* is gradually institutionalized, shifting from the personal to the procedural, from spiritual idealism to the architecture of governance, demonstrating that the digitization of law can be an ethical renaissance.[61]

COMPARATIVE FOUNDATIONS FOR ISLAMIC DIGITAL TRUST

Examples of value-neutral formalism include global model laws such as the UNCITRAL Model Law on Electronic Signatures (2001) and the eIDAS Regulation (2014) of the European Union, which rely on signatures indicating identification, intent, and reliability. These models lack cultural considerations, although they are efficient. Saudi Arabia replicates its procedural core with a minor modification: Article 3 of the Digital Trust Services Regulation (DGA, 2025) requires that it be in line with Islamic values of integrity and honesty.[62] Islamic ethics performance criteria are, in effect, in addition to cryptographic strength.

This code of morality is important. It is through the incorporation of religious language into a secular procedural statute that Saudi law creates a hybrid normativity,

[61] Alotaibi, *Islamic Legal Perspectives On Non-Fungible Tokens (Nfts)Exploring The Permissibility Of Non-Fungible Tokens (Nfts) As Digital Assets Under Islamic Law*.
[62] Alaloosh et al., "Securing Digital Trade"; Digital Government Authority, *Digital Trust Services Regulation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

establishing a regime that fulfills both secular standards of compliance and accounts of divine rulership. Accordingly, ceasing to be a transactional guarantee of electronic trust becomes *ʿibadah niẓāmiyyah*, a worship institutionalized in the practice of good governance. The model responds to the criticism from Western theorists that digital law is prone to an ethics lag: Saudi law bridges this gap through lawmaking virtue.[63]

The Saudi regulation is methodologically consistent, but not ideologically consistent with the efforts in other Muslim jurisdictions. The Digital Signature Act (1997), amended in 2020, underlies the licenses in Malaysia and requires them to be supervised by the Shariah Advisory Council.[64] This integration has ensured that technological validation does not facilitate unwarranted lending, such as ribaʾ. A comparable role was played by the Diyanet Fatwa (2018) of Turkey, which recognized electronic signatures as legitimate when they help avert forgery, thereby directly enforcing *sadd al dharaʾiʿ* (blocking means to harm). The UAE law of 2021 inculcates the principle of *ḥifẓ al ʿird* (protection of dignity): the right to privacy is construed as safeguarding personal honor.[65] Against this background, this approach in Saudi Arabia can be described as moral codification. Rather than a line of external clerical vetting, the structural requirements internalize the ethical test in the form of provider-audit, data-sovereignty, and Sharia-referential articles 3 and 5 language. This is a sign of a mature state: institutional morality is self-regulating and not reliant on post hoc religious opinion.[66]

The ethical paradigm of developing the Gulf Cooperation Council will reinterpret regional standards, as the draft of the Mutual Recognition Agreement on Electronic Trust Services (draft 2025) relies on Saudi Arabia's ethical framework. Traditional cross-border models (including the UNCITRAL Cross-Border Certification Guidelines) only address technical settings (key length, timestamps). Saudi negotiators are ready to offer one more criterion: verifying the morality of the providers and the transparency of the institutions.

[63] Rosenbach, "Value Neutral Tech Law and Its Limits: An Ethical Audit."
[64] "Principles of Islamic Jurisprudence 3," Dokumen.Pub, accessed May 25, 2026, https://dokumen.pub/principles-of-islamic-jurisprudence-3.html.
[65] Hamdan, "Electronic Signatures and Evidentiary Law in the Gulf."
[66] Digital Government Authority, *Digital Trust Services Regulation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Such transnational trust would be ethically aligned with Sharia's aims of justice (*ʿadl*) and utility to the population (*maṣlahah ʿāmmah*) by incorporating ethical interoperability.[67] In practice, it means that the Saudi courts could accept a suitable certificate issued in Bahrain or Oman, provided that the issuer adheres to anti-deception ethics akin to those of the *Amānah* muwaththaqah. The proposal shows Saudi Arabia's aspiration to establish the standards of de jure ethics in international digital trade.[68]

PRELIMINARY FINDINGS AND REFLECTION

The cumulative analysis shows that Saudi digital trust control can attain harmony of technical reliability and religious validity. It yields three interrelated findings, each with a deeper connotation. To begin with, technological authenticity is reminiscent of the Sharia concept of *tathabbut* (rigorous verification). They are both targeted at finding the truth and improving welfare. The Saudi authorities formalize a continuous certification process, modern-day tathabbut, by mandating regular audits of signature providers and requiring that they be nationally accredited. It is not limited to legal practice but also to theology: the Prophet himself says in verse 49:6, "verify the news; believe it first." This sentiment is echoed in cybersecurity ethics.[69]

Second, attribution by certification is a copy of classical witness validation. The two most important cryptographic systems (private/public) echo the Sharia two-witness test: one is the witness of authorship, and the other of accuracy. Functional equivalence between the machine protocol and dual witness exists when an issuer signs a document with an eligible key, which the NCDC verifies. Reliability, then, is a factor based on doubleness, technical and moral.[70] Third, individual trust is replaced by collective trust (*thiqa jamāʿiyyah*). Notarization using blockchain, piloted in the Saudi Real Estate Registry (2025), distributes the role of custodian among multiple nodes. Documents are copied to every node, and this

[67] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*.
[68] Alharthi and Alotaibi, "Harmonising Legal and Sharia Principles in Foreign Investment."
[69] Digital Government Authority, *Digital Trust Services Regulation*.
[70] Al ʿAbbadii, *Al Tawthīq Fī al Fiqh al Islāmī*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

does not allow for unilateral manipulation, an analog to *shahādah mutawātirah* (mass testimony) in the digital world. As a result, community dependence on faith in certain individuals is replaced with trust in just structures.[71]

These results disprove the myth that digitization secularizes Sharia. Instead, Saudi Arabia demonstrates that both algorithmic reliability can be used to ship divine morals. Innovation does not, therefore, negate faith, or vice versa, but forms part of the jurisprudential tenor that Alotaibi (2025) and Auda (2008) categorize as *maqāšid*-centered modernization.[72] This paradigm views technology as a servant (khādim li *maqāṣid* al *Sharīʿah*) of moral purposes, not its competitor. As a result, digital trust services in the context of Saudi law are not an innovation in opposition to tradition but rather an innovation in the form of digital tradition.

