Justicia Islamica: Jurnal Kajian Hukum dan Sosial
Vol 23 No 1, June 2026

Evidentiary Challenges in AI-Mediated E-Commerce Disputes: Comparative Perspectives from the EU, US, GCC, and Islamic Law

***Shatha Ismaeel*,[1*] *Khalid Alammari*,[2] *Zinah Ghanim Younus*[3]**
[1] College of Law, Prince Mohammad bin Fahd University, Saudi Arabia
[2] College of Law, Prince Mohammad bin Fahd University, Saudi Arabia
[3] College of Law, Nineveh University, Mosul, Iraq

[*]*Corresponding Author*: *sismaeel@pmu.edu.sa*

DOI: https://doi.org/10.21154/justicia.v23i1.11809
Received: *August 10, 2025* | *Revised*: *Nov 16, 2025* | *Accepted*: *Jan 27, 2026*

Abstract: This article aims to analyse the use of artificial intelligence (AI) as an intermediary in e-commerce transactions, thereby increasing the challenges of proving damages, particularly due to algorithmic opacity, system autonomy, and the fragmentation of legal liability subjects. Using a comparative legal approach in the European Union, the United States, and Saudi Arabia in the context of the Gulf Cooperation Council (GCC), with Islamic law as an autonomous regime of proof. Using a doctrinal comparative method, the study analyses statutory instruments, judicial practices, and emerging AI regulatory initiatives to evaluate how different legal systems address evidentiary burdens and liability attribution in AI-mediated disputes. The findings demonstrate that the European Union adopts a preventive, risk-based approach to digital evidence and accountability. In contrast, the United States relies on an ex-post, fault-oriented, and fragmented adjudicatory model. In contrast, Saudi Arabia and the broader GCC remain in a transitional phase, gradually integrating electronic evidence into civil law without a comprehensive AI-specific liability framework. Crucially, the article argues that Islamic law offers a coherent and independent evidentiary framework grounded in principles such as *bayyinah*, *qarīnah*, moral accountability (*amānah*), and harm prevention (*lā ḍarar*), which are particularly relevant in addressing AI opacity by treating AI outputs as corroborative rather than determinative proof. The study proposes doctrinal and evidentiary reforms that integrate comparative legal insights with Islamic jurisprudence to enhance legal certainty, justice, and accountability in AI-driven e-commerce disputes.
Keywords: e-commerce; legal liability; digital evidence; AI intermediaries; legal reform.

Abstrak: Artikel ini bertujuan menganalisis penggunaan kecerdasan buatan (*Artificial Intelligence*/AI) sebagai perantara dalam transaksi e-commerce, sehingga memperbesar tantangan pembuktian kerugian, terutama akibat opasitas

algoritmik, otonomi sistem, dan terfragmentasinya subjek tanggung jawab hukum. Dengan menggunakan pendekatan hukum komparatif di Uni Eropa, Amerika Serikat, serta Arab Saudi dalam konteks Dewan Kerja Sama Teluk (*Gulf Cooperation Council/GCC*), dengan menempatkan hukum Islam sebagai rezim pembuktian yang berdiri otonom. Penelitian ini menggunakan metode doktrinal komparatif dengan menelaah peraturan perundang-undangan, praktik peradilan, dan inisiatif regulasi AI untuk menilai bagaimana berbagai sistem hukum mengatur beban pembuktian dan tanggung jawab dalam sengketa e-commerce berbasis AI. Hasil penelitian menunjukkan bahwa Uni Eropa menerapkan pendekatan preventif berbasis risiko, Amerika Serikat mempertahankan model pembuktian ex post yang berorientasi pada kesalahan, sementara Arab Saudi dan kawasan GCC masih berada pada tahap transisi dalam pengakuan bukti elektronik tanpa kerangka tanggung jawab AI yang komprehensif. Lebih lanjut, artikel ini menegaskan bahwa hukum Islam memiliki kerangka pembuktian yang sistematis melalui konsep *bayyinah*, *qarīnah*, *amānah*, dan prinsip pencegahan mudarat (*lā ḍarar*), yang relevan untuk merespons opasitas AI dengan menempatkan keluaran AI sebagai indikasi pendukung, bukan bukti utama. Studi ini menawarkan reformasi doktrinal dan pembuktian yang mengintegrasikan hukum komparatif dan hukum Islam guna memperkuat keadilan dan kepastian hukum dalam sengketa e-commerce berbasis AI.
Kata Kunci: e-commerce; tanggung jawab hukum; bukti digital; perantara AI; reformasi hukum.

Introduction

Artificial intelligence (AI) has become a transformative force in global e-commerce, driving innovation in digital transactions, consumer personalisation, and operational efficiency. Recent industry reports indicate that AI-driven recommendation systems account for more than 35% of consumer purchases on leading platforms such as Amazon and Alibaba, illustrating the profound economic and social impact of this technology.[1] Yet alongside these benefits, the deployment of AI raises pressing legal concerns, particularly regarding liability, evidentiary standards, and fault attribution in

[1] OECD, *Artificial Intelligence in Society* (OECD Publishing, 2019), https://doi.org/10.1787/eedfee77-en; Ransome Epie Bawack et al., "Artificial Intelligence in E-Commerce: A Bibliometric Study and Literature Review," *Electronic Markets* 32, no. 1 (March 2022): 297–338, https://doi.org/10.1007/s12525-022-00537-z.

disputes involving AI intermediaries. For example, in *Loomis v. Wisconsin* 2016,[2] an algorithmic risk-assessment tool influenced a criminal sentencing decision, sparking debate over transparency and accountability in automated decision-making. Similarly, the 2021 case of the Dutch "Toeslagenaffaire" (Childcare Benefits Scandal) revealed how biased AI-driven systems used by tax authorities led to unjustified penalties against thousands of families, emphasising the risks of unregulated algorithmic governance.[3] In the e-commerce context, Amazon faced legal scrutiny when an AI-powered recommendation engine facilitated the sale of defective hoverboards linked to fire hazards, prompting questions about product liability for algorithmic actions.[4] These cases demonstrate the urgent need for coherent legal frameworks to govern the evidentiary and liability dimensions of AI systems, ensuring that innovation does not outpace accountability.

Existing scholarship has examined the intersection of artificial intelligence (AI) and law from multiple perspectives, primarily focusing on transparency, accountability, and algorithmic bias.[5] Early works emphasised the need for explainable AI to ensure procedural fairness and uphold due process rights. In contrast, others explored the ethical and regulatory implications of autonomous decision-making in both public and private sectors.[6] In the field of liability, researchers analysed whether existing tort and product liability doctrines are sufficient to address harms caused by

---

2 Marc Levin, "881 NW 2d 749 (Wis. 2016). Judges rightly view sentencing as a weighty responsibility. They must consider not only the appropriate punishment for the offense but also the risk the offender poses, predicting the probability of the of-fender's recidivism. 2 A potential solution to this judicial anxiety has."

3 Philipp Hacker, Johann Cordes, and Janina Rochon, "Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond," *European Journal of Risk Regulation* 15, no. 1 (March 2024): 49–86, https://doi.org/10.1017/err.2023.81.

4 Fatma Abudaqqa, "Artificial Intelligence for IT Governance in Saudi Arabia: Opportunities, Challenges, and Future Directions within COBIT 2019 and ISO/IEC 38500 Frameworks," *European Scientific Journal, ESJ* 21, no. 25 (September 2025): 157, https://doi.org/10.19044/esj.2025.v21n25p125.

5 Seyedeh Negin Malja and Hossein Afrasiabi, "Artificial Intelligence and Society: Mapping the Research through a Systematic Review," *AI & SOCIETY*, ahead of print, September 8, 2025, https://doi.org/10.1007/s00146-025-02555-9.

6 Aybike Mergen, Nergiz Çetin-Kılıç, and Mustafa F. Özbilgin, "Artificial Intelligence and Bias Towards Marginalised Groups: Theoretical Roots and Challenges," in *AI and Diversity in a Datafied World of Work: Will the Future of Work Be Inclusive?*, vol. 12, ed. Joana Vassilopoulou and Olivia Kyriakidou (Emerald Publishing Limited, 2025), 17–38, https://doi.org/10.1108/S2051-233320250000012004. Emerald Publishing Limited, 2025.

autonomous systems, proposing hybrid models of human–machine accountability.[7] Comparative analyses have also begun to emerge: European scholars have discussed the implications of the EU AI Act and its risk-based approach to liability. At the same time, Anglo-American literature has centred on negligence and foreseeability principles in AI-mediated harm.[8]

However, despite this growing body of research, much of the literature remains descriptive, focusing on normative debates rather than empirical or doctrinal assessments of liability frameworks across jurisdictions. Few studies systematically address the evidentiary complexities of proving causation and damages in AI-driven environments, especially within civil and commercial disputes. Moreover, cross-jurisdictional comparisons between common law and Sharia-influenced systems remain scarce, leaving a critical gap in understanding how legal doctrines adapt to AI-mediated decision-making in non-Western contexts. This study seeks to fill that gap by providing a comparative doctrinal analysis of liability and evidentiary rules in selected jurisdictions, identifying shortcomings, and proposing legal reforms to enhance accountability and procedural justice in the age of AI.

The objective of this research is to assess the adequacy of current legal responses to AI in e-commerce, with a focus on liability, causation, and digital evidence. To achieve this, the article employs a comparative legal methodology, drawing on doctrinal analysis of statutory texts, judicial decisions, and regulatory instruments in the European Union, the United States, and Saudi Arabia within the Gulf Cooperation Council (GCC).[9] This selection enables the examination of three distinct legal models: the EU's harmonised, risk-based regulatory approach, the U.S.'s sectoral, fault-oriented framework, and the GCC's emerging yet still fragmented legal landscape.

---

7 Pinchas Huberman, "Tort Law, Corrective Justice and the Problem of Autonomous-Machine-Caused Harm," *Canadian Journal of Law & Jurisprudence* 34, no. 1 (February 2021): 105–47, https://doi.org/10.1017/cjlj.2020.3.

8 W. Michael Schuster, Joseph Avery, and Camilla Alexandra Hrdy, "The AI Penalty in Trade Secret Law," SSRN Scholarly Paper no. 5610270 (Rochester, NY: Social Science Research Network, June 1, 2025), https://doi.org/10.2139/ssrn.5610270. 71.

9 Shaping Europe's digital future, "Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence," April 21, 2021, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence; Matúš Mesarčík et al., "Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence Act," preprint, SocArXiv, March 9, 2022, https://doi.org/10.31235/osf.io/yzfg8.

