Al-Madina: Journal of Islamic Law
Volume 1, Issue 1 (March, 2026), pp. 49–70
https://nayottamareswara.co.id/index.php/amjil/home
Published by: Yayasan Bantuan Hukum Nayottama Reswara

Maqāsid al-Sharī'ah amid digital distortion: an integrative Islamic legal framework addressing deepfakes

Dhimas Rizky Nur Firmansyach
Universitas Islam Negeri Sunan Kalijaga Yogyakarta, Indonesia

Rian Dwiyanto*
Universitas Islam Negeri Syarif Hidayatullah Jakarta, Indonesia

Ngaliyah Dwi Lestari
Universitas Islam Negeri Profesor Kiai Haji Saifuddin Zuhri Purwokerto, Indonesia

Talita Alba Salsabila
Institut Agama Islam Negeri Syaikh Abdurrahman Siddik Bangka Belitung, Indonesia

Alwi Ibrahim Lubis
Universitas Islam Negeri Syekh Ali Hasan Ahmad Addary Padangsidimpuan, Indonesia

*Corresponding Author Email: riandwiyanto2911@gmail.com

How to Cite–*Chicago Manual of Style 17th Edition (fullnote):*

Firmansyach, Dhimas Rizky Nur, Rian Dwiyanto, Ngaliyah Dwi Lestari, Talita Alba Salsabila, and Alwi Ibrahim Lubis. "Maqāsid al-Sharī'ah amid digital distortion: An integrative Islamic legal framework addressing deepfakes." *Al-Madina: Journal of Islamic Law* 1, no. 1 (2026): 49–70.

Abstract

This study examines the threat deepfakes pose to the realization of *maqāsid al-sharī'ah*, and develops an integrative Islamic-legal framework to protect honour (*hifz al-'ird*) in the era of digital distortion. Using a doctrinal and comparative normative-qualitative method, the analysis reviews contemporary literature on *maqāsid al-sharī'ah*, the ITE Law, the PDP Law, the TPKS Law, and digital-forensics research. The study identifies three interrelated threat dimensions: technical (biometric manipulation of faces and voices), epistemic (erosion of the evidentiary value of audiovisual material), and normative (defamation, slander, blackmail, and synthetic pornography). Findings

Article history:
Received: *14-02-2026* | ***Revised:*** *27-02-2026* | ***Accepted:*** *06-03-2026* | ***Published:*** *11-03-2026*

indicate that existing statutory frameworks are partial and general, forensic capacity remains limited, and current evidentiary procedures are ill-equipped to secure admissibility of AI-generated evidence. Interpreting these gaps through the *maqāsid al-sharī'ah* lens shows that assaults on honour affect the five fundamental protections, requiring an integrated normative response. The proposed framework comprises: narrowly defined offences criminalizing creation and distribution of degrading or exploitative deepfakes; AI-aware evidentiary standards—accredited forensic laboratories, secure electronic chains-of-custody, and admissibility criteria consonant with sharia evidence principles; and proportional *ta'zīr* sanctions coupled with restorative justice and victim compensation. For implementation, the study advocates a cross-agency pilot, steering committee, verification SOPs, rapid takedown channels, and measurable evaluation indicators. Safeguards, limited offence definitions, high mens rea thresholds, and appeal mechanisms, are essential to prevent oversuppression. The study concludes that effective solutions must be transdisciplinary and *maqāsid al-sharī'ah*-consistent. Further empirical research and pilot testing are required to validate and adapt policy responses to evolving technology.

Keywords: AI-aware; deepfakes; Islamic legal framework; *maqāsid al-sharī'ah*.

Introduction

In today's digital age of rapid technological advancement, deepfake technology—artificial intelligence (AI)-based audiovisual engineering capable of mimicking a person's face, voice, and expressions with a high degree of realism and persuasiveness—has emerged as a significant global threat.[1] In addition to being exploited as a tool for financial fraud and political disinformation, deepfakes are frequently used to produce content that violates the dignity and privacy of victims.[2] According to data from VIDA, deepfake cases in Indonesia increased dramatically by 1,550% between 2022 and 2023.[3] Even regional leaders and high-ranking state officials have become targets of deepfake manipulation, both materially and reputationally.[4] This phenomenon therefore constitutes not only a technological risk but also an urgent legal, social, and ethical challenge that must be addressed comprehensively.