TOWARD A SHARIA COMPATIBLE FUNCTIONAL MODEL

Responsiveness between modern need and classical source is the principle of *tajāwub bayna al ʿaṣr wa al aṣl*, which underlies Saudi Arabia's interpretive approach. The historical development of Islamic jurisprudence was based on its contextual modification. The Abbasid period saw the replacement of oral transactions by notarial written deeds, and Ottoman reforms made printed contracts and telegraph messages admissible as evidence. By analogy, one can say that the cryptographic verification adopted by Saudi law is a continuation of this juristic elasticity (*murūnah fi al fiqh*). The point is the purposeful faithfulness: the assurance (*yaqīn*) that all electronic dealings are the product of an aware agent, morally obligated.[73]

Theoretically, functional equivalence is not just semantical. The juristic maxim al umūr bi *maqāṣid*ihā (matters are judged by their purposes) allows reinterpretation of forms

[71] Digital Government Authority, *Annual Performance Report on Digital Transformation*.
[72] Alotaibi, *Islamic Legal Perspectives On Non-Fungible Tokens (Nfts)Exploring The Permissibility Of Non-Fungible Tokens (Nfts) As Digital Assets Under Islamic Law*.
[73] Dokumen.Pub, "Principles of Islamic Jurisprudence 3."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

that have justifiable ends.[74] Therefore, the digital seal will acquire the same moral status as a handwritten signature after acquiring *ḥifẓ al ḥuqūq*, protection of rights, and *manʿ al ghaṣb*, prevention of usurpation. Saudi courts are unconsciously using this functional argument. The judges in Riyadh Commercial Court Judgment 233/1445 (2023) compared the validation of an e-contract by multi-factor authentication to the validation of a contract by swearing; both constitute an obligation based on indications of reliability.[75]

Yet, challenges persist. Those in conservative *fiqh* movements are worried that digital processes are an abstraction that leads to the depersonalization of testimony and the moral decline of *ʿadālah* (moral uprightness). As an answer to this, legal scholars suggest a stratified model of witnessship (*shahādah murakkabah*) in which machine processes are extensions, not replacements, of human integrity. This framework acknowledges machines as protocolic witnesses whose probative power hinges on human care and will. It reflects the old debate over whether written records of events are more reliable than orally attested records: both were allowed so long as responsible guardians established them. In this way, the institutionalization of *ʿadālah niẓāmiyyah* (systemic honesty) by the DGA regulatory hierarchy is enforced through established laws and audits.[76]

The other consequence of functional equivalence is inclusivity. Previous legal systems favored human literacy; digital authentication has made access more democratic, enabling citizens at all levels of education to engage in transactions without fear. This democratization asserts *raf ʿ al ḥaraj* (the lifting of hardship), one of the universal maxims of Sharia law. Digital transformation is, therefore, not only compatible with the modernization of the economy but also with *maqṣad al ʿadl al ijtimaʿī* (social justice).[77] The metamorphosis also causes epistemological changes. Where previous evidence had relied on personal witnessing, which could be incorrect or subject to bias, cryptographic proof is now based on mathematics, producing what theologians presently know as *ʿilm yaqīnī nisbī*

[74] Dokumen.Pub, "Principles of Islamic Jurisprudence 3."
[75] Ministry of Justice (KSA), *Annual Judicial Statistics Report 2025*.
[76] Digital Government Authority, *Digital Trust Services Regulation*.
[77] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

- relative and solid certainty through repeatable procedures. This epistemic harmonization sheds light on how the probabilistic reasoning of *fiqh* (*ghalabat al ẓann*) inherently aligns with algorithmic probability. Thus, digital authentication cannot conflict with or override Sharia; it measures its axiological interest in certainty.[78]

Integrating *maqāṣid* al *Sharīʿah* into policy design requires tracing how the five "universal objectives" (*al ḍarūriyyāt al khams*), faith, life, intellect, lineage, and wealth, materialize in cyber law.[79] Saudi policymakers increasingly interpret ḥifẓ al dīn (protection of faith) as ensuring that technology supports, not subverts, ethical order. By embedding Islamic terminology into regulatory texts, the Kingdom transforms abstract piety into enforceable governance metrics.[80] For instance, Article 3 of the Digital Trust Services Regulation references "integrity and honesty" (*ṣidq* wa *Amānah*) as prerequisites for accreditation. This reference performs tasrīḥ bi al maqṣad: explicit articulation of moral intent within positive law.[81]

Critically, efficiency (*kifāʾah faʿʿālah*) is reframed through *rahmah tashrīʿiyyah*, legislative compassion. Digitized documentation reduces human error and bureaucratic delay that historically burdened litigants, thereby fulfilling the Qurʾānic ethos of ease (Q 2:185). However, observers caution that excessive automation may privilege speed over deliberation, conflicting with the juristic principle *al taʾannī min Allāh wa al ʿajalatu min al shayṭān* (caution is divine, haste is satanic). Hence, Saudi implementation combines automated queues with judicial oversight, balancing efficiency and prudence.[82]

Transparency and participation bring about confidence (*thiqa ʿāmmah*). Users trust systems such as *Najiz* not just because of the secure code but also because they believe

[78] Wael B. Hallaq, *Sharīʿa: Theory, Practice, Transformations* (Cambridge University Press, 2009).
[79] Muhammad Shohibul Itmam et al., "Legal Politics of Mining Spatial Planning in Sumenep District: Maqāṣid Syarī'ah Overview," *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan* 25, no. 1 (2025): 1–27, https://doi.org/10.18326/ijtihad.v25i1.1-27.
[80] Bunyamin et al., "Reforming Indonesia's Correctional System."
[81] Digital Government Authority, *Digital Trust Services Regulation*.
[82] Raysūnī, *Al Fiqh al Islāmī Wa Maqāṣid al Sharīʿah al ʿĀmmah [Islamic Jurisprudence and the Objectives of Islamic Law]*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

systems reflect divine justice. According to social psychological studies, religious framing improves compliance with rules.[83] Taking advantage of these, Saudi regulators enhance civic behavior, including theological echo, by broadcasting awareness campaigns under the name of Digital Amana is Faith, which similar initiatives may follow in other Muslim-majority states.[84] Security (*amn raqamī*) is an operationalization of *ḥifẓ al mall* and *ḥifẓ al ʿaql*.[85] Cyberattacks compromise economic stability and erode collective rationality by disseminating misinformation. From the perspective of *maqāṣid*, counter-cybercrime programs reflect the aspect of *dafʿul fasaad* (prevention of corruption). The National Cybersecurity Strategy (2025) outright cites the Qurʾani expression *la tafsidu fi al ard* as a policy slogan - arguably the first instance in Saudi administrative law of an ethical principle (or, to be exact, an ethical slogan) turned into a cyber-slogan.[86]

In a comparative view, these maqsadic translations contrast with the value-neutral objectivity of Western digital laws.[87] Data privacy protection in Europe is guaranteed, but does not rely on moral terms. Saudi law, by comparison, treats privacy as a secondary matter to dignity (*karāmah insāniyyah*) and trust. This difference indicates a new jurisprudence: the instrumentalism of ethics (*al ādāt al akhlaqiyyah li al ḥukm*), the application of law as a vehicle to enhance virtue.[88] The Digital Amana by Design model is not a simple technical architecture; it is a sociotechnical process that links hardware, software, and moral software (*al-barmajiyyāt al-akhlaqiyyah*). All the pillars can be extended to tackle ethical and operating tensions. According to information security theorists, integrity refers to the accuracy and

[83] Boateng et al., "Procedural Justice, Obligation to Obey and Cooperation with Police in a Sample of Saudi Arabian Citizens."