The contribution of this study lies in its effort to systematise the literature, clarify the doctrinal and evidentiary challenges posed by AI in e-commerce, and propose reforms that can enhance legal certainty and fairness. By comparing diverse jurisdictions, the article does not address an underexplored research gap but also offers recommendations that may inform future regional and international regulatory harmonisation.

This study adopts a comparative doctrinal legal methodology to examine the challenges of liability and evidentiary rules in e-commerce disputes involving artificial intelligence (AI). The doctrinal approach involves the systematic analysis of statutory provisions, judicial decisions, and regulatory instruments to identify how different legal systems conceptualise and respond to disputes arising from AI intermediaries. The comparative dimension focuses on the European Union, the United States, and Saudi Arabia within the broader Gulf Cooperation Council (GCC), representing three distinct regulatory models: a harmonised and risk-based framework (EU), a sectoral and fault-oriented approach (US), and an emerging regulatory landscape (Saudi Arabia/GCC). The research draws on both primary legal sources—such as legislation, case law, and international conventions—and secondary literature, including academic commentary, policy reports, and institutional guidelines. Through this methodology, the article evaluates doctrinal consistency and divergence, highlights evidentiary gaps, and develops reform-oriented proposals to enhance legal certainty and fairness in AI-driven commerce.

The Role of AI Intermediaries in E-Commerce:

In the emerging landscape of e-commerce, AI intermediaries have become pivotal agents that blur the boundary between the traditional seller-customer relationship and digitise many commercial transactions. Such systems, which range from algorithm-based recommendation advisories and customised ad-generation systems to self-executing contract negotiation agents, mediate interactions between consumers and providers with degrees of autonomy and data-measuredness.[10] Using machine learning, AI intermediaries analyse large

[10] Kate Crawford and Ryan Calo, "There Is a Blind Spot in AI Research," *Nature* 538, no. 7625 (October 2016): 311–13, https://doi.org/10.1038/538311a; Nur Amalyna Yusrin, "Ai-Powered E-Commerce: Elevating E-Service Quality Through Utilitarian And Hedonic With E-Satisfaction As The Bridge To E-Loyalty," *Jurnal Multidisiplin Sahombu* 5, no. 01 (January 2025): 216–31.

datasets in real time to increase profitability, forecast shopper behaviour, and influence purchase decisions. For example, innovative recommendation systems can recommend products based on a user's browsing history, stagger them, and cause contracts without active negotiation, raising issues of informed consent and consumer autonomy.[11]

Moreover, AI intermediaries are not neutral pipelines of information; they are often endowed with decision-making powers that influence the legal outcome, for example, by proposing dynamic pricing to some individuals based on profiling or automatically activating contract terms, acting here as quasi-legal agents in the e-commerce transaction chain.[12] This abdication of decision-making responsibility to non-human agents confronts conventional legal conceptions of agency, intentionality, and liability, notably when the reasoning behind AI behaviour is opaque and not explainable to end-users or, indeed, developers.[13]

Indeed, as AI intermediaries become key determinants of the digital economy, they generate information asymmetries that may erode consumer protection principles if they are not correctly managed.[14] The growing complexity and opacity of these systems, with the conditions under which they are deployed, would require a reinvention of legal models for holding account in an era when harm can arise from non-human interventions.

---

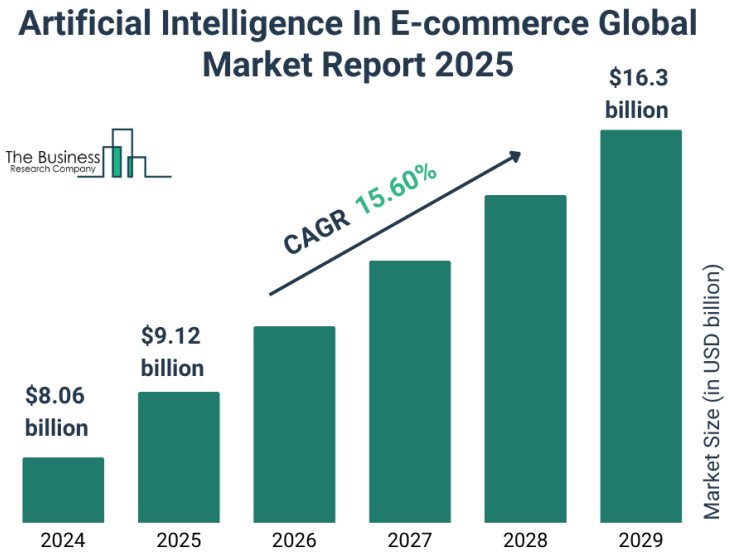
[11] Alan Rubel, "The Black Box Society: The Secret Algorithms That Control Money and Information, by Frank Pasquale. Cambridge: Harvard University Press, 2015. 320 Pp. ISBN 978–0674368279," *Business Ethics Quarterly* 26, no. 4 (October 2016): 568–71, https://doi.org/10.1017/beq.2016.50; "The Black Box Society: The Secret Algorithms That Control Money and Information," *Contemporary Sociology* 45, no. 3 (May 2016): 367–68, https://doi.org/10.1177/0094306116641409c.

[12] Philipp Hacker and Jan-Hendrik Passoth, "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond," in *xxAI - Beyond Explainable AI: International Workshop, Held in Conjunction with ICML 2020, July 18, 2020, Vienna, Austria, Revised and Extended Papers*, ed. Andreas Holzinger et al. (Cham: Springer International Publishing, 2022), 17, https://doi.org/10.1007/978-3-031-04083-2_17.

[13] European Commission, "Proposal for a Regulation of the European Parliament and of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts," 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

[14] Karen Yeung, "Algorithmic Regulation: A Critical Interrogation," *Regulation & Governance* 12, no. 4 (2018): 505–23, https://doi.org/10.1111/rego.12158.

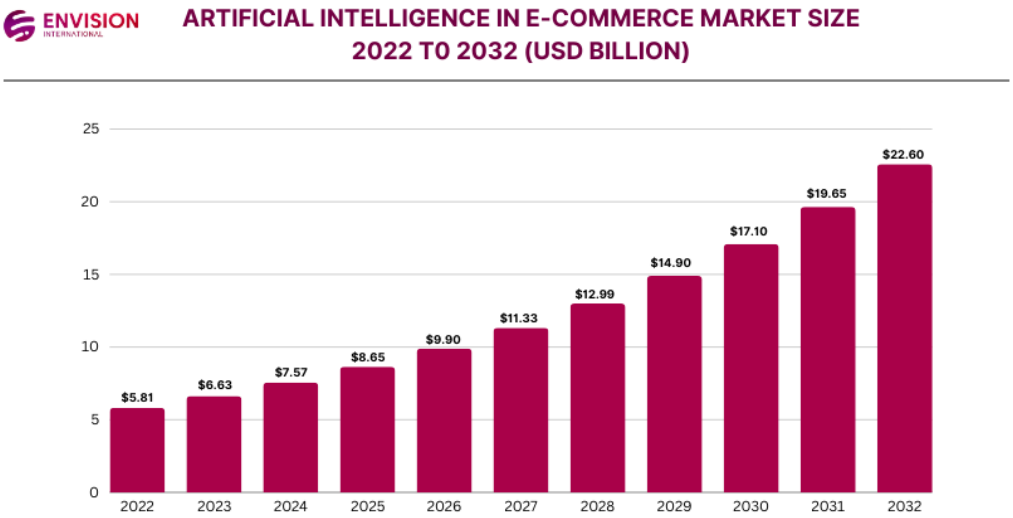
Figure 1. Global Market Report 2025



Source: https://www.thebusinessresearchcompany.com, 2025

Resource: The Business Research Company, "Artificial Intelligence in E-commerce Global Market Report 2025." The global AI in e-commerce market is projected to grow from US $8.06 billion in 2024 to US $16.42 billion by 2029, at a CAGR of 15.6 %.[15]

Figure 2. Market Size



Source: Envision Int, 2025.

[15] Envision Market Insights, "Artificial intelligence in e-commerce market size 2022 to 2032 (USD billion) [Graph]. Envision Market Insights. (2023). Retrieved from https://envisioninteligence.com

Algorithmic Opacity, Causation, and Moral Accountability in Proving AI-Related Damage

With the increasing integration of AI into numerous aspects of life, legal systems in coordination with governments are grappling with how to address the unique problems posed by AI-related disputes.[16] Among the central issues in establishing AI liability is the opacity and complexity of these systems. The "black box" nature of AI makes it difficult to determine how harm occurs, complicating conventional legal concepts such as causation, defect, and breach. In addition, liability may involve multiple parties—including users, deployers, and developers—making the allocation of responsibility particularly challenging.[17]

Although recent AI developments have had positive global impacts, their rapid growth has outpaced the creation of robust accountability frameworks, resulting in a fragmented landscape of approaches, each with strengths and limitations. For example, the principal–agent model assigns liability to professionals supervising the AI system, but this may discourage adoption, as practitioners may be reluctant to accept responsibility for failures beyond their understanding or control.[18] Similarly, the product liability paradigm holds entities in the AI supply chain accountable.[19] Yet, AI's unpredictability and the opacity of its systems often make it difficult to prove specific defects, thereby undermining the effectiveness of this model.

Beyond liability, the risks of bias in AI systems highlight further social and legal concerns. AI bias refers to the unjust treatment of individuals based on

---

[16] Sruthi Rajendran and Akshay Dinesh Kumar, "Liability for Harm Caused by AI: Examining the Legal Responsibility for the Actions of Autonomous Systems | International Journal of Law Management & Humanities," *International Journal of Law Management and Humanities* 6, no. 2 (2023): 214–24, https://doij.org/10.10000/IJLMH.114348; Anna Nicolis, Nigel Kingsman, and Hughes Hall, *AI Explainability in the EU AI Act: A Case for an NLE Approach Towards Pragmatic Explanations*, 1, no. 1 (July 2024).

[17] Fatemeh Kiani and Alireza Shafiee, "Global Harmonization of AI Regulation: Addressing Cross-Border Challenges in Ethical Standards, Accountability, and Liability," *Legal Studies in Digital Age* 1, no. 1 (October 2022): 14–26.

[18] Femi Osasona et al., "Reviewing The Ethical Implications Of AI In Decision Making Processes," *International Journal of Management & Entrepreneurship Research* 6, no. 2 (February 2024): 322–35, https://doi.org/10.51594/ijmer.v6i2.773; Anne David et al., "Public Perceptions of Responsible AI in Local Government: A Multi-Country Study Using the Theory of Planned Behaviour," *Government Information Quarterly* 42, no. 3 (September 2025): 102054, https://doi.org/10.1016/j.giq.2025.102054.