The impact of deepfakes is multidimensional. *First*, individual victims may suffer economic losses, psychological trauma, and reputational harm. *Second*, the unchecked dissemination of deepfakes can erode public trust in

---

1 Mekhail Mustak et al., "Deepfakes: Deceptions, Mitigations, and Opportunities," *Journal of Business Research* 154 (2023): 113368, https://doi.org/10.1016/j.jbusres.2022.113368.

2 Felipe Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content," *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297–326, https://doi.org/10.1080/13600869.2024.2324540.

3 VIDA, "Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya," VIDA, October 28, 2024, https://vida.id/id/pressrelease/penipuan-deepfake-indonesia-melonjak-1550-begini-cara-vida-memeranginya. Accessed on December 15, 2025.

4 Dinas Kominfo Provinsi Jawa Timur, "Polda Jatim Ungkap Kasus Penipuan Deepfake AI Kepala Daerah, Pelaku Kantongi Keuntungan Hingga Rp87 Juta," Dinas Kominfo Provinsi Jawa Timur, April 28, 2025, https://kominfo.jatimprov.go.id/berita/polda-jatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87-juta. Accessed on December 15, 2025.

audiovisual evidence, the media, and public institutions, thereby contributing to an epistemic crisis.[5] *Third*, if left unaddressed, deepfakes may create significant loopholes for organized crime, ranging from systematic financial fraud to political manipulation, which in turn can undermine democratic governance and the protection of human rights.[6] Therefore, the urgency of addressing deepfakes is evident, as the rapid adoption of AI-based technologies has outpaced the formulation and implementation of effective regulatory policies.

A number of regulations have established a partial legal framework for addressing the phenomenon of deepfakes; however, their effectiveness remains constrained by normative gaps and limited enforcement capacity. Some of the relevant regulations are summarized in Table 1.

Table 1. Regulations relevant to deepfakes

Regulation	Relevance to Deepfake
Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law)	Provides a legal basis for imposing sanctions on the dissemination of harmful electronic content, including hoaxes, defamation, pornography, and related offenses.[7]
Law Number 27 of 2022 on Personal Data Protection (PDP Law)	Establishes a legal framework for addressing the unauthorized use of personal data, including images and other identifiable information.[8]
Law Number 12 of 2022 on Sexual Violence Crimes (*Tindak Pidana Kekerasan Seksual*/TPKS Law)	Encompasses sexual violence offenses committed in digital environments, including technology-facilitated abuse.[9]

Source: processed by the author from various sources.

Although a normative framework is already in place and several legal instruments may be invoked to prosecute the creators or distributors of deepfakes and to protect victims, significant practical challenges remain. Existing norms are often general in nature and do not fully accommodate the

[5] Ebba Lundberg and Peter Mozelius, "The Potential Effects of Deepfakes on News Media and Entertainment," *AI & SOCIETY* 40, no. 4 (2025): 2159–70, https://doi.org/10.1007/s00146-024-02072-1.

[6] Romero-Moreno, "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content," 315.

[7] Mahrina Mahrina, Joko Sasmito, and Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation," *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 21, no. 2 (2023): 345–62, https://doi.org/10.31941/pj.v21i2.2680.

[8] Supeno Supeno, Rosmidah Rosmidah, and Syed Mohd Uzair Iqbal, "Personal Data Protection in Review of Legal Theories and Principles," *Journal of Law and Legal Reform* 6, no. 3 (2025): 1349–76, https://doi.org/10.15294/jllr.v6i3.10252.

[9] Topo Santoso and Hariman Satria, "Sexual-Violence Offenses in Indonesia: Analysis of the Criminal Policy in the Law Number 12 of 2022," *Padjadjaran Jurnal Ilmu Hukum* 10, no. 1 (2023): 59–79, https://doi.org/10.22304/pjih.v10n1.a4.

specific technical characteristics of deepfake technology. In addition, the complex nature of modern digital evidence presents evidentiary challenges in judicial proceedings, while inter-agency coordination and digital forensic capacities remain insufficient.[10] This situation creates a gap between the availability of normative sanctions and the practical effectiveness of their enforcement.