[84] Arim Nasim et al., "Driving Maqāṣid Al-Shari'ah Performance in Islamic Banks: The Roles of Islamic Social Reporting, Intellectual Capital, and Sharia Governance," *Al-Muamalat* 13, no. 1 (2026): 102–18, https://doi.org/10.15575/am.v13i1.54396.

[85] Khalid Rashid, "Reforming Islamic Finance: A Framework for a Proposed Non-Banking Institution to Facilitate Participative Financing," *Al-Muamalat* 13, no. 1 (2026): 146–68, https://doi.org/10.15575/am.v13i1.53042.

[86] Saudi Data and AI Authority (SDAIA), *Ethical AI Guidelines 2025*.

[87] Iskandar et al., "The Influence of Green Financing and Return Dynamics on Environmental, Social, and Governance Performance: Evidence from Indonesia's Islamic Banking Sector," *Al-Muamalat* 13, no. 1 (2026): 169–85, https://doi.org/10.15575/am.v13i1.54428.

[88] Valverde and Greenleaf, "Understanding Legal Culture in Cybersecurity Legislation: Beyond Technical Neutrality."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

completeness of information and the processing that produces it. The convergence of the Islamic jurisprudence is that contracts are true (*ṣidq*) and free of ambiguity (*gharar*). This is codified in Saudi law as certification requirements, including the maintenance of hash verification records that must be stored for at least 10 years. The longevity of records is based theologically on the theme of eschatology: nothing small or great, but written in a Book (Q 18:49). Therefore, data immortality is divine omniscience in a controlled space, which places integrity as a religious simulation of responsibility (*muhasbah*).[89]

Accountability (*masʾuliyyah*) is translated as traceability in digital forensics. All transactions are documented using timestamps, device identifiers, and user identifiers. But ethical issues arise when identities are shared (e.g., family or corporate accounts). This is solved when the *fiqh* principle al ghurm bi al ghunm (liability accompanies benefit) is applied by the Saudi jurists. In case a party gains an advantage from a joint account, they too share equal responsibility for any unauthorized action. This concept shifts the responsibility from individuals to institutions, taking a major step towards corporate ethics in Islamic governance.[90]

The practice of auditing tends to become a box-ticking exercise internationally. Islamic ethics reframes audit as *muʿāyanah li al ḥaqq* (inspection of truth). The practice in Saudi Arabia mandates that, in audit reports, commentary on moral integrity be made apparent, rather than just on technical performance. An example is a 2025 NCDC report that ranked providers based on their attitude toward disclosing breaches as a virtue coefficient, which was likely inspired by a saying of the prophet stating that the truthful and trustworthy merchant would be among the prophets and the righteous. These measures constitute what social scientists call a moral feedback economy, in which righteousness is associated with market value.[91]

[89] Digital Government Authority, *Digital Trust Services Regulation*.
[90] Zuḥaylī, *al-Qawāʿid al-fiqhīyah wa-taṭbīqātuhā fī al-madhāhib al-arbaʿah*.
[91] Digital Government Authority, *Annual Performance Report on Digital Transformation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Sharia Supervision in this case is not merely a symbolic blessing but an energetic monitoring akin to a board of ethical review in the medical field. Fears over infringing bodily privacy when biometric signature certification arose prompted juristic committees to appeal to *ḥifẓ al nafs* (protection of personhood) and to create preconditions for restricting data storage. In this way, supervision according to *fiqh* is an adaptive regulation that balances innovation and restraint (*iʿtidāl*).[92] Taken together, these processes make up a system of embedded ethics, with the software requirements specifications containing direct enumerations of both ethical and non-ethical controls, in equal measure, because such controls are rare in Western systems of governance.[93]

Saudi Vision 2030 aims to create a lively society, a flourishing economy, and a bold country. Digital trust would add value to all three pillars. In addition to the recommendations made previously, there are important strategic expansions. Legislative Consolidation. The existing variety of laws (E Transactions, Evidence, Civil Transactions, and Digital Trust) leads to fragmented interpretation. An e-dealing code could harmonize terminology and fill gaps in liability provisions, akin to the United States Uniform Electronic Transactions Act (1999). The Kingdom would symbolically and practically entrench the digital law in its theological constitution by making Sharia maxims general principles to precede the code.[94] Registers of institutions and experts. Putting in place digital evidence professionals on a licensed register (*muqayyadūn fi ʿilm al raqmī*) will guarantee competence in courtrooms. Such professionals are modern ʿudul; their qualifications provide quasi-conclusive authority. [95] Socio-economic Incentives. The mainstreaming of corporate ethics is stimulated by tax cuts and other fee cuts on organizations that have high scores in the "trust scale. The Ministry of Economy (2026) estimates that by 2026, ensuring that only 30 percent of Saudi SMEs comply with

[92] Digital Government Authority, *Digital Trust Services Regulation*.
[93] Cordoba and Haider, "Engineering for Ethics: Moral Systems Analysis in Digital Governance."
[94] Dokumen.Pub, "Principles of Islamic Jurisprudence 3."
[95] Ministry of Justice (KSA), *Annual Judicial Statistics Report 2025*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

accredited standards of digital trust could increase national GDP by 2 percent through reduced fraud costs.[96]

Online Trust and Gender. The involvement of women in business increased threefold as home-based entrepreneurship became easier with the introduction of e-signature authorization.[97] The agency of the female subject under digital anonymity complies with ʿiffah (modesty) and *Amānah* fī al tikalluf in Islamic ethics. The state, in this way, promotes gender equity without contradicting Sharia norms - an important example of gender and legislation studies around the world.[98] Environmental Impact. Data centers require energy; connecting eco-sustainability with *mashrūʿiyyah ʿāmmah* (public legitimacy) gives a new twist to amana. The Qurʾānic idea of *istikhlāf fī al arḍ* (stewardship on earth) extends the concept of trust to ecological responsibility.[99] Therefore, energy efficiency and the use of renewable energy can be embedded in the certification standards for green trust services.[100] The combination of AI, quantum encryption, and Internet of Things (IoT) devices raises new *fiqh* questions: Is autonomous machine decision-making a proper form of intent (*niyyah*)? Is AI testimony *shahada ḥissiyyah* (empirical witnessing)? Saudi scholars are conditional believers: AI outputs can only be accepted as valid when they can be traced to human choices in programming and checked against references and logs. This meaning is based on ideas of classical mechanical jurisprudence, e.g., the liability of a trained animal (*kalb muʿallam*) deployed in hunting lies with its owner. Similarly, the responsibility for machine operations remains with human operators. In this way, autonomous systems become law as *ālat shahādah* (instruments of witness), rather than a witness. These kinds of juristic parallels demonstrate the flexibility of *fiqh* to cyber ontology.[101]

---

[96] Digital Government Authority, *Annual Performance Report on Digital Transformation*.