[19] OECD, *Artificial Intelligence in Society* (OECD Publishing, 2019), https://doi.org/10.1787/eedfee77-en.

gender, race, or other protected traits. This can manifest in discriminatory practices such as biased loan approvals, unfair recruitment, or even life-threatening errors in autonomous vehicles.[20] A well-known study by Microsoft and MIT researchers revealed substantial gender and racial biases in facial recognition systems, which misidentified women with darker skin tones at higher rates than lighter-skinned men.[21] If such systems were deployed in law enforcement, innocent individuals from minority groups could be wrongly targeted solely based on appearance. Courts have already begun grappling with these challenges. For instance, in 2019, a court ruled against an insurer that relied solely on an AI algorithm to determine medical coverage, finding that it unjustly denied claims for individuals with mental health conditions. Such cases demonstrate a growing recognition of the need for accountability and fairness in AI systems.

For Muslim societies, however, these evidentiary and liability issues must also be examined in light of Islamic law. The principles of *bayyinah* (evidence) and *shahādah* (testimony) strongly emphasise authenticity, honesty, and justice (*'adl*), requiring that evidence be presented by a morally accountable human subject.[22] AI-generated outputs, including deepfakes and algorithmically produced decisions, lack the moral agency necessary to bear witness, raising questions about whether they can satisfy Islamic evidentiary requirements. Classical jurists consistently emphasised that valid testimony requires a witness with moral integrity (*'adālah*) and the capacity for truthfulness (*sidq*).[23] This suggests that AI-based evidence, while useful as a supporting tool, may not, on its own, meet the threshold of *bayyinah* in Islamic

---

[20] Miriam Buiten, Alexandre de Streel, and Martin Peitz, "The Law and Economics of AI Liability," *Computer Law & Security Review* 48 (April 2023): 105794, https://doi.org/10.1016/j.clsr.2023.105794.

[21] Sruthi Rajendran and Akshay Dinesh Kumar, "Liability for Harm Caused by AI: Examining the Legal Responsibility for the Actions of Autonomous Systems," *International Journal of Law Management & Humanities* 6, no. 2 (2023): 214–24, https://doij.org/10.10000/IJLMH.114348; Dane Bottomley and Donrich Thaldar, "Liability for Harm Caused by AI in Healthcare: An Overview of the Core Legal Concepts," *Frontiers in Pharmacology* 14 (December 2023), https://doi.org/10.3389/fphar.2023.1297353.

[22] Hafsa Abbasi, Summayyah Summayyah, and Syed Naeem Badshah, "English-5 Principles of Electronic Evidence in Sharī'Ah and Law-A Comparative Study," *Al-Aijaz Research Journal of Islamic Studies & Humanities* 5, no. 2 (June 2021): 50–67, https://doi.org/10.53575/English5.v5.02(21).50-67.

[23] Hijrian Angga Prihantoro, "Examining Witness Interest: The Obstacles of Testimony in Islamic Jurisprudence and Positive Law," *Justicia Islamica* 21, no. 1 (June 2024): 1–22, https://doi.org/10.21154/justicia.v21i1.8653.

jurisprudence. Modern Islamic legal scholars echo this concern, stressing that digital or AI-generated evidence must be carefully scrutinised for reliability, authenticity, and chain of custody before it can be reconciled with Shari'ah principles.[24] Thus, while international legal systems debate liability and causation, Muslim-majority jurisdictions face the additional normative challenge of reconciling AI-based evidence with Islamic rules of testimony. This raises more profound questions about the legitimacy and fairness in balancing transparency, innovation, and accountability.[25]

Evidentiary and Contractual Uncertainty in AI-Mediated E-Commerce

With the increasing integration of AI into numerous aspects of life, legal systems in coordination with governments are grappling with how to address the unique problems posed by AI-related disputes.[26] Among the central issues in establishing AI liability is the opacity and complexity of these systems. The "black box" nature of AI makes it difficult to determine how harm occurred, complicating conventional legal concepts such as causation, defect, and breach. In addition, liability may involve multiple parties—including users, deployers, and developers—making the allocation of responsibility particularly challenging.[27] From a socio-legal perspective, these complexities extend beyond technical liability to affect consumer rights and trust in e-commerce transactions, particularly where contracts are standardised and heavily mediated by AI.

Although recent AI developments have had positive global impacts, their rapid growth has outpaced the creation of robust accountability frameworks, resulting in a fragmented landscape of approaches, each with strengths and limitations. For example, the principal–agent model assigns liability to professionals supervising the AI system, but this may discourage adoption, as practitioners may be reluctant to accept responsibility for failures beyond their

---

[24] Mohammad Hashim Kamali, "Between Separation and Unity: The Interplay of Law and Morality in Islamic Jurisprudence," in *Sharia Law in the Twenty-First Century*, by Muhammad Khalid Masud and Hana Jalloul Muro (WORLD SCIENTIFIC (EUROPE), 2022), 21–46, https://doi.org/10.1142/9781800611689_0002.

[25] Sargiotis Dimitrios, "Ethical AI in Information Technology: Navigating Bias, Privacy, Transparency, and Accountability," *Advances in Machine Learning and Artificial Intelligence* 5, no. 3 (2024): 1–14.

[26] Sruthi Rajendran and Akshay Dinesh Kumar, "Liability for Harm Caused by AI." 13.

[27] Fatemeh and Shafiee, "Global harmonization of AI regulation." 14-26.

understanding or control.[28] Similarly, the product liability paradigm holds entities in the AI supply chain accountable.[29] Yet, AI's unpredictability and opacity often make it difficult to prove specific defects, undermining the effectiveness of this model. Within Islamic contract law (*fiqh al-muʿāmalāt*), however, the validity of contracts (*ʿaqd/akad*) rests on the principles of clarity, fairness, and the avoidance of *gharar* (excessive uncertainty). Shaleh stressed that contracts should define their subject matter, rights, and obligations with sufficient precision to prevent ambiguity.[30] Opaque AI systems, where inputs and outputs are difficult to interpret, raise the question of whether reliance on such systems in digital contracts introduces uncertainty that falls within the prohibition of *gharar* as articulated in Islamic jurisprudence.

Beyond liability, the risks of bias in AI systems highlight further concerns from both legal and social perspectives. AI bias refers to the unjust treatment of individuals based on gender, race, or other protected traits, which can manifest in discriminatory practices such as biased loan approvals, unfair recruitment, or even life-threatening errors in autonomous vehicles.[31] A study by Microsoft and MIT researchers revealed substantial gender and racial biases in facial recognition systems, which misidentified women with darker skin tones at higher rates than lighter-skinned men.[32] If such systems are integrated into e-commerce contracts, Muslim consumers could face unfair treatment in access to services, pricing, or eligibility assessments, undermining the Islamic legal principle of fairness (*ʿadl*).[33] Courts have already begun addressing such issues. For instance, in 2019, a court ruled against an insurer that relied solely on an AI algorithm to determine medical coverage, finding that it unjustly

---

[28] Nikos Th. Nikolinakos, "Reforming the EU Civil Liability Framework Applicable to Artificial Intelligence and Other Emerging Digital Technologies: Defective Products—the Revised Product Liability Directive," in *Adapting the EU Civil Liability Regime to the Digital Age: Artificial Intelligence, Robotics, and Other Emerging Technologies*, vol. 68, by Nikos Th. Nikolinakos, Law, Governance and Technology Series (Cham: Springer International Publishing, 2024), 477–621, https://doi.org/10.1007/978-3-031-67969-8_9.

[29] OECD, *Artificial Intelligence in Society* (OECD Publishing, 2019).

[30] Ahmad Syukri Shaleh, "Ibn Taymiyya's Concept of Istiḥsān : An Understanding of Legal Reasoning in Islamic Jurisprudence" (Thesis, McGill University, 1995), http://digitool.Library.McGill.CA:80/R/?func=dbin-jump-full&object_id=23241.

[31] M. Buiten, A. De Streel, and M. Peitz, "The Law and Economics of AI Liability," *Computer Law & Security Review* 48 (2023): 105794, https://doi.org/10.1016/j.clsr.2023.105794. 13.

[32] Sruthi Rajendran and Akshay Dinesh Kumar, "Liability for Harm Caused by AI." 61.

[33] Saudi Ministry of Commerce. "E-Commerce Law (Royal Decree No. M/126)." (2019).

denied claims for individuals with mental health conditions.[34] For Muslim-majority jurisdictions, the challenge is therefore twofold: not only ensuring accountability and fairness under modern legal standards, but also aligning AI-mediated contracts with Shariʿah principles that safeguard clarity, equity, and justice in transactions.

Contractual Ambiguities and Standard Terms in AI-Mediated E-Commerce

AI is complex because it involves numerous stakeholders and has highly interdependent components. The various elements of digital products, such as software, content, and hardware, may be manufactured and sold separately by multiple parties, making it challenging to identify the precise source of malfunction or to attribute liability to a single producer. Consumers may also face challenges proving why their AI-based products or services do not function properly, particularly when tangible goods are replaced by AI delivered as digital services. Irrespective of whether AI is offered as a product or service, multiple actors are typically involved in its provision and operation.

The involvement of multiple parties in liability is not new in law; for example, the European Union's existing liability frameworks already address complex products such as cars. However, the multi-actor ecosystem of AI raises sharper questions regarding the precise allocation of responsibilities for ensuring compatibility, safety, and accountability.[35] A related challenge arises from the interdependence of probabilistic and data-driven AI systems, where risks can escalate if components from different producers lack compatibility. Hardware devices, sensors, applications, software, and data services all interact, and these interlinked systems increase the likelihood of cascading failures and systemic vulnerabilities.[36] The opacity of AI adds another dimension of risk: injured parties may not realise they have been harmed, or may be unable to trace the harm back to a responsible actor. As AI becomes

---

[34] George Benneh Mensah, *Artificial Intelligence and Ethics*: A *Comprehensive Review of Bias Mitigation, Transparency, and Accountability in AI Systems*, version 1, 2023, https://doi.org/10.13140/RG.2.2.23381.19685/1.

[35] OECD, "*Artificial Intelligence in Society*."