Previous relevant studies have identified several important findings. An empirical study by Irene Amerini et al. that maps the surge and distribution patterns of deepfake cases emphasizes the need to expand digital forensic capacity.[11] Jeniver Loovens and Hasan Tinmaz echoed this sentiment in a systematic literature review, noting that, despite advances in deepfake detection and forensic analysis, interdisciplinary collaboration is essential to establish standard methods and frameworks to combat digital manipulation.[12] A comparative legal study between Indonesia and South Korea by Maya Ruhtiani et al. highlights normative gaps, particularly regarding evidentiary rules and emerging criminal offenses related to media manipulation.[13] Another study by Abdul Aziz Pamungkas et al. underscores the need to strengthen legal protections for Indonesian citizens against the misuse of deepfake technology, citing provisions in the ITE Law and the PDP Law.[14]

A normative study by Evyta Rosiyanti Ramadhani et al. in Islamic law demonstrates the potential to integrate the principles of *maqāsid al-sharī'ah* to strengthen the protection of victims' honor, dignity, and rights in the digital realm.[15] Furthermore, research by Sahajuddin et al. reaffirms that digital literacy should be understood not merely as a set of technical skills but as a moral and legal tool that reflects the principles of *maqāsid al-sharī'ah*, particularly *hifz al-'ird* (protection of honor) and *hifz al-'aql* (protection of

---

[10] Angelica Vanessa Audrey Nasution, Suteki, and Anggita Doramia Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse," *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489–2517, https://doi.org/10.1007/s11196-025-10265-0.

[11] Irene Amerini et al., "Deepfake Media Forensics: Status and Future Challenges," *Journal of Imaging* 11, no. 3 (2025): 73, https://doi.org/10.3390/jimaging11030073.

[12] Jenifer Loovens and Hasan Tinmaz, "A Systematic Literature Review of Deepfakes in Forensic Science," *Forensic Imaging* 43 (2025): 200647, https://doi.org/10.1016/j.fri.2025.200647.

[13] Maya Ruhtiani et al., "Generative AI and Copyright Law: A Rule of Law Comparison between Indonesia and South Korea," *Kosmik Hukum* 25, no. 3 (2025): 428–49, https://doi.org/10.30595/kosmikhukum.v25i3.26268.

[14] Abdul Aziz Pamungkas, Nanik Sutarni, and Burham Pranawa, "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity," *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 24, no. 1 (2025): 4562–74, https://doi.org/10.31941/pj.v24i2.6311.

[15] Evyta Rosiyanti Ramadhani, Ayudya Rizqi Rachmawati, and Roro Hera Kurnikova, "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia," *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 112–31, https://doi.org/10.18860/j-fsh.v17i1.28880.

reason), when addressing contemporary digital challenges.[16] These findings support the argument that effective solutions must be interdisciplinary and context-sensitive.

This study proposes a *maqāsid al-sharī'ah* approach to the threat posed by deepfakes as a protective measure, employing an integrative Islamic legal framework.[17] The proposed conceptual framework positions *maqāsid al-sharī'ah* as the guiding principle for defining offenses, assessing evidence, and prescribing sanctions for actions involving deepfakes, with particular attention to the protection of honour (*hifz al-'ird*) and to the five fundamental objectives of *maqāsid al-sharī'ah*: the protection of religion (*hifz al-dīn*), life (*hifz al-nafs*), intellect (*hifz al-'aql*), lineage (*hifz al-nasl*), and property (*hifz al-māl*).[18]

This framework clarifies the elements of deepfakes from an Islamic legal perspective, including slander, defamation, extortion, and technology-facilitated sexual violence, and formulates standards for digital evidence that integrate AI-sensitive forensic methods with the principles of shari'ah evidence. In addition, the framework proposes a model of proportionate *ta'zīr* (discretionary) sanctions,[19] outlines a restorative justice mechanism for victim rehabilitation, and establishes standard operating procedures for cooperation among judicial institutions, the police, relevant ministries, and data protection agencies.[20]

The research question of this study is how deepfake threats disrupt the realization of *maqāsid al-sharī'ah*, especially the protection of honor and the five basic protections, in the context of positive law and judicial practice in Indonesia. To what extent are existing legal instruments sufficient to prevent and mitigate these impacts, and what integrative framework model is most appropriate for formulating offenses, evidence, and victim recovery

---

16 Sahajuddin et al., "Beyond Regulation: Rethinking Deepfake Pornography Prevention Through Digital Literacy," *JURIS (Jurnal Ilmiah Syariah)* 24, no. 2 (2025): 357–67, https://doi.org/10.31958/juris.v24i2.15775.