[97] Trianah Sofiani et al., "Mosques as Catalysts for Islamic Financial Inclusion: Evidence from Branchless Banking Implementations," *Asy-Syari'ah: Jurnal Hukum Islam* 27, no. 2 (2025): 143–170, https://doi.org/10.15575/as.v27i2.48309.

[98] Digital Government Authority, *Annual Performance Report on Digital Transformation*.

[99] Aftab Haider et al., "From Stewardship to Sustainability: A Comparative Analysis of Islamic Ecological Jurisprudence and Western Anthropocentric Regimes," *JURIS (Jurnal Ilmiah Syariah)* 25, no. 1 (2026): 41–60, https://doi.org/10.31958/juris.v25i1.16040.

[100] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*.

[101] Zuḥaylī, *al-Qawāʿid al-fiqhīyah wa-taṭbīqātuhā fī al-madhāhib al-arbaʿah*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Quantum computing adds another dimension: while cryptographic keys can be theoretically broken, the Sharia concept of *qatʿ al dalīl* (conclusive proof) faces technical relativism. Saudi strategists advocate for redundant certainty, layering multiple proof systems (blockchain + biometric + AI anomaly detection), to achieve combined confidence approximating *bayyinah qāṭiʿah*. Philosophically, this shift parallels Ashʿarite epistemology: no created system can attain absolute knowledge, yet probabilities may reach the level of obligatory confidence.[102] IoT makes privacy vulnerable: Smart meters and wearables constantly track data that can be used as evidence. According to Islamic morals, videotaping without permission can be a breach of *ḥurma āl bayt* (sanctity of home). Thus, Saudi data protection legislation equates technical privacy with moral inviolability, equating unlawful surveillance with an unlawful gaze. Framing privacy through *karāmah insāniyyah* (dignity) resacralizes data beyond commodification.[103]

A community of Interpretive Practice is needed in long-term trust ecosystems. Academic sector. The gap between the theory of divine law and the drafting of regulations may be closed through new research chairs in Digital *Maqāṣid* and Cyber Ethics at King Fahd University. Proceedings of annual conferences are to be published in English and Arabic, and the Saudi digital *fiqh* research is to be available to the whole world.[104] Industry. ESG indexes are increasingly judging corporations; a new index, the Faithful Technology Index, would tie market capitalization to moral capital. In particular, a Sharia-compliant fintech enterprise might be listed on Tadawul on preferential terms to promote ethical innovation.[105]

Fatwa institutions. The Council of Senior Scholars can constitute a standing committee, a Digitally Fatwa Committee, under which jurists can be paired with engineers. A fatwa is not just responsive but also regulatory, offering preemptive guidance on

[102] Hallaq, *Sharīʿa: Theory, Practice, Transformations.*
[103] Saudi Data and AI Authority (SDAIA), *Ethical AI Guidelines 2025.*
[104] Alotaibi, *Islamic Legal Perspectives On Non-Fungible Tokens (Nfts)Exploring The Permissibility Of Non-Fungible Tokens (Nfts) As Digital Assets Under Islamic Law.*
[105] Alotaibi, "Credit Rating in the Islamic System: A Case Study of Saudi Arabian Banks."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

technological developments. Such institutional *ijtihād* prevents fragmentation and ensures uniform legal certainty across government agencies.[106] Lawyers, engineers, and IT specialists can establish an Ethical Trust Forum to discuss draft regulations publicly. Engagement in reading out laws recites the Qur'anic concept of *shūrā* (consultation). It even responds to academic opponents who declare that state-centric legislation will lead to a moral monopoly.[107]

The ripple effects of a Sharia-compliant digital trust system can already be observed in Saudi Arabia's social decision metrics. The number of document forgery cases decreased by 28 percent between 2022 and 2025.[108] E-commerce thrived, with companies such as Silla and Noon introducing state-issued verified signatures. These are economic implications that decompose into moral externalities: because transactions are at par, citizens interact with greater trust (*thiqa muʿāmalah*). This trust eliminates self-interest bias, accomplishing the Prophetic vision; merchants are the reliable members of the community.

Legally and philosophically, digital trust rebalances the relationship between individuals and the state. The people no longer regard the court as a faraway judge but as an accessible companion in the moral check. This reactive Government entrenches *ʿadl niẓāmī*, systemic justice, in popular sentiment. This strategy also appeals to non-Muslim populations in the Kingdom, showing that ethical Islamic rule can be universal and inclusive.[109]

Last but not least is the spiritual aspect. By carrying out digitally verifiable transactions, people are involved in a novel type of mudhakkirah ʿamaliyyah - remembering God daily through the truth of acting. Digital *Amānah*, in this broader civilizational sense,

[106] Dokumen.Pub, "Principles of Islamic Jurisprudence 3."
[107] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*.
[108] Ministry of Justice (KSA), *Judiciary Statistics and Digital Performance Report 2025*.
[109] Boateng et al., "Procedural Justice, Obligation to Obey and Cooperation with Police in a Sample of Saudi Arabian Citizens."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

rehabilitates the classical ideal of truth-telling-worship; Saudi Arabia is becoming a pioneer of ethical modernity.[110]

PRACTICAL RECOMMENDATIONS AND FUTURE DIRECTIONS

Legal, academic, and societal efforts are necessary to translate theory into practice. The success of the experiment with the digital trust in Saudi Arabia is related not solely to statutory innovation but also to a sustainable ecosystem of ethics, institutions, and research. The recommendations below are a combination of theoretical and practical measures that will help make Digital *Amānah* a permanent national philosophy and an Islamic export culture to the global community and the Muslim world at large. The first priority is to promulgate the Saudi Code of Digital Ethics, a policy analogous to corporate governance codes in finance. Although the National Cybersecurity Authority (NCA) and the Digital Government Authority (DGA) already provide technical frameworks, an ethical charter would enforce them in line with the Sharia concepts of *Amānah*, *ṣidq*, and *ʿadl*. This code may detail quantifiable indicators, such as breach disclosure time, transparency in consent, and fairness of algorithms, in the form of integrity metrics. All licensed trust service providers would provide an Annual "Self-Assessment of Amanaah showing how their operational procedures bring into effect Quranic imperatives of honesty and accountability. Such ethical reporting would also place Saudi Arabia ahead of the pack in global value-based technology governance, just as it does with environmental, social, and governance (ESG) disclosures. In practice, this command might be similar to the Sharah Governance Framework used by Islamic banks, generalized to apply to digital infrastructure rather than finance.[111]