[36] Alfonso Min, "Artifical Intelligence and Bias: Challenges, Implications, and Remedies," *Journal of Social Research* 2, no. 11 (2023): 3808–17.

more autonomous, accountability shifts further away from users and potentially even producers, creating legal uncertainty.[37]

From the perspective of Islamic contract law (*fiqh al-muʿāmalāt*), these challenges also raise critical normative issues. The concept of *ʻaqd* (contract) requires clarity in the subject matter, rights, and obligations of the parties to avoid *gharar* (excessive uncertainty). Opaque AI systems, where the relationship between input and output is difficult to understand, may therefore introduce contractual uncertainty that falls within the prohibition on *gharar*. In Islamic jurisprudence, contracts that involve significant ambiguity or unpredictability may be deemed invalid, as they undermine fairness (ʿadl) and transparency (ṣidq) between the parties.[38]

From a socio-legal perspective, biased AI-based service contracts present further concerns for Muslim consumers in e-commerce. Algorithmic bias in pricing, eligibility assessments, or service provision can unfairly disadvantage individuals based on race, gender, or other attributes.[39] In Muslim-majority contexts, this not only raises issues of consumer protection but also conflicts with Islamic principles of justice and fairness in transactions. Addressing such challenges requires not only adapting liability frameworks but also ensuring that AI-based contracts align with Shariʿah principles to safeguard clarity, equity, and consumer trust.

Comparative Legal Analysis of AI Liability and Evidentiary Standards in E-Commerce Disputes

The European Union has adopted a comprehensive ex-ante, risk-based framework under Regulation (EU) 2024/1689 – the Artificial Intelligence Act - which entered into force in August 2024 and has a staged applicability from 2025 to 2026.[40] The AI Act imposes upstream compliance duties designed to

---

[37] European Commission, "Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts."

[38] Hashim M Kamali, "*Principles of Islamic Jurisprudence*." 121.

[39] Buiten, De Streel, and Peitz, "The Law and Economics of AI Liability," 9; Sholahuddin Al-Fatih et al., "Artificial Intelligence in Indonesia's Financial Sector: Regulatory and Islamic Law Perspectives," *Justicia Islamica* 22, no. 2 (November 2025): 303–26, https://doi.org/10.21154/justicia.v22i2.10479.

[40] Nathalie Nevejans, "European Union's Regulation on the Placing on the Market and Use of AI Systems: A Critical Overview of the AI Act," in *Research Handbook on the Law of Artificial Intelligence*, ed.

mitigate risks before deployment, particularly for "high-risk" systems defined in Article 6 and Annexe III, encompassing applications in biometric identification, recruitment, credit scoring, education, and critical infrastructure.[41] Under Articles 8–15, providers of high-risk AI systems must implement rigorous risk-management, data-governance, and technical-documentation controls, ensure transparency and human oversight, and affix the CE conformity mark before placing systems on the market.[42] The Act also introduces obligations for General-Purpose AI (GPAI) models under Articles 52–55, mandating that developers disclose summaries of their training data, maintain cybersecurity standards, and respect copyright in datasets.[43]

Complementary guardrails stem from Article 22 of the General Data Protection Regulation (GDPR), which grants individuals the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. This provision, reinforced by Recitals 71 and 72 GDPR, anchors the principle of human oversight in AI decision-making.[44] On the ex post side, the EU modernised its product-liability regime through the 2024 Product Liability Directive (Directive (EU) 2024/..., replacing 85/374/EEC), which explicitly extends liability to software and AI components. Article 6(1)(f) defines "product" to include digital manufacturing files and AI software, ensuring compensation where an autonomous system causes damage.[45] Although the Proposal for an AI Liability Directive (COM/2022/496)

Woodrow Barfield and Ugo Pagallo (Edward Elgar Publishing, 2025), 489–540, https://doi.org/10.4337/9781035316496.00031..

41 Vladyslav Korshenko, "Risk Regulation Approach to Governing Artificial Intelligence on the Example of the EU's Artificial Intelligence Act / Submitted by Vladyslav Korshenko" (Thesis, University of Salzburg, 2024), 51, http://eplus.uni-salzburg.at/Abschlussarbeiten/9648422.

42 Ronit Justo-Hanani, "Risk-Based Approach to EU AI Act: Benefits and Challenges of Co-Regulation," *Policy Design and Practice*, January 2, 2026, world, https://www.tandfonline.com/doi/abs/10.1080/25741292.2025.2610869; Korshenko, "Risk Regulation Approach to Governing Artificial Intelligence on the Example of the EU's Artificial Intelligence Act / Submitted by Vladyslav Korshenko," 77.

43 Dao Gia Phuc and Nguyen Van Duong, "A Risk-Based Approach to Artificial Intelligence Regulation: Lessons from the European Union for Vietnam," *VNU Journal of Science: Legal Studies* 41, no. 4 (December 2025), https://doi.org/10.25073/2588-1167/vnuls.4799; Korshenko, "Risk Regulation Approach to Governing Artificial Intelligence on the Example of the EU's Artificial Intelligence Act / Submitted by Vladyslav Korshenko," 99.

44 Daria Lunca, "Towards a Coherent EU Civil Liability Regime for AI-Caused Harm," *European Journal of Law and Public Administration* 12, no. 1 (August 2025): 23–50, https://doi.org/10.18662/eljpa/12.1/253.

45 Nikos Th. Nikolinakos, "Adapting EU Liability Rules to the Digital Age and Artificial Intelligence: The 2021–2022 Public Consultation," in *Adapting the EU Civil Liability Regime to the Digital Age: Artificial*

was withdrawn, the revised PLD and general tort rules under Articles 4–7 provide redress mechanisms for injured parties. Together, these instruments produce a layered framework combining ex-ante compliance duties with ex-post remedial safeguards. However, allocating liability across complex AI value chains remains an open challenge.[46]

In contrast, the United States continues to rely on an ex-post liability model, grounded in negligence and product-defect doctrines rather than on a unified federal AI statute.[47] The Restatement (Third) of Torts, §§ 1–2, governs product liability by requiring proof of defect, causation, and foreseeability, all of which are strained in opaque, algorithmic systems. Federal oversight occurs through soft-law and sectoral instruments: the National Institute of Standards and Technology (NIST) AI Risk Management Framework (2023) outlines non-binding principles of transparency, accountability, and explainability; while the Executive Order on Safe, Secure, and Trustworthy AI (2023) directs federal agencies to integrate AI risk assessments into procurement and enforcement.[48]

At the state level, the Colorado Artificial Intelligence Act (SB24-205, 2024) marks the first comprehensive AI statute in the U.S. It classifies "high-risk" AI systems and imposes reasonable-care duties on developers and deployers (§3-102 to §3-105)[49], with rebuttable presumptions of compliance for entities adhering to recognised standards such as the NIST Framework.[50] Despite these developments, the American approach remains fragmented and

---

Intelligence, Robotics, and Other Emerging Technologies, vol. 68, by Nikos Th. Nikolinakos, Law, Governance and Technology Series (Cham: Springer International Publishing, 2024), 327–75, https://doi.org/10.1007/978-3-031-67969-8_7.

46 Daria Lunca, "Towards a Coherent EU Civil Liability Regime for AI-Caused Harm." *European Journal of Law and Public Administration* 12, no. 1 (2025): 23-50.

47 Steven Benerofe, "AI Governance and the Verification Gap: A Framework for Law and Policy Under Computational Intractability," SSRN Scholarly Paper no. 5629290 (Rochester, NY: Social Science Research Network, September 29, 2025), https://doi.org/10.2139/ssrn.5629290.

48 Joseph R. Biden, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, ed. Fred Zimmerman (Nimble Books LLC, 2023); "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," *Digital Government Hub*, n.d., accessed January 27, 2026, http://digitalgovernmenthub.org/examples/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

49 Colorado General Assembly. "SB24-205: Consumer Protections for AI." (2024). 59.

50 Mayur Jariwala, "A Comparative Analysis of the EU AI Act and the Colorado AI Act: Regulatory Approaches to Artificial Intelligence Governance," *International Journal of Computer Applications* 186, no. 38 (September 2024): 23–29, https://doi.org/10.5120/ijca2024923954..

reactive, leaving questions of foreseeability, duty allocation, and black-box opacity largely to judicial interpretation on a case-by-case basis.[51]

By comparison with the above approaches, Saudi Arabia's regulatory evolution reflects a more centralised, preventive paradigm, embedding AI governance within broader frameworks of digital integrity and legal modernisation.[52] Saudi Arabia's emerging AI-related framework follows a foundational approach combining digital governance, data protection, and evidentiary modernisation.[53] The E-Commerce Law (Royal Decree No. M/126 of 2019), notably Articles 5, 7, and 11, requires merchants and platforms to ensure transparency, consumer protection, and the reliability of electronic communications.[54] The Law of Evidence (Royal Decree No. M/43 of 2022), particularly Articles 35–38, recognises digital evidence and electronic records as having full probative value, thus facilitating the use of AI-generated or AI-processed data in judicial proceedings.[55]

The Personal Data Protection Law (PDPL) (Royal Decree No. M/19 of 2021), implemented by the Saudi Data and Artificial Intelligence Authority (SDAIA) and supplemented by its Executive Regulations (2023)[56], establishes principles of lawful processing, purpose limitation, accuracy, and data-subject rights (Articles 3–10).[57] Together with the National Strategy for Data & AI (2020), a policy vision led by SDAIA and the Ministry of Communications and

---

51 Martin Ebers, "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act," *European Journal of Risk Regulation* 16, no. 2 (June 2025): 684–703, https://doi.org/10.1017/err.2024.78; Jariwala, "A Comparative Analysis of the EU AI Act and the Colorado AI Act," 8887..

52 Beata Polok and Mariana Dussin, "AI Governance in Saudi Arabia: Cultural Values and Ethical AI Regulations in Comparative Perspective," *Yearbook of Islamic and Middle Eastern Law Online* 24, no. 1 (April 2025): 191–219, https://doi.org/10.1163/22112987-bja00004.

53 Beata Polok and Dussin Mariana "AI Governance in Saudi Arabia." 1-29; Tobias Mahler, "Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal," SSRN Scholarly Paper no. 4001444 (Rochester, NY: Social Science Research Network, September 30, 2021), https://papers.ssrn.com/abstract=4001444.

54 Mohammad Omar Mohammad Alhejaili, "Securing the Kingdom's e-Commerce Frontier: Evaluation of Saudi Arabia's Cybersecurity Legal Frameworks," *Journal of Governance and Regulation* 13, nos. 2, special issue (2024): 275.

55 Richard Aggrey et al., "The Role of Blockchain, IoT and AR in Future Healthcare: A Review," *IJFMR - International Journal For Multidisciplinary Research* 6, no. 6 (December 2024), https://doi.org/10.36948/ijfmr.2024.v06i06.33535.