17 Zumiyati Sanu Ibrahim et al., "Integration of Maqaṣid Al-Shari'ah in the Criminal Law Reform to Achieve Justice and Human Dignity," *Jurnal Hukum Islam* 23, no. 1 (2025): 105–44, https://doi.org/10.28918/jhi.v23i1.04.

18 Iffatin Nur, Syahrul Adam, and M. Ngizzul Muttaqien, "Maqāṣid Al-Sharī'at: The Main Reference and Ethical-Spiritual Foundation for the Dynamization Process of Islamic Law," *Ahkam: Jurnal Ilmu Syariah* 20, no. 2 (2020): 331–60, https://doi.org/10.15408/ajis.v20i2.18333.

19 *Ta'zīr* is a type of punishment in Islamic law whose provisions are not explicitly stated in the Qur'an or hadith. Its purpose is to teach a lesson and prevent the perpetrator from repeating crimes that harm the rights of Allah SWT and human rights. Scholars explain *ta'zīr* as a sanction for acts of disobedience that are not included in *hudūd* (sanctions that have been determined by the Qur'an and hadith) or *kafārāt* (fines or compensation that are obligatory due to violations of sharia provisions or negligence in religious obligations). See: Muhammad Mawardi Djalaluddin et al., "The Implementation of Ta'zīr Punishment as an Educational Reinforcement in Islamic Law," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 7, no. 1 (2023): 399–417, https://doi.org/10.22373/sjhk.v7i1.15101.

20 Ali Sodiqin, "Legal, Moral, and Spiritual Dialectics in The Islamic Restorative Justice System," *Ahkam: Jurnal Ilmu Syariah* 21, no. 2 (2021): 357–78, https://doi.org/10.15408/ajis.v21i2.22675.

mechanisms? The objectives of this study are to analyze the impact of deepfakes on the realization of *maqāsid al-sharī'ah*, evaluate the adequacy of existing norms and enforcement practices, and design an integrative Islamic legal conceptual framework that combines *maqāsid al-sharī'ah* principles with modern standards of evidence, fair sanctions, and mechanisms for recovery and institutional cooperation.

To achieve these research objectives, the study will combine a normative review of Islamic legal sources and the principles of *maqāsid al-sharī'ah* with a comparative analysis of positive-law regulations, and will examine digital-forensic evidence practices and victim-support mechanisms in Indonesia. The expected outcome is practical, principled policy recommendations to strengthen protection against deepfakes through a *maqāsid al-sharī'ah* approach in the digital age.

Methods

This research employs a normative methodology with a doctrinal approach, enriched by comparative analysis and a study of *maqāsid al-sharī'ah*.[21] The analysis was conducted on primary legal sources, including arguments drawn from the contemporary *maqāsid al-sharī'ah* literature. Positive law sources include Law No. 1 of 2024 concerning Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law No. 27 of 2022 concerning Personal Data Protection Law (PDP Law), and Law No. 12 of 2022 concerning Sexual Violence Crimes (TPKS Law). Secondary literature comprised scientific journal articles, digital-forensic reports, and relevant empirical data. Methodologically, the study combines three strands: (1) legal-text analysis paired with *maqāsid al-sharī'ah* interpretation to apply *maqāsid al-sharī'ah* principles to the threat of deepfakes; (2) comparative analysis of norms to identify regulatory gaps; and (3) content analysis to map digital-evidence practices.

An inductive data analysis approach is used, qualitative data are coded thematically and then synthesized into normative findings and policy recommendations. Validity is maintained through triangulation of sources among Islamic legal texts, positive law, and empirical evidence, and through triangulation of methods to ensure the traceability of conclusions.[22] Conclusions are drawn by prioritizing the convergence of evidence and the coherence between the principles of *maqāsid al-syarī'ah* and positive law provisions. Recommendations are formulated as operational, normative propositions and are constrained by empirical findings to ensure that the scope and limitations of the research are transparent.

---

[21] Faraji M. Rushagama, "Combined Doctrinal and Qualitative Approach in Legal Researches: An over View," *International Journal of Innovative Science and Research Technology* 9, no. 1 (2024): 1780–85, https://doi.org/10.5281/zenodo.10634265.