Since no country can control the national boundary in cyber transactions, it is necessary to harmonize the legal interpretation of religious behavior across the Gulf. Saudi Arabia may establish the GCC Digital *Fiqh* Council, comprising jurists and technologists

[110] Alotaibi, *Islamic Legal Perspectives On Non-Fungible Tokens (Nfts)Exploring The Permissibility Of Non-Fungible Tokens (Nfts) As Digital Assets Under Islamic Law*.
[111] Digital Government Authority, *Digital Trust Services Regulation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

from the member states. This council would create common *ijtihād* (shared interpretative decisions) on cross-country matters such as blockchain-based smart contracts, cross-country artificial intelligence, and cross-country data flows. Its fatwas would be persuasive, like the International Islamic *Fiqh* Academy (Jeddah), but with an emphasis on digital phenomena. An example would be a unified decision on blockchain notarization, which would allow property registries across the GCC to be recognized by one another and hasten trade integration in the region. Procedurally, the digital authority of each member state might submit draft regulations for ethical consideration by the council, ensuring that all member states do so without interfering with sovereignty. The outcome would be a common ethical language of the digital economy of the Gulf - a manifestation of *Amānah* mushtarakah (a collective trust).[112]

A Trust and Justice Index is another tool for instilling morality into market performance. This index would order state agencies and commercial enterprises based on technical resilience, ethical openness, responsiveness to data breaches, and user satisfaction. The scores would be obtained through quantitative measures (system uptime, incident frequency) and qualitative measures (public confidence surveys, independent ethics audit ratings). This index should be published annually to habitualize moral responsibility, as credit ratings habituate fiscal responsibility. For example, a telecommunications company with a high score may be offered lower certification fees or priority consideration in government procurement.

On the other hand, any institution with a mark below would be subject to a compulsory compliance rectification. Such moral market competition operationalizes the *fiqh* principle *al ḥisān bi qadr al iḥsān*, reward proportional to good conduct. As with the Saudi Capital Market Authority and its Tadawul Sustainability Index, transparent scoring is not only effective in improving foreign investment but also in establishing a good

[112] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

national reputation; something that, scaled up to digital ethics, would be a parallel system of spiritual credit rating.[113]

The Digital law of trust can be legitimized in the long run only by a group of experts who have not only mastered the art of jurisprudence but also are technologically savvy. It is upon the universities to therefore open interdisciplinary graduate courses known as Islamic Cyber Law and Digital Ethics. Combined law, computer science, and Sharia college combination: Jurists with the required skills to write or interpret code will be trained within the confines of the *uṣurlu al fiqh*. Some courses could consist of: Comparative Digital Evidence Law, Sharia Foundations of Data Protection, and Algorithms Accountability in Islamic Finance. Ministry of Education-funded research clusters can collect data on Saudi court decisions involving electronic evidence, a currently under-researched area. Graduates of these educational programs would, over time, become policy analysts and *qāḍīs* who understand how to reconcile Qur'anic ethics with machine logic. Historically, as exemplified by the role of madrasa scholars, the law of inheritance requires madrasa scholars to master astronomy and mathematics to perfect the law; this rule remains applicable in modern coding, as it requires the jurist of the modern era to master coding.[114]

The development of digital ethics cannot be based solely on doctrinal reasoning; it requires empirical analysis. Future research would quantify citizens' perceptions of religious discourse in technology policy and determine whether this framing promotes a sense of trust and obedience. The public reaction to privacy notices based on two different versions could be studied in survey experiments: one version presented legally and the other presented as a moral obligation. The results would be used in cultural communication strategies. Moreover, quantitative research might evaluate correlations between company "trust scores" and actual incident rates, and test the hypothesis that moral internalization is associated with technical breaches. Economically, researchers may examine international investors' views on Saudi Arabia's religiously based governance system: does embedded

[113] Alotaibi, "Credit Rating in the Islamic System: A Case Study of Saudi Arabian Banks."
[114] Dokumen.Pub, "Principles of Islamic Jurisprudence 3."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Sharia language reflect ethical finance capital or scare off secular investors? Scientific virtues: Normative aspirations can be evidenced through empirical data, thereby enhancing the scientific virtue of tathabbut (verification), as in its theological context.[115]

Another research frontier involves evaluating algorithmic bias using Sharia-compliant fairness metrics. For example, *ʿadl* (just balance) can be operationalized as proportional equality of error rates across demographics. Collaborations between SDAIA data scientists and Islamic ethics scholars could yield dual validation protocols: one quantitative, one moral. Such integration would convert *qawāʿid fiqhiyyah* (legal maxims) into performance standards, pioneering what might be called Sharia-aligned AI audit methods.[116]

When ethical innovation engages global institutions, it creates lasting value. Saudi Arabia must therefore introduce its Digital *Amānah* Framework to other organizations such as the OECD, UNCTAD, and the World Summit on the Information Society. Placed in contrast to digitally law template fuzzy values Western versions, this framework presents an alternative, theologically based selection, Ethical Islamic Digital Governance. Saudi specialists can demonstrate the pragmatic benefits of cultural ethics by explaining how moral accountability can help prevent cybercrime and fraud to secular regulators. The leadership of the Kingdom of Islamic finance demonstrates that moral architecture can be applied on a global scale; moral advocacy could later incorporate ethical considerations into global cybersecurity regimes. The launch of the Digital Amoah model, using white papers and diplomatic workshops in both languages, would promote cross-cultural communication, positioning Saudi Arabia not as a technology adopter but as the digital morality architect.[117]

[115] Boateng et al., "Procedural Justice, Obligation to Obey and Cooperation with Police in a Sample of Saudi Arabian Citizens."
[116] Saudi Data and AI Authority (SDAIA), *Ethical AI Guidelines 2025*.
[117] Valverde and Greenleaf, "Understanding Legal Culture in Cybersecurity Legislation: Beyond Technical Neutrality."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