56 SDAIA. "National Strategy for Data & AI (NSDAI)." (2020).

57 Siddharth Kanojia, "Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments in Personal Data Protection Law in Saudi Arabia," *Manchester Journal of Transnational Islamic Law and Practice* 19, no. 3 (October 2023): 270–76.

Information Technology[58], the Saudi framework aligns with the OECD and UNESCO AI ethics principles, promoting transparency and accountability.[59]

However, unlike in the EU, there is no dedicated civil liability statute for autonomous systems. Liability for AI-related harm must therefore be extrapolated from general tort and contractual principles under the Civil Transactions Law (Royal Decree No. M/191 of 2023)—especially Articles 162–165, which govern fault, causation, and damage.[60] This leaves courts with significant interpretive discretion in assigning responsibility among AI developers, users, and intermediaries.[61] Consequently, the Saudi system may be characterised as regulatory-in-principle but liability-in-transition, with the building blocks for ex-ante governance present but lacking a coherent ex-post remedial framework.[62]

Across all three models, AI's interdependent stack (sensors/hardware, models/software, data services, connectivity, platform operators) multiplies interface risk and complicates fault attribution when components originate from different producers. EU PLD reform aims to close historical gaps by explicitly covering software/AI; the U.S. relies on judicial adaptation of existing doctrines (design defect, failure to warn, negligence per se), and Saudi law currently uses general civil liability norms alongside sectoral guidance. System opacity and autonomy continue to frustrate defect-proof, causation-tracing, and producer-foreseeability assessments.[63] Orrick+1 Modern legal systems are increasingly converging on stricter rules for digital evidence and chain-of-custody integrity, as seen in Saudi Arabia's *Law of Evidence* and other regional reforms. Yet, the rise of AI-generated outputs, such as algorithmic scores,

---

58 SDAIA. "Personal Data Protection Law & Implementing Regulations." (2023–2025).

59 Siddharth, "Ensuring privacy of personal data." 270; Mohammad Bashayreh, *Saudi Arabia's Vision 2030, Shariah, and Contemporary Legal Trends: The Transformative Power of Law in Guiding Reforms* (Revival Press Limited, 2024), https://revivalpress.co.uk/books/saudi-arabia%E2%80%99s-vision-2030-shariah-and-contemporary-legal-trends.

60 Ketan Ramakrishnan, Gregory Smith, and Conor Downey, *U.S. Tort Liability for Large-Scale Artificial Intelligence Damages: A Primer for Developers and Policymakers* (2024), https://www.rand.org/pubs/research_reports/RRA3084-1.html.

61 Redeer Avdal Saleh and Subhi R. M. Zeebaree, "Artificial Intelligence in E-Commerce and Digital Marketing: A Systematic Review of Opportunities, Challenges, and Ethical Implications," *Asian Journal of Research in Computer Science* 18, no. 3 (February 2025): 395–410, https://doi.org/10.9734/ajrcos/2025/v18i3601.

62 Saudi Ministry of Justice/MISA. (2022/2025). Law of Evidence (English).

63 Julia Apostle, "New EU Directive Modernizes Defective Product Liability to Address New Technologies," Orrick, accessed October 31, 2025,

predictive classifications, and deepfakes, poses serious challenges to the principles of authenticity, reliability, and attribution. These technologies blur the distinction between original and synthetic data, complicating the process of establishing evidentiary trustworthiness.

Within Islamic legal methodology, the principles of *bayyinah* (proof) and *qarīnah* (circumstantial indicators) provide a robust framework for addressing such concerns.[64] They emphasise that evidence must not only be demonstrably true but also ethically grounded in fairness (*ʿadl*) and honesty (*ṣidq*).[65] By requiring courts to examine the provenance and integrity of AI-derived evidence, these principles help safeguard against manipulation and ensure procedural justice. Moreover, the *fiqh* maxim *al-bayyināt ʿalā al-muddaʿī wa-l-yamīn ʿalā man ankara* ("the burden of proof rests upon the claimant, and the oath upon the denier") preserves the balance of evidentiary responsibility even in the digital context. Under this maxim, AI outputs may serve as supporting *qarā'in* (indicia) that corroborate or refute digital traces, provided their authenticity and source are independently verified. Saudi Arabia's recognition of digital evidence, reflected in both statutory provisions and judicial practice, aligns with this evolving interpretive trajectory.

Ultimately, integrating modern evidentiary protocols with Islamic jurisprudential principles creates a more holistic and ethically coherent approach. This synthesis ensures that technological innovation remains accountable to the enduring objectives of *maqāṣid al-sharīʿah*—justice, protection of rights, and prevention of harm, thereby harmonising contemporary AI evidentiary challenges with classical legal wisdom.

In the Kingdom of Saudi Arabia, the avoidance of *gharar* (excessive uncertainty) in contractual relations is a doctrinal cornerstone, reflected in both classical *fiqh al-muʿāmalāt* and in contemporary statutes. Under Article 52 of the Civil Transactions Law (2023), contracts must be concluded with full consent (*tarāḍī*) and clarity regarding rights and obligations, echoing the

---

[64] Muhammad Husni Mubaroq, "Truth In Two Faces: An Epistemological Examination Of Islamic Law between Material And Formal," *Al-Ulum: Multidisciplinary Journal of Science* 1, no. 2 (July 2025): 85–95.

[65] USIM. "Al-Qarīnah: Circumstantial Evidence and its place in Islamic law." (2024); Anowar Zahid et al., "Qarinah: Admissibility of Circumstantial Evidence in Hudud and Qisas Cases," SSRN Scholarly Paper no. 2753353 (Rochester, NY: Social Science Research Network, 2015), https://papers.ssrn.com/abstract=2753353.

Islamic requirement that the object of the contract (*maḥall al-ʿaqd*) must be known and deliverable. Article 94 further invalidates contracts tainted by deception, fraud, or ambiguity, principles that align with the Sharia prohibition of *gharar*.[66]

When AI systems autonomously determine eligibility, pricing, or contract terms, their opaque decision-making processes may introduce *gharar* unless transparency measures, such as explainability, audit trails, and human review, are embedded in the contractual architecture. The E-Commerce Law (Royal Decree No. M/126 of 2019, Arts. 5–8) reinforces these principles by requiring clear disclosure of service conditions and supplier identity, thus operationalising *ʿadl* (fairness) and *tarāḍī* in digital commerce. In addition, the Law of Evidence[67] explicitly recognises electronic data and digital records as admissible proof, provided authenticity and integrity can be established, an evolution consistent with *bayyinah* (proof) and *qarīnah* (circumstantial indicators). These statutory developments embody the higher objectives of *maqāṣid al-sharīʿah*, particularly *maṣlaḥah mursalah* (public benefit) and *lā ḍarar wa-lā dirār* (no harm), which justify regulatory intervention to prevent deception, ensure consumer confidence, and maintain market stability without stifling innovation.

Modern consumer-protection institutions in Saudi Arabia and other GCC jurisdictions perform functions analogous to the classical *ḥisbah*, market oversight to uphold honesty and public welfare. Under Article 17 of the Saudi E-Commerce Law, the Ministry of Commerce is empowered to monitor digital transactions, investigate complaints, and sanction violations to prevent deception or unfair trade practices. Algorithmic bias in eligibility, ranking, or pricing thus falls within the purview of these supervisory duties. Embedding *amānah* (trustworthiness) in data handling, model updates, and algorithmic transparency ensures that AI intermediaries operate within the ethical boundaries of *fiqh al-muʿāmalāt*. This approach is consistent with recent scholarship emphasising that *ḥisbah* can serve as a normative foundation for algorithmic accountability and fairness.[68]

---

[66] Hashim M, Kamali, "Between Separation and Unity" 21-46.

[67] Royal Decree No. M/43 of 2022, Arts. 15–17.

[68] Julien Kiesse Bahangulu and Louis Owusu-Berko, "Algorithmic Bias, Data Ethics, and Governance: Ensuring Fairness, Transparency and Compliance in AI-Powered Business Analytics Applications,"

In the United States, regulatory adaptation remains primarily sectoral and ex-post. Under the Federal Trade Commission Act, §5, deceptive AI practices may constitute unfair trade practices, while the Colorado Artificial Intelligence Act (SB24-205, 2024) establishes a duty for deployers to perform "impact assessments" and maintain transparency in automated decision-making. Similarly, the NIST AI Risk Management Framework (2023, §§ 3.1–3.3) encourages documentation, traceability, and audit logs as procedural safeguards.[69]

These principles resonate with the Islamic legal maxim *taghayyur al-aḥkām bi-taghyur al-azmān wa-l-amkinah* (rulings evolve with time and place), which legitimises the iterative calibration of standards, such as watermarking, model versioning, and data lineage verification, as AI systems evolve. Coupled with *amānah*, this framework provides an ethical rationale for maintaining the authenticity and completeness of digital evidence across multiple actors and platforms, mirroring the American emphasis on duty of care in multi-party AI value chains.

Building on these parallel developments, a broader pattern of regulatory harmonisation is emerging, most notably in the European Union and Saudi Arabia, where distinct legal traditions appear to converge toward a shared vision of anticipatory, ethically grounded AI governance. This emerging alignment suggests an incipient harmonised reform trajectory, integrating the EU's ex-ante model with Saudi Arabia's Sharia-rooted normative framework. The EU Artificial Intelligence Act[70] mandates risk-based compliance, including transparency, data governance, and human oversight, which safeguards concepts that conceptually parallel the avoidance of *gharar* in Islamic contract law. Article 22 of the GDPR[71] prohibits fully automated decisions with significant legal effects unless subject to human review, reinforcing procedural fairness akin to *tarāḍī*.

World Journal of Advanced Research and Reviews 25, no. 2 (2025): 1746–63, https://doi.org/10.30574/wjarr.2025.25.2.0571.

69 Stuart D. Levi et al., "Colorado's Landmark AI Act: What Companies Need To Know," Skadden, Arps, Slate, Meagher & Flom LLP, June 24, 2024, https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act.