[22] Drishti Yadav, "Criteria for Good Qualitative Research: A Comprehensive Review," *The Asia-Pacific Education Researcher* 31, no. 6 (2022): 679–89, https://doi.org/10.1007/s40299-021-00619-0.

Results and Discussion

Dimensions of the deepfake threat

Deepfakes, generative AI products that synthesize faces, lip movements, and voices, pose significant technical challenges for biometric verification and multimedia forensics. Mika Witerslund's research shows that generative techniques—such as Generative Adversarial Networks (GANs), face swapping, and speech cloning—are becoming increasingly sophisticated, rendering synthetic visual and audio artifacts often indistinguishable from the originals to the naked eye.[23] Reliable detection therefore requires continuously learning forensic models together with layered verification protocols. The findings of a recent technical survey by Tianyi Wang et al. also confirm that detection methods must be rigorously evaluated for cross-dataset robustness and resistance to adaptive attacks, underscoring that technical solutions alone are insufficient without forensic laboratory accreditation standards and explainable evidence.[24]

From an epistemic perspective, the proliferation of deepfakes erodes the foundation of trust in audiovisual evidence. Don Fallis's research highlights how synthetic media can cause a "crisis of knowledge": when recordings can be convincingly faked, law-enforcement institutions lose the verification backstop that had relied on visual or audio evidence as an indicator of truth.[25] As a result, the burden of proof increases and litigation becomes more complex, because judges and forensic experts must assess not only a file's authenticity but also its processing chain, metadata, and the reliability of the detection methods used.[26] Early study by Joshua Habgood-Coote examining these epistemic risks developed this approach and explored its implications for the production and maintenance of public truth.[27]

The normative impact of deepfakes is extensive, encompassing defamation (including slander), blackmail, and sexual exploitation via synthetic pornography—all of which can harm victims' dignity, privacy, and social integrity.[28] Local empirical data show a sharp increase in incidents of fraud and other misuses of deepfakes: case-tracking organizations reported a marked rise

---

[23] Mika Westerlund, "The Emergence of Deepfake Technology: A Review," *Technology Innovation Management Review* 9, no. 11 (2019): 39–52, https://doi.org/10.22215/timreview/1282.

[24] Tianyi Wang et al., "Deepfake Detection: A Comprehensive Survey from the Reliability Perspective," *ACM Computing Surveys* 57, no. 3 (2025): 1–35, https://doi.org/10.1145/3699710.

[25] Don Fallis, "The Epistemic Threat of Deepfakes," *Philosophy & Technology* 34, no. 4 (2021): 623–43, https://doi.org/10.1007/s13347-020-00419-2.

[26] Danielle K. Citron and Robert Chesney, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics," *Foreign Affairs*, January 2019, https://perma.cc/TW6Z-Q97D.

[27] Joshua Habgood-Coote, "Deepfakes and the Epistemic Apocalypse," *Synthese* 201, no. 3 (2023): 103, https://doi.org/10.1007/s11229-023-04097-3.

[28] Furizal et al., "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review," *Social Sciences & Humanities Open* 12 (2025): 101882, https://doi.org/10.1016/j.ssaho.2025.101882.

in deepfake fraud between 2022 and 2023, underscoring the threat to individuals and institutions.[29] Moreover, limited forensic capacity and the absence of standard operating procedures for verification hinder the effective use or admissibility of digital evidence in judicial proceedings, thereby denying victims timely and effective remedies.[30] These findings underscore the normative imperative to define appropriate offenses and protection mechanisms that are responsive to the technical characteristics of the phenomenon.

Table 2. Dimensions of the deepfake threat

Dimensions	Risk Examples	Forensic and Policy Implications
Technical	Face or voice manipulation, biometric spoofing	Adaptive detector requirements, laboratory accreditation, model audits.
Epistemic	Erosion of trust in audiovisual recordings	Electronic chain-of-custody standards, cross-platform provenance verification.
Normative	Slander, synthetic pornography, blackmail	Formulation of specific offenses, rapid takedown mechanism, compensation scheme.

Source: processed by the author from various sources.

Table 2 summarizes the relationship among the dimensions of threat, concrete examples of impact, and the practical consequences for evidence collection and policy-making. The combination of these three elements is essential for digital evidence to be admissible and for legal protection to become not merely normative but also operational.