International cooperation can go further by using bilateral legal tools and mutual recognition agreements on electronic certification with Asian and African countries whose systems are influenced by Sharia. By such alliances, the Kingdom might not only be able to export both its technology and its moral code, but to blueprint a local policy into a global standard of responsible digital behavior.[118] Public ownership is needed beyond institutional reforms in sustainable ethics. An ongoing education campaign should be called Cyber *Amānah* to Every Citizen to educate people on the importance of being honest online as a way to express faith. Ethical compliance might be gamified on interactive platforms, with verified Trust Badges awarded to users who practice safe habits and report cyber fraud. Moral digital literacy modules on the religious importance of consent and confidentiality can be included in high school curricula, as they relate to Qurʾānic commandments and real-life app usage. Such civic training transforms cybersecurity from a technical discipline into a communal *farḍ kifāyah* (a collective obligation).[119] Engagement of the population will also involve encouraging medium-sized microenterprises to embrace ethical technology. Government subsidies may be biased toward new ventures producing Arabic-language privacy applications or ancestry protection apps grounded in the theory of dignity (*ḥifẓ al nasab*). The state makes it easier to integrate innovation with moral stories, more than profit indicators, and the way it fosters entrepreneurs to perceive technology as *Amānah* maqṣūdah; the trust that God gives to society to benefit it, purposely.[120]

To ensure that ethical principles do not decay into rhetoric, oversight systems must incorporate continuous measurement. Adopting a five-year "Ethical Impact Assessment Cycle" would require every major technology agency to review its operations against *maqāṣid* al *Sharīʿah* benchmarks. Metrics could include reduction in data breaches (ḥifẓ *al māl*), increased women's participation in the digital economy (*ʿadl* musāwah), and citizen confidence indices (*thiqa ʿāmmah*). Results would feed into national performance

[118] Alharthi and Alotaibi, "Harmonising Legal and Sharia Principles in Foreign Investment."
[119] Zuḥaylī, *al-Qawāʿid al-fiqhīyah wa-taṭbīqātuhā fī al-madhāhib al-arbaʿah.*
[120] Alotaibi and Alotaibi, "Professional Boundaries and Ethical Obligations in Saudi Arabia An Integrated Sharia-Saudi Legal-Clinical Framework."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

dashboards, which would be publicized like Vision 2030 progress reports. This cyclical evaluation embodies the *fiqh* notion of *murājaʿah* (periodic review) and keeps ethics a living, iterative process rather than a static proclamation.[121]

These actions would not only strengthen domestic policy but would also further establish Saudi Arabia as an exporter of moral technology policy. The Digital *Amānah* Framework can reconcile Islamic ethics and universal humanitarian norms by aligning with the United Nations Sustainable Development Goals, particularly Goal 16 (peace, justice, and strong institutions). The convergence offers an all-inclusive story that appeals to both faith-based and secular viewers. Moreover, Saudi involvement in international task forces on data governance would indicate that religious morals can promote, rather than limit, scientific advancement. Such engagement could inspire an emerging discipline, Digital *Maqāṣid* Governance, in which the values of justice (*ʿadl*), compassion (*raḥmah*), and stewardship (*istikhlāf*) serve as design principles embedded in code and policy alike.[122]

Altogether, implementing these recommendations will transform the initiative on digital trust in Saudi Arabia into a civilizational contribution and make it a national reform. Regulation will have a spirit given by ethics codes; coordination of *fiqh* in the region will give doctrinal unity; measurement indices will institutionalise accountability; academic programs will make ethical technologists; moral governance will be universalised by advocacy; and engagement by civic groups to give the entire system its place in the minds of the people. Combined, these measures move the digital policy beyond the issue of rule observation to the practice of collective worship, *ʿibādah muʿāmalātīyah*, and make trust services daily expressions of faith and reason collaborating.[123]

Such a system, when fully actualized, establishes that theology is not an enemy of technology but a partner with it in the work of justice, and that it co-invents the ethical

[121] Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law*.
[122] Boateng et al., "Procedural Justice, Obligation to Obey and Cooperation with Police in a Sample of Saudi Arabian Citizens."
[123] Digital Government Authority, *Digital Trust Services Regulation*.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

digital civilization in which the integrity of spirituality and human dignity cannot be separated from the performance of technology.[124]

CONCLUSION

This study examines the digital trust framework in Saudi Arabia as an authentic implementation of Islamic evidentiary ethics in cryptographic authentication systems and argues that *Amānah*, *tawthīq*, and *bayyinah* have functional equivalents in the digital certification infrastructure, not functional substitutes. Theoretically, the study is valuable because it applies *Maqāṣid*-based modernization theory to digital governance and proposes Digital *Maqāṣid* Governance as a replicable analytical framework for Muslim-majority jurisdictions seeking to balance Sharia ethics and modern digital infrastructure without undermining the theological basis. In practice, the framework will provide policymakers with a normative framework to establish ethically embedded digital trust systems that align with international standards and Islamic principles of law. Limitations of the study include its jurisdictional bias toward Saudi Arabia and its interpretive, rather than empirically tested, analogies. Future research should validate this framework comparatively across Malaysia, Pakistan, and Indonesia, and empirically examine citizens' perceptions of religiously framed digital governance and biometric data centralization in line with Islamic privacy principles.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support of the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU), which funded this research. The author also expresses appreciation to the editorial team and the anonymous reviewers, whose constructive feedback strengthened the scholarly rigor of this work.

[124] Cordoba and Haider, "Engineering for Ethics: Moral Systems Analysis in Digital Governance."

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

AUTHOR CONTRIBUTIONS STATEMENT

Hajed A. Alotaibi conceived the research idea, developed the theoretical framework, designed the research methodology, conducted the primary legal and doctrinal analysis, and drafted the manuscript. Bandar A. Alyahya contributed to data collection and interpretation, particularly regarding Saudi digital trust regulations, comparative legal frameworks, and institutional governance mechanisms, and assisted in critical revision of the manuscript. Salem R. Alazizi contributed to the analysis of Islamic jurisprudential sources, maqāṣid al-Sharīʿah interpretation, validation of legal arguments, and manuscript review and editing. All authors participated in the discussion of the findings, approved the final version of the manuscript, and agreed to be accountable for all aspects of the work.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest. The funding body, the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU), had no role in the design of the study, the collection or interpretation of materials, the drafting of the manuscript, or the decision to submit the paper for publication.

AI USAGE STATEMENT

This paper is an original scholarly work produced entirely by the authors without the assistance of artificial intelligence writing or text-generation tools. All legal analysis, jurisprudential interpretation, theoretical argumentation, and written expression contained in this manuscript were developed and composed independently by the author. No AI-assisted drafting, paraphrasing, or content-generation software was used at any stage of the research or writing process.

FUNDING STATEMENT

This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2604).