70 Regulation (EU) 2024/1689, Arts. 9–15

71 Regulation (EU) 2016/679

Saudi law, however, continues to rely primarily on ex-post liability and evidentiary evaluation. This gap may be bridged through reforms that combine (1) ex-ante controls such as algorithmic disclosure and audit duties to mitigate *gharar* before harm occurs, and (2) ex-post evidentiary presumptions calibrated to data integrity and explainability standards. To reconcile these approaches, Islamic principles such as *maṣlaḥah* (public interest), *lā ḍarar* (no harm), *amānah* (trustworthiness), and *bayyinah/qarīnah* (proof and circumstantial inference) can supply the moral ballast for a hybrid legal model. Practically, reform should focus on four directions: *First*, explainability and disclosure obligations proportional to algorithmic risk (AI Act, Art. 13). *Second*, evidentiary presumptions tied to audit logs and traceability mechanisms.[72]

Third, shared or proportionate liability for multi-actor AI systems (EU Product Liability Directive 85/374/EEC, as amended 2024). *Fourth*, codified consumer redress and supervisory auditing powers, reflecting the *ḥisbah* mandate and ensuring Sharia-compliant fairness while aligning with global standards.

The above description shows that the standard of proof in disputes mediated by artificial intelligence (AI) is still presented narratively and scattered across various legal regimes. To overcome these limitations and improve analytical clarity, this article presents a comparative table that systematically summarises the standards of proof in four legal regimes, namely the European Union, the United States, Saudi Arabian civil law, and Islamic law. This comparative mapping clarifies the similarities, differences, and analytical implications of each system in addressing issues of causality, the burden of proof, and the use of AI-based evidence. Thus, the table below provides a coherent analytical basis for formulating recommendations for legal reform. Through this integration, Saudi Arabia's developing digital legal framework is expected to achieve legal certainty and ethical legitimacy, while balancing technological innovation with the principles of justice (*ʿadl*) and prevention of harm (*dafʿ al-ḍarar*).

To overcome the previously fragmented presentation of analysis and to strengthen the systematics of comparative studies, the following table presents an analytical summary of the standards of proof in AI-based disputes

[72] Saudi Evidence Law, Arts. 15–17

in four legal regimes: the European Union, the United States, Saudi Arabian civil law, and Islamic law. This table does not place Islamic law solely as a normative supplement, but rather as an autonomous evidentiary regime with its own principles, mechanisms, and standards of proof. Through its structured presentation, this table highlights how each legal system understands the concept of evidence, allocates the burden of proof, and addresses the challenges posed by algorithmic opacity and autonomy. Thus, this table serves as an analytical bridge connecting the doctrinal discussion with the section on legal reform recommendations.

Table 1. Comparison of Evidentiary Regimes in Artificial Intelligence Disputes

	European Union	**United States**	**Saudi Civil Law**	**Islamic Law**
Concept of Evidence	Digital and documentary evidence regulated *ex ante* (AI Act, GDPR)	Evidence is assessed on a case-by-case basis under the Federal Rules of Evidence	Electronic evidence is formally recognised under the 2022 Law of Evidence	*Bayyinah*, *shahādah*, and *qarīnah* are grounded in moral accountability
Burden of Proof	Placed on the claimant, with an increasing tendency toward evidentiary presumptions	Placed on the claimant (negligence and product liability)	Placed on the claimant, subject to judicial discretion	*Al-bayyinah ʿalā al-muddaʿī wa-l-yamīn ʿalā man ankara*
AI Opacity	Addressed through transparency and explainability obligations	Managed through *ex post* judicial assessment	Evaluated through the authenticity and integrity of digital evidence	AI is treated as a *qarīnah*, not as an autonomous witness
Role of Ethics	Integrated into risk-based regulatory frameworks	Predominantly soft law and sector-specific	Integrated through regulatory objectives	Core principles: *ʿadl*, *amānah*, *lā ḍarar*
Status of AI Evidence	Regulated and accountable digital evidence	Contestable evidence subject to adversarial scrutiny	Valid evidence is authentic and intact	Supporting indication, not primary *bayyinah*

Normative Objective	Risk prevention and protection of fundamental rights	Loss allocation and deterrence	Legal certainty and market integrity	Justice, prevention of harm, and moral responsibility

Source: compiled by the author, 2025

The table above shows the fundamental differences in how each legal regime frames the evidence and accountability for AI use. The European Union places digital evidence within a strict ex ante regulatory framework, emphasising risk prevention through transparency, explainability, and accountability obligations integrated into the AI Act and GDPR. In contrast, the United States maintains a casuistic ex post approach, in which the validity and weight of AI evidence are determined through an adversarial process under the Federal Rules of Evidence, particularly in the context of negligence and product liability. Saudi Arabia's civil law occupies a position between these two models by formally recognising electronic evidence through the 2022 Evidence Act, while still granting judges broad discretion in assessing the authenticity and integrity of evidence. These differences underscore that the main challenges of AI evidence are not only technical but also normative, relating to choices about when and how states intervene to manage technological risks.

Thus, Islamic law appears as a regime of proof with its own internal logic and mechanisms, rather than merely as an ethical complement to positive law. The principle of *al-bayyinah ʿalā al-muddaʿī wa-l-yamīn ʿalā man ankara* affirms a clear structure of the burden of proof. At the same time, the classification between *bayyinah*, *shahādah*, and *qarīnah* allows AI-based evidence to be placed as supporting indications that must be verified morally and procedurally. By treating AI as *qarīnah* rather than an independent witness, Islamic law has conceptually anticipated the problem of algorithmic opacity and the risk of shifting responsibility from humans to machines. The integration of ethical principles such as *ʿadl*, *amānah*, and *lā ḍarar* into the evidentiary regime shows that the normative goals of Islamic law do not end at efficiency or the allocation of losses, but are oriented toward preventing harm and maintaining moral responsibility. Therefore, this table not only maps the differences between legal systems but also serves as an analytical basis for formulating AI evidence reforms that are fair, adaptive, and ethically legitimate.

Reform Proposals and Policy Implications

The increasingly massive integration of artificial intelligence (AI) into legal systems requires a review of doctrines and regulatory structures developed in a pre-digital context. Previous comparative findings show that standards of proof, causality, and legal liability in AI-based disputes still face doctrinal gaps, mainly due to the opaque, autonomous, and multi-actor nature of algorithms. Therefore, legal reform should be directed at ensuring coherence between technological advances and ethical governance, with an emphasis on three main areas: adjusting legal doctrine, strengthening digital standards of proof, and harmonising cross-jurisdictional regulations grounded in reconcilable legal and moral values.

First, legal doctrine must be adjusted to address the inadequacy of traditional concepts such as fault, causation, and individual responsibility in addressing losses caused by AI systems. A comparative analysis shows that a fault-based liability approach is challenging to apply when decisions are made by algorithmic systems not entirely under the control of a single human actor.[73] Therefore, doctrinal reform needs to lead to the development of more adaptive liability models, such as proportional liability, a risk-based causation presumption, and a duty of care tailored to the level of autonomy and impact of AI.[74] In the context of Islamic law, this adjustment is possible through the ijtihad mechanism, based on maqāṣid al-sharīʿah and fiqh principles such as lā *ḍarar wa-lā ḍirār* and *al-ghurm bi-l-ghunm*, which place the realisation of *mudarat* and risk distribution at the basis of liability.[75] Hus, Islamic law functions not only as an ethical framework, but also as an operational doctrinal source in responding to the legal challenges of AI.[76]

Second, strengthening digital evidence standards is a key prerequisite for resolving disputes mediated by AI. The technical complexity and "black box" nature of algorithms demand stricter standards regarding the authenticity,

---

[73] Lawrence Nderu et al., "DataLawCompanion: Enhancing Data Protection Law Compliance in the Digital Age," *Data Science Journal* 23, no. 1 (June 2024), https://doi.org/10.5334/dsj-2024-036.

[74] Nderu et al., 57; Saleh and Zeebaree, "Artificial Intelligence in E-Commerce and Digital Marketing."

[75] Nderu et al., "DataLawCompanion," 23; Aidatul Fitriyah and Daryna Dzemish Abdulovna, "EU's AI Regulation Approaches and Their Implication for Human Rights," *Media Iuris* 7, no. 3 (October 2024): 417–38, https://doi.org/10.20473/mi.v7i3.62050.

[76] Souha Korbatieh, "The Law of Evidence in the Islamic Criminal Justice System: A Critical Appraisal in the Light of Modern Technology" (thesis, Macquarie University, 2022), https://doi.org/10.25949/19440422.v1.

integrity, and traceability of digital evidence. In positive law systems, this is reflected in the increased role of audit logs, technical documentation, and digital forensic mechanisms to ensure the reliability of AI-based evidence. In line with this, Islamic law has, from the outset, developed a typology of evidence that distinguishes between bayyinah as primary evidence and qarīnah as supporting evidence.[77] This framework provides a clear methodological basis for placing AI output as supporting evidence that must be independently verified, rather than as independent testimony. The integration of fiqh principles such as *al-kitābah* (written evidence) and *raʾy al-khabīr* (expert opinion) with modern digital forensic practices strengthens evidentiary standards that guarantee procedural justice while maintaining normative legitimacy in both Sharia and civil justice systems.[78]

Third, international regulatory harmonisation is needed to address the cross-border nature of AI systems, particularly in e-commerce and digital services. However, such harmonisation should not lead to normative unification that ignores the diversity of legal traditions. Instead, a pluralistic approach based on universal values such as the protection of human dignity, justice, transparency, and the prevention of harm is more conducive to the creation of inclusive AI governance.[79] The principles of *maqāṣid al-sharīa* and the rule of *maṣlaḥah* (public interest) are substantively compatible with global standards of human rights and AI ethics, thereby actively contributing to the formation of an international harmonisation framework that is neither hegemonic nor dialogical.

The policy implications of these reforms require the active role of the state and regulatory authorities in alleviating the burden of proof for parties harmed by AI, including by introducing presumptions of causation and obligating AI system providers and managers to disclose technical evidence. The proposed legal framework should also allow for fault-based and non-contractual claims to complement the existing liability regime. In this case, even though the discourse on the legal personification of AI is beginning to

---

77 Buiten, De Streel, and Peitz, "The Law and Economics of AI Liability," 11.

78 Omar Alakayleh, "The Role of the Jordanian Public Security in Collecting Digital Evidences and Its Impact on the Detection of Crime," SSRN Scholarly Paper no. 5359002 (Rochester, NY: Social Science Research Network, July 20, 2025), https://doi.org/10.2139/ssrn.5359002.

79 Min, "Artifical Intelligence and Bias," 3811.

develop, the existing legal structure still appropriately places responsibility on human actors involved in the development, application, and supervision of AI. This approach maintains a balance between protecting victims and providing legal certainty for businesses investing in AI technology.