Theoretically, the *maqāsid al-sharī'ah* perspective provides an evaluative framework for assessing the moral and social harms caused by deepfakes—particularly with respect to *hifz al-'ird* (protection of honor), but also affecting *hifz al-dīn*, *hifz al-nafs*, *hifz al-'aql*, *hifz al-nasl*, and *hifz al-mal*. By placing *maqāsid al-sharī'ah* as a benchmark, the analysis not only quantifies individual harms but also evaluates systemic consequences for social cohesion and institutional legitimacy.[31] Therefore, this study recommends a transdisciplinary policy response that combines accountable forensic standards, evidentiary procedures consistent with Islamic evidentiary principles, and normative frameworks that prioritize restoring victims' dignity and safeguarding public trust.

Legal challenges in proving deepfakes

Indonesia's legal framework provides a partial normative basis for addressing the misuse of information technology (including deepfakes) but it does not yet fully account for the technical and forensic characteristics of AI products.[32]

[29] VIDA, "Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya."
[30] Amerini et al., "Deepfake Media Forensics: Status and Future Challenges."
[31] Sahajuddin et al., "Beyond Regulation: Rethinking Deepfake Pornography Prevention Through Digital Literacy."
[32] Nasution, Suteki, and Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse."

Relevant laws include the ITE Law (as a cyber umbrella), the PDP Law, and the TPKS Law, which establish obligations, data-subject rights, and sanctions that can be used to prosecute perpetrators and protect victims. However, doctrinal and literature reviews reveal a gap between these general norms and the specific technical evidentiary requirements encountered in court.[33]

Upon closer examination, the ITE Law contains provisions relevant to electronic content abuse. Examples include Article 27A (attacking honor or reputation), Articles 27B and 28 (which regulate content that "violates decency" and carry criminal sanctions), Article 29, Article 40(2)(b)–(c) (granting electronic-system operators the authority to terminate access or moderate content), and Article 45B (extortion via electronic media), all of which potentially provide administrative sanctions and authority for rapid response to deepfakes.[34] However, because these provisions are framed as general offences, such as defamation, dissemination of false information, and indecency, the technical elements specific to deepfakes (the synthesis process, cross-platform processing, and reusable model generators) are not explicitly mentioned in the text of the ITE Law.[35] This gap creates ambiguity in application and raises questions about the admissibility of AI-aware forensic evidence in court.

The PDP Law provides instruments that are highly relevant to victims of deepfakes: it defines the rights of data subjects, the obligations of data controllers, and mechanisms for access and deletion requests, as well as for recording processing traces.[36] For example, Articles 5, 7–13, and 31–34 establish core rights and obligations, while Article 43 sets out the obligation to delete data. Provisions on data protection impact assessments (DPIAs) and the obligation to record processing activities provide a procedural basis for investigating the processing chain that produces or disseminates deepfakes.[37] However, the implementation of these rights faces several challenges, including procedures for executing cross-platform deletion requests, ambiguity around response times, and limited capacity among controllers and supervisors to trace AI models and pipelines. Implementation studies by Wanda Iqwatul Qofifah et al. highlight the gap between the PDP Law's strong principles and enforcement capacity, and emphasize the need for rapid remedial mechanisms for victims.[38]

---

[33] Pamungkas, Sutarni, and Pranawa, "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity."

[34] Mahrina, Sasmito, and Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation."

[35] Pamungkas, Sutarni, and Pranawa, "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity."

[36] Supeno, Rosmidah, and Iqbal, "Personal Data Protection in Review of Legal Theories and Principles."

[37] Firsta Rahadatul 'Aisy, Muhammad Azil Maskur, and A.M Adzkiya' Amiruddin, "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore," *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431–82, https://doi.org/10.15294/jils.v10i1.13755.

[38] Wanda Iqwatul Qofifah et al., "Organizational Communication Ethics and Personal Data Protection: A Review of the Personal Data Protection Law," *SHISHYA: Studies and*

The TPKS Law classifies electronically facilitated sexual violence as a distinct category within the national criminal code.[39] Specifically, Article 4 and related provisions define its forms and establish obligations to provide restitution and other rights to victims as part of criminal sentencing and special judicial mechanisms.[40] The law permits the imposition of sanctions and the award of redress where deepfakes are used for sexual exploitation, including synthetic pornography, threats to disseminate intimate material, or blackmail predicated on the threatened publication of synthetic material