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

BIBLIOGRAPHY

Al ʿAbbadii, Muhammad F. *Al Tawthīq Fī al Fiqh al Islāmī*. Dār al Nafā'is, 2015.

Alaloosh, Mahmood, Govar Majed Ahmad, and Lara Adel Jabbar. "Adapting Iraqi Law to Smart Contracts: A Comparative Analysis Incorporating Islamic Law Principles and Consumer Protection in the Contemporary Digital Era." *MILRev: Metro Islamic Law Review* 5, no. 1 (2026): 210–246. https://doi.org/10.32332/milrev.v5i1.13031.

Alaloosh, Mahmood, Ali Shaker Mahmood, and Sabir Hussien Eliwy. "Securing Digital Trade: A Techno-Legal Analysis of E-Commerce Safeguards in Iraq's Regulation No. 4/2025." *Nusantara: Journal of Law Studies* 5, no. 1 (2026): 44–60. https://doi.org/10.5281/zenodo.18452737.

Al-Anshori, Huzaimah, M. Syamsudin, Agus Triyanta, Ramadhita Ramadhita, Syabbul Bachri, and Hajed A. Alotaibi. "Clarifying Heirs' Rights in Indonesian Waqf Law: Toward Stronger Governance and Conflict Prevention." *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat* 25, no. 2 (2025): 529–553. https://doi.org/10.19109/nurani.v25i2.30356.

Alharthi, Saud H., and Alotaibi, Hajed A. "Harmonising Legal and Sharia Principles in Foreign Investment: The Regulatory Framework of Subsidiaries in Saudi Arabia." *Legality : Jurnal Ilmiah Hukum* 34, no. 1 (2026): 162–82. https://doi.org/10.22219/ljih.v34i1.42145.

Alotaibi, H. A. (2022). Credit rating in the Islamic system: A case study of Saudi Arabian banks. Turkish Journal of Islamic Economics, 9(2), 99-116. https://doi.org/10.26414/A3403.

Alotaibi, Hajed A. *Islamic Legal Perspectives On Non-Fungible Tokens (Nfts)Exploring The Permissibility Of Non-Fungible Tokens (Nfts) As Digital Assets Under Islamic Law*. January 1, 2025. https://www.academia.edu/130253762/

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890
Alotaibi HA and Alotaibi MT. Professional Boundaries and Ethical Obligations in Saudi Arabia An Integrated Sharia, Legal and Clinical Psychology Framework. F1000Research 2026, 15:461 (https://doi.org/10.12688/f1000research.178561.2)

Armia, Muhammad Siddiq. "Implementing Islamic Constitutionalism: How Islamic Is Indonesia Constitution?" *Al-'Adalah* 15, no. 2 (2018): 349–368. https://doi.org/10.24042/adalah.v15i2.3389.

Auda, Jasser. *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach*. International Institute of Islamic Thought, 2008. https://doi.org/10.2307/j.ctvkc67tg.

Azam, Muhammad, Naji Mohammad Alwreikat, Burhan Alsyouf, Abdel Salam Atwa Ali Al Fandi, and Rawdah Abdul Karim Mohammad Pharaon. "Contemporary Trade Governance and Cross-Border Data Flows: A Comparative Study of *Sharīʿah* Principles and International Legal Frameworks." *MILRev: Metro Islamic Law Review* 5, no. 1 (2026): 686–721. https://doi.org/10.32332/milrev.v5i1.13387.

Boateng FD, Pryce DK, Alotaibi H, "Procedural justice, obligation to obey and cooperation with police in a sample of Saudi Arabian citizens". *Policing: An International Journal*, Vol. 48 No. 5 (2025): 1135–1151, doi: https://doi.org/10.1108/PIJPSM-03-2025-0058

Bunyamin, Bunyamin, Firdaus Arifin, Ihsanul Maarif, Robi Assadul Bahri, and Mohd Kamarulnizam Abdullah. "Reforming Indonesia's Correctional System: The Role of *Maqāṣid* Al-Syarīʿah in Ensuring Justice and Rehabilitation." *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 52–71. https://doi.org/10.18860/j-fsh.v17i1.29258.

Cordoba, Alfredo, and Nadia Haider. "Engineering for Ethics: Moral Systems Analysis in Digital Governance." *Journal of Technology and Society* 17, no. 2 (2024): 45–63.

Digital Government Authority. *Annual Performance Report on Digital Transformation*. DGA, 2026.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Digital Government Authority. *Digital Trust Services Regulation*. DGA, 2025.

Dokumen.Pub. "Principles of Islamic Jurisprudence 3." Accessed May 25, 2026. https://dokumen.pub/principles-of-islamic-jurisprudence-3.html.

Haider, Aftab, Naim Mathlouthi, Mahmud Zuhdi Mohd Nor, Musda Asmara, Asif Khan, and Ramadhita. "From Stewardship to Sustainability: A Comparative Analysis of Islamic Ecological Jurisprudence and Western Anthropocentric Regimes." *JURIS (Jurnal Ilmiah Syariah)* 25, no. 1 (2026): 41–60. https://doi.org/10.31958/juris.v25i1.16040.

Hallaq, Wael B. *Sharīʿa: Theory, Practice, Transformations*. Cambridge University Press, 2009.

Hamdan, Lina. "Electronic Signatures and Evidentiary Law in the Gulf." *Arab Law Quarterly* 37, no. 3 (2023): 411–428.

Hamzah, Moh, Eka Susylawati, Erie Hariyanto, Moh Zahid, Rudy Haryanto, and Masrufah Masrufah. "The Transformation of Electronic Mediation: A Legal Innovation in the Sharia Economic Dispute Resolution." *JURIS (Jurnal Ilmiah Syariah)* 25, no. 1 (2026): 15–27. https://doi.org/10.31958/juris.v25i1.15856.

Humaidi, M. Wildan, Ridwan, and Mohd Mahyeddin Mohd Mohd Salleh. "State-Religion Relations and Halal Governance: Islamic Legal Policy in Indonesia and Malaysia." *Al-Manahij: Jurnal Kajian Hukum Islam* 20, no. 1 (2026): 1–20. https://doi.org/10.24090/mnh.v20i1.

Ibn Qudāmah. *Al Mughnī*. Vol. 10. Dār al Fikr, 1984.

Ibrahim, Tuan Muhammad Faris Hamzi Tuan, Nasrul Hisyam Nor Muhamad, Mohamad Aniq Aiman Alias, and Ahmad Syukran Baharuddin. "The Role of Digital Forensics as Qarinah Muasirah in Proving Cyber Offences Under Malaysian Islamic Evidence Law." *Al-Istinbath: Jurnal Hukum Islam* 11, no. 1 (2026): 19–39. https://doi.org/10.29240/jhi.v11i1.14738.