Overall, legal and policy reforms related to AI evidence and liability must be directed towards establishing an adaptive, flexible, and ethically based legal framework. Legislators and regulators need to design rules that can be updated in line with technological developments, while strengthening international cooperation to address cross-jurisdictional challenges. On the other hand, businesses are required to integrate ethical considerations, transparency, and accountability from the design and implementation stages of AI systems. With this approach, technological innovation can serve as a trustworthy and responsible instrument, in line with the objectives of substantive justice, the protection of rights, and the prevention of harm in both positive law and Islamic law.

Conclusion

This article has examined the challenges of proving damage in AI-mediated e-commerce disputes through a comparative doctrinal analysis of the European Union, the United States, Saudi Arabia, and Islamic law, demonstrating that existing liability and evidentiary frameworks remain strained by the opacity, autonomy, and multi-actor nature of AI systems. The findings reveal a clear divergence between the EU's preventive, risk-based ex-ante model, the United States' fragmented, ex-post, fault-oriented approach, and Saudi Arabia's transitional framework that combines modern evidentiary recognition with discretionary judicial assessment. At the same time, Islamic law emerges as an autonomous evidentiary regime grounded in structured principles of proof, moral accountability, and harm prevention. The novelty of this study lies in systematically positioning Islamic law not merely as an ethical supplement, but as a functional evidentiary system capable of addressing algorithmic opacity by treating AI outputs as corroborative indications (*qarīnah*) rather than autonomous proof. By integrating comparative insights with Islamic jurisprudential principles, the article demonstrates that effective AI governance requires adaptive liability doctrines, strengthened digital evidence standards, and pluralistic regulatory harmonisation that balances innovation

with justice and accountability. Future research may further explore operationalising these principles through empirical judicial analysis, cross-border enforcement mechanisms, and the development of hybrid evidentiary presumptions tailored to high-risk AI applications in global digital markets.

Acknowledgement

The authors would like to express their sincere gratitude to the academic institutions that have provided a supportive environment for the writing of this publication. Special thanks are extended to the Faculty of Law, Prince Mohammad bin Fahd University, Saudi Arabia, for its ongoing academic support and research facilities, which have greatly contributed to the development of this work. The authors also thank the Faculty of Law, Nineveh University, Mosul, Iraq, for its academic encouragement and intellectual contributions. The constructive academic discussions, collaborative support, and institutional resources from both universities have played an important role in refining the analysis and strengthening the quality of this research. Any limitations or errors that remain in this research are entirely the responsibility of the authors.

Disclosure Statement

The authors declare that there are no conflicts of interest related to the research, writing, and publication of this article. This study was conducted independently without financial support, grants, or sponsors that could be considered to influence the research process or results. The authors are affiliated with Prince Mohammad bin Fahd University, Saudi Arabia, and Nineveh University, Mosul, Iraq, and affirm that these institutional affiliations do not affect the objectivity, integrity, or academic independence of the research. All analyses, interpretations, and conclusions presented in this article are entirely those of the authors and do not necessarily reflect the official views or policies of their respective institutions. The authors affirm that this research was conducted in accordance with accepted academic and ethical standards.

References

Abbasi, Hafsa, Summayyah Summayyah, and Syed Naeem Badshah. "English-5 Principles of Electronic Evidence in Sharī'Ah and Law-A Comparative Study." *Al-Aijaz Research Journal of Islamic Studies & Humanities* 5, no. 2 (June 2021): 50–67. https://doi.org/10.53575/English5.v5.02(21).50-67.

Abudaqqa, Fatma. "Artificial Intelligence for IT Governance in Saudi Arabia: Opportunities, Challenges, and Future Directions within COBIT 2019 and ISO/IEC 38500 Frameworks." *European Scientific Journal, ESJ* 21, no. 25 (September 2025): 125–59. https://doi.org/10.19044/esj.2025.v21n25p125.

Aggrey, Richard, Emmanuel Adjirachor, Bright Ansah Adjei, Karl Osei Afoduo, Nana Adwoa Konadu Dsane, and Gladys Doe. "The Role of Blockchain, IoT and AR in Future Healthcare: A Review." *IJFMR - International Journal For Multidisciplinary Research* 6, no. 6 (December 2024). https://doi.org/10.36948/ijfmr.2024.v06i06.33535.

Alakayleh, Omar. "The Role of the Jordanian Public Security in Collecting Digital Evidences and Its Impact on the Detection of Crime." SSRN Scholarly Paper No. 5359002. Rochester, NY: Social Science Research Network, July 20, 2025. https://doi.org/10.2139/ssrn.5359002.

Al-Fatih, Sholahuddin, Putri Shafarina Thahir, Nafik Muthohirin, and Norhasliza Ghapa. "Artificial Intelligence in Indonesia's Financial Sector: Regulatory and Islamic Law Perspectives." *Justicia Islamica* 22, no. 2 (November 2025): 303–26. https://doi.org/10.21154/justicia.v22i2.10479.

Alhejaili, Mohammad Omar Mohammad. "Securing the Kingdom's e-Commerce Frontier: Evaluation of Saudi Arabia's Cybersecurity Legal Frameworks." *Journal of Governance and Regulation* 13, nos. 2, special issue (2024): 275.

Bahangulu, Julien Kiesse, and Louis Owusu-Berko. "Algorithmic Bias, Data Ethics, and Governance: Ensuring Fairness, Transparency and Compliance in AI-Powered Business Analytics Applications." *World Journal of Advanced Research and Reviews* 25, no. 2 (2025): 1746–63. https://doi.org/10.30574/wjarr.2025.25.2.0571.

Bashayreh, Mohammad. *Saudi Arabia's Vision 2030, Shariah, and Contemporary Legal Trends: The Transformative Power of Law in Guiding Reforms*. Revival Press Limited, 2024. https://revivalpress.co.uk/books/saudi-arabia%E2%80%99s-vision-2030-shariah-and-contemporary-legal-trends.

Bawack, Ransome Epie, Samuel Fosso Wamba, Kevin Daniel André Carillo, and Shahriar Akter. "Artificial Intelligence in E-Commerce: A Bibliometric

Study and Literature Review." *Electronic Markets* 32, no. 1 (March 2022): 297–338. https://doi.org/10.1007/s12525-022-00537-z.

Benerofe, Steven. "AI Governance and the Verification Gap: A Framework for Law and Policy Under Computational Intractability." SSRN Scholarly Paper No. 5629290. Rochester, NY: Social Science Research Network, September 29, 2025. https://doi.org/10.2139/ssrn.5629290.

Biden, Joseph R. *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. Edited by Fred Zimmerman. Nimble Books LLC, 2023.

Bottomley, Dane, and Donrich Thaldar. "Liability for Harm Caused by AI in Healthcare: An Overview of the Core Legal Concepts." *Frontiers in Pharmacology* 14 (December 2023). https://doi.org/10.3389/fphar.2023.1297353.

Buiten, M., A. De Streel, and M. Peitz. "The Law and Economics of AI Liability." *Computer Law & Security Review* 48 (2023): 105794. https://doi.org/10.1016/j.clsr.2023.105794.

Buiten, Miriam, Alexandre de Streel, and Martin Peitz. "The Law and Economics of AI Liability." *Computer Law & Security Review* 48 (April 2023): 105794. https://doi.org/10.1016/j.clsr.2023.105794.

Crawford, Kate, and Ryan Calo. "There Is a Blind Spot in AI Research." *Nature* 538, no. 7625 (October 2016): 311–13. https://doi.org/10.1038/538311a.

David, Anne, Tan Yigitcanlar, Kevin Desouza, Karen Mossberger, Pauline Hope Cheong, Juan Corchado, Prithvi Bhat Beeramoole, and Alexander Paz. "Public Perceptions of Responsible AI in Local Government: A Multi-Country Study Using the Theory of Planned Behaviour." *Government Information Quarterly* 42, no. 3 (September 2025): 102054. https://doi.org/10.1016/j.giq.2025.102054.

Ebers, Martin. "Truly Risk-Based Regulation of Artificial Intelligence How to Implement the EU's AI Act." *European Journal of Risk Regulation* 16, no. 2 (June 2025): 684–703. https://doi.org/10.1017/err.2024.78.

European Commission. "Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts." 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

"Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." *Digital Government Hub*, n.d. Accessed January 27, 2026. http://digitalgovernmenthub.org/examples/executive-order-

on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

Fitriyah, Aidatul, and Daryna Dzemish Abdulovna. "EU's AI Regulation Approaches and Their Implication for Human Rights." *Media Iuris* 7, no. 3 (October 2024): 417–38. https://doi.org/10.20473/mi.v7i3.62050.

Hacker, Philipp, Johann Cordes, and Janina Rochon. "Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond." *European Journal of Risk Regulation* 15, no. 1 (March 2024): 49–86. https://doi.org/10.1017/err.2023.81.

Hacker, Philipp, and Jan-Hendrik Passoth. "Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond." In *xxAI - Beyond Explainable AI: International Workshop, Held in Conjunction with ICML 2020, July 18, 2020, Vienna, Austria, Revised and Extended Papers*, edited by Andreas Holzinger, Randy Goebel, Ruth Fong, Taesup Moon, Klaus-Robert Müller, and Wojciech Samek, 343–73. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-04083-2_17.

Huberman, Pinchas. "Tort Law, Corrective Justice and the Problem of Autonomous-Machine-Caused Harm." *Canadian Journal of Law & Jurisprudence* 34, no. 1 (February 2021): 105–47. https://doi.org/10.1017/cjlj.2020.3.

Jariwala, Mayur. "A Comparative Analysis of the EU AI Act and the Colorado AI Act: Regulatory Approaches to Artificial Intelligence Governance." *International Journal of Computer Applications* 186, no. 38 (September 2024): 23–29. https://doi.org/10.5120/ijca2024923954.

Julia Apostle. "New EU Directive Modernizes Defective Product Liability to Address New Technologies." Orrick. Accessed October 31, 2025. https://www.orrick.com/en/Insights/2025/06/New-EU-Directive-Modernizes-Defective-Product-Liability-to-Address-New-Technologies?utm_source=chatgpt.com.

Justo-Hanani, Ronit. "Risk-Based Approach to EU AI Act: Benefits and Challenges of Co-Regulation." *Policy Design and Practice*, January 2, 2026. World. https://www.tandfonline.com/doi/abs/10.1080/25741292.2025.2610869.

Kamali, Mohammad Hashim. "Between Separation and Unity: The Interplay of Law and Morality in Islamic Jurisprudence." In *Sharia Law in the Twenty-First Century*, by Muhammad Khalid Masud and Hana Jalloul Muro, 21–46.

World Scientific (Europe), 2022. https://doi.org/10.1142/9781800611689_0002.