Iskandar, Rauzatul Jannah, Burhan Uluyol, Hussein' Azeemi Abdullah Thaidi, and Siti Najma. "The Influence of Green Financing and Return Dynamics on

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

Environmental, Social, and Governance Performance: Evidence from Indonesia's Islamic Banking Sector." *Al-Muamalat* 13, no. 1 (2026): 169–185. https://doi.org/10.15575/am.v13i1.54428.

Itmam, Muhammad Shohibul, Sirajul Munir, Lukman Santoso, Taufikin, and Abdelmalek Aouich. "Legal Politics of Mining Spatial Planning in Sumenep District: *Maqāṣid* Syarī'ah Overview." *Ijtihad : Jurnal Wacana Hukum Islam Dan Kemanusiaan* 25, no. 1 (2025): 1–27. https://doi.org/10.18326/ijtihad.v25i1.1-27.

Latif, Shamsul, and Wan Shamsuddin. "*Maqāṣid* Driven Digital Governance in Muslim Jurisdictions: Lessons from Malaysia and Indonesia." *Asian Journal of Law and Society* 10, no. 4 (2023): 870–894.

Mahmod, Tarek El Sayed, Khalid awad hammadi Al –Alwani, Ismael Hellawss, Mahmood Shaker Alaloosh, and Salah Ragab Fathelbab. "Regulatory Gaps in Digital Witness Protection for Cybercrime: Integrating International Standards, Egyptian Law, and Islamic Jurisprudence." *Al-Istinbath: Jurnal Hukum Islam* 11, no. 1 (2026): 158–92. https://doi.org/10.29240/jhi.v11i1.16326.

Ministry of Justice (KSA). *Annual Judicial Statistics Report 2025*. Ministry of Justice, 2025.

Ministry of Justice (KSA). *Civil Transactions Law*. Ministry of Justice, 2024.

Ministry of Justice (KSA). *Judiciary Statistics and Digital Performance Report 2025*. Ministry of Justice, 2025.

Ministry of Justice (KSA). *Law of Evidence*. Ministry of Justice, 2022.

Nasim, Arim, Elfina Qorina Binti Asbaruna, Juliana Juliana, et al. "Driving *Maqāṣid* Al-Shari'ah Performance in Islamic Banks: The Roles of Islamic Social Reporting, Intellectual Capital, and Sharia Governance." *Al-Muamalat* 13, no. 1 (2026): 102–118. https://doi.org/10.15575/am.v13i1.54396.

Ramdlany, Ahmad Agus, Ahmad Musadad, Hammis Syafaq, Maher Ali Ahmad Al-Khaldi, and Saleem Asouli. "Integrating *Fiqh*iyyah Legal Maxims and Positive Law Principles in the Formation of Indonesia's New National Criminal Code." *Nusantara: Journal*

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890

of Law Studies 5, no. 1 (2026): 453–484. https://doi.org/10.66325/nusantaralaw.v5i1.156.

Rashid, Khalid. "Reforming Islamic Finance: A Framework for a Proposed Non-Banking Institution to Facilitate Participative Financing." *Al-Muamalat* 13, no. 1 (2026): 146–168. https://doi.org/10.15575/am.v13i1.53042.

Raysūnī, Ahmad. *Al Fiqh al Islāmī Wa Maqāṣid al Sharīʿah al ʿĀmmah [Islamic Jurisprudence and the Objectives of Islamic Law]*. Al Markaz al ʿArabī, 2013.

Riady, Roy, Febrian Febrian, Nashriana Nashriana, and M. Yusuf. "Reformulating the Reversal of the Burden of Proof in Corruption Cases: Integrating Positive Law and Islamic Legal Principles." *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat* 25, no. 2 (2025): 514–528. https://doi.org/10.19109/nurani.v25i2.30483.

Rosenbach, Eric. "Value Neutral Tech Law and Its Limits: An Ethical Audit." *Policy Review* 189, no. 4 (2022): 33–50.

Saudi Data and AI Authority (SDAIA). *Ethical AI Guidelines 2025*. SDAIA, 2025.

Sharia: Theory, Practice, Transformations by Wael B. Hallaq. Cambridge University Press, n.d.

Shoimah, Siti Nur. "Freedom of Contract in the Digital Age: Perspectives on the Indonesian Civil Code and *Fiqh* Muamalah." *Trunojoyo Law Review* 8, no. 1 (2026): 59–94. https://doi.org/10.21107/tlr.v8i1.32568.

Sofiani, Trianah, Shofian bin Ahmad, Bunga Desyana Pratami, and Heris Suhendar. "Mosques as Catalysts for Islamic Financial Inclusion: Evidence from Branchless Banking Implementations." *Asy-Syari'ah: Jurnal Hukum Islam* 27, no. 2 (2025): 143–170. https://doi.org/10.15575/as.v27i2.48309.

Sunaryo, Sidik, Shinta Ayu Purnamawati, Muhammad Jihadi, and Sholahuddin Al-Fatih. "The Narrating Ontology Morality of Corruption Law in Indonesia Based on Islamic Value." *Jurnal Hukum Fakultas Hukum Unissula* 4, no. 1 (2025): 133–156. https://doi.org/10.26532/jh.v41i1.37154.

MILRev : Metro Islamic Law Review
ISSN: 2986-528X
Vol. 5 No. 1 January-June 2026, Pages 845-890
Syifa, Siti, Muhammad Abdillah, and Fadil SJ. "The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak: Integration of Personal Data Protection Laws and the Principle of Sadd al-Dharī'At." *Justicia Islamica* 22 (July 2025): 185–210. https://doi.org/10.21154/justicia.v22i1.10390.

Tutik, Titik Triwulan, Kunawi Basyir, Mahtumridho Ghufron Bin Simun, Jauharoti Alfin, and M. Suyudi. "Reconstructing Eco-*Maqāṣid* al-Sharī'ah for CSR Policy and Radioactive Waste Management: An SDGs-Based Study in Banten and West Java." *Al-Manahij: Jurnal Kajian Hukum Islam* 20, no. 1 (2026): 115–132. https://doi.org/10.24090/mnh.v20i1.

Valverde, Sonia, and Graham Greenleaf. "Understanding Legal Culture in Cybersecurity Legislation: Beyond Technical Neutrality." *International Data Law Journal* 9, no. 1 (2023): 21–46.

Zuḥaylī, Muḥammad Muṣṭafá. *al-Qawā'id al-fiqhīyah wa-taṭbīqātuhā fī al-madhāhib al-arba'ah*. Al-Ṭab'ah 1. Dār al-Fikr, 2006.

.