———. *Principles of Islamic Jurisprudence*. 3. rev. and Enlarged ed., Repr. Cambridge: The Islamic Texts Society, 2011.

Kanojia, Siddharth. "Ensuring Privacy of Personal Data: A Panoramic View of Legal Developments in Personal Data Protection Law in Saudi Arabia." *Manchester Journal of Transnational Islamic Law and Practice* 19, no. 3 (October 2023): 270–76.

Kiani, Fatemeh, and Alireza Shafiee. "Global Harmonization of AI Regulation: Addressing Cross-Border Challenges in Ethical Standards, Accountability, and Liability." *Legal Studies in Digital Age* 1, no. 1 (October 2022): 14–26.

Korbatieh, Souha. "The Law of Evidence in the Islamic Criminal Justice System: A Critical Appraisal in the Light of Modern Technology." Thesis, Macquarie University, 2022. https://doi.org/10.25949/19440422.v1.

Korshenko, Vladyslav. "Risk Regulation Approach to Governing Artificial Intelligence on the Example of the EU's Artificial Intelligence Act / Submitted by Vladyslav Korshenko." Thesis, University of Salzburg, 2024. http://eplus.uni-salzburg.at/Abschlussarbeiten/9648422.

Levi, Stuart D., Ken D. Kumayama, William E. Ridgway, and Mana Ghaemmaghami. "Colorado's Landmark AI Act: What Companies Need To Know." Skadden, Arps, Slate, Meagher & Flom LLP, June 24, 2024. https://www.skadden.com/insights/publications/2024/06/colorados-landmark-ai-act.

Lunca, Daria. "Towards a Coherent EU Civil Liability Regime for AI-Caused Harm." *European Journal of Law and Public Administration* 12, no. 1 (August 2025): 23–50. https://doi.org/10.18662/eljpa/12.1/253.

Mahler, Tobias. "Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal." SSRN Scholarly Paper No. 4001444. Rochester, NY: Social Science Research Network, September 30, 2021. https://papers.ssrn.com/abstract=4001444.

Malja, Seyedeh Negin, and Hossein Afrasiabi. "Artificial Intelligence and Society: Mapping the Research through a Systematic Review." *AI & SOCIETY*, ahead of print, September 8, 2025. https://doi.org/10.1007/s00146-025-02555-9.

Mensah, George Benneh. *Artificial Intelligence and Ethics: A Comprehensive Review of Bias Mitigation, Transparency, and Accountability in AI Systems*. Version 1. 2023. https://doi.org/10.13140/RG.2.2.23381.19685/1.

Mergen, Aybike, Nergiz Çetin-Kılıç, and Mustafa F. Özbilgin. "Artificial Intelligence and Bias Towards Marginalised Groups: Theoretical Roots

and Challenges." In *AI and Diversity in a Datafied World of Work: Will the Future of Work Be Inclusive?*, vol. 12, edited by Joana Vassilopoulou and Olivia Kyriakidou, 0. Emerald Publishing Limited, 2025. https://doi.org/10.1108/S2051-233320250000012004.

Mesarčík, Matúš, Sara Solarova, Juraj Podroužek, and Maria Bielikova. "Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence Act." Preprint, SocArXiv, March 9, 2022. https://doi.org/10.31235/osf.io/yzfg8.

Min, Alfonso. "Artifical Intelligence and Bias: Challenges, Implications, and Remedies." *Journal of Social Research* 2, no. 11 (October 2023): 3808–17. https://doi.org/10.55324/josr.v2i11.1477.

Mubaroq, Muhammad Husni. "Truth In Two Faces: An Epistemological Examination Of Islamic Law between Material And Formal." *Al-Ulum: Multidisciplinary Journal of Science* 1, no. 2 (July 2025): 85–95.

Nderu, Lawrence, Ruth Oginga, Bonface Butichi, John Rono, Florence Njau, Felista Mogire, Derrick Matindo, Daniel Muiruri, and Agnes Kiragga. "DataLawCompanion: Enhancing Data Protection Law Compliance in the Digital Age." *Data Science Journal* 23, no. 1 (June 2024). https://doi.org/10.5334/dsj-2024-036.

Nevejans, Nathalie. "European Union's Regulation on the Placing on the Market and Use of AI Systems: A Critical Overview of the AI Act." In *Research Handbook on the Law of Artificial Intelligence*, edited by Woodrow Barfield and Ugo Pagallo, 489–540. Edward Elgar Publishing, 2025. https://doi.org/10.4337/9781035316496.00031.

Nicolis, Anna, Nigel Kingsman, and Hughes Hall. *AI Explainability in the EU AI Act: A Case for an NLE Approach Towards Pragmatic Explanations*. 1, no. 1 (July 2024).

Nikolinakos, Nikos Th. "Reforming the EU Civil Liability Framework Applicable to Artificial Intelligence and Other Emerging Digital Technologies: Defective Products—the Revised Product Liability Directive." In *Adapting the EU Civil Liability Regime to the Digital Age: Artificial Intelligence, Robotics, and Other Emerging Technologies*, vol. 68, by Nikos Th. Nikolinakos, 477–621. Law, Governance and Technology Series. Cham: Springer International Publishing, 2024. https://doi.org/10.1007/978-3-031-67969-8_9.

OECD. *Artificial Intelligence in Society*. OECD Publishing, 2019. https://doi.org/10.1787/eedfee77-en.

Osasona, Femi, Olukunle Oladipupo Amoo, Akoh Atadoga, Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, and Benjamin Samson Ayinla.

"Reviewing The Ethical Implications Of AI In Decision Making Processes." *International Journal of Management & Entrepreneurship Research* 6, no. 2 (February 2024): 322–35. https://doi.org/10.51594/ijmer.v6i2.773.

Phuc, Dao Gia, and Nguyen Van Duong. "A Risk-Based Approach to Artificial Intelligence Regulation: Lessons from the European Union for Vietnam." *VNU Journal of Science: Legal Studies* 41, no. 4 (December 2025). https://doi.org/10.25073/2588-1167/vnuls.4799.

Polok, Beata, and Mariana Dussin. "AI Governance in Saudi Arabia: Cultural Values and Ethical AI Regulations in Comparative Perspective." *Yearbook of Islamic and Middle Eastern Law Online* 24, no. 1 (April 2025): 191–219. https://doi.org/10.1163/22112987-bja00004.

Prihantoro, Hijrian Angga. "Examining Witness Interest: The Obstacles of Testimony in Islamic Jurisprudence and Positive Law." *Justicia Islamica* 21, no. 1 (June 2024): 1–22. https://doi.org/10.21154/justicia.v21i1.8653.

Rajendran, Sruthi, and Akshay Dinesh Kumar. "Liability for Harm Caused by AI: Examining the Legal Responsibility for the Actions of Autonomous Systems." *International Journal of Law Management & Humanities* 6, no. 2 (2023): 214–24. https://doij.org/10.10000/IJLMH.114348.

Ramakrishnan, Ketan, Gregory Smith, and Conor Downey. *U.S. Tort Liability for Large-Scale Artificial Intelligence Damages: A Primer for Developers and Policymakers*. 2024. https://www.rand.org/pubs/research_reports/RRA3084-1.html.

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). *General Data Protection Regulation (GDPR)*, Article 22. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Rubel, Alan. "The Black Box Society: The Secret Algorithms That Control Money and Information, by Frank Pasquale. Cambridge: Harvard University Press, 2015. 320 Pp. ISBN 978–0674368279." *Business Ethics Quarterly* 26, no. 4 (October 2016): 568–71. https://doi.org/10.1017/beq.2016.50.

Saleh, Redeer Avdal, and Subhi R. M. Zeebaree. "Artificial Intelligence in E-Commerce and Digital Marketing: A Systematic Review of Opportunities, Challenges, and Ethical Implications." *Asian Journal of Research in Computer Science* 18, no. 3 (February 2025): 395–410. https://doi.org/10.9734/ajrcos/2025/v18i3601.

Sargiotis, Dimitrios. "Ethical AI in Information Technology: Navigating Bias, Privacy, Transparency, and Accountability." *Advances in Machine Learning and Artificial Intelligence* 5, no. 3 (2024): 1–14. https://doi.org/10.33140/amlai.05.03.03.

Saudi Ministry of Commerce. "*E-Commerce Law* (Royal Decree No. M/126)." (2019). https://mc.gov.sa/en/RulesRegulations/Regulations/Pages/EcommerceLaw.aspx

Saudi Ministry of Justice/MISA. (2022/2025). Law of Evidence (English). MISA

SDAIA. "Personal Data Protection Law & Implementing Regulations." (2023–2025). SDAIA+2SDAIA+2

Schuster, W. Michael, Joseph Avery, and Camilla Alexandra Hrdy. "The AI Penalty in Trade Secret Law." SSRN Scholarly Paper No. 5610270. Rochester, NY: Social Science Research Network, June 1, 2025. https://doi.org/10.2139/ssrn.5610270.

Shaleh, Ahmad Syukri. "Ibn Taymiyya's Concept of Istiḥsān : An Understanding of Legal Reasoning in Islamic Jurisprudence." Thesis, McGill University, 1995. http://digitool.Library.McGill.CA:80/R/?func=dbin-jump-full&object_id=23241.

Shaping Europe's digital future. "Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence." April 21, 2021. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

Sruthi Rajendran and Akshay Dinesh Kumar. "Liability for Harm Caused by AI: Examining the Legal Responsibility for the Actions of Autonomous Systems | International Journal of Law Management & Humanities." *International Journal of Law Management and Humanities* 6, no. 2 (2023): 214–24. https://doij.org/10.10000/IJLMH.114348.

UNCITRAL. "Digital Economy and Legal Frameworks for Electronic Commerce." (2023).

Yeung, Karen. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12, no. 4 (2018): 505–23. https://doi.org/10.1111/rego.12158.

Yusrin, Nur Amalyna. "Ai-Powered E-Commerce: Elevating E-Service Quality Through Utilitarian And Hedonic With E-Satisfaction As The Bridge To E-Loyalty." *Jurnal Multidisiplin Sahombu* 5, no. 01 (January 2025): 216–31.

Zahid, Anowar, Ahmad Azam Mohd Shariff, Mohd Munzil bin Muhamad, Ramalinggam Rajamanickam, Mazupi Abdul Rahman, and Noorfajri Ismail. "Qarinah: Admissibility of Circumstantial Evidence in Hudud and Qisas Cases." SSRN Scholarly Paper No. 2753353. Rochester, NY: Social Science Research Network, 2015. https://papers.ssrn.com/abstract=2753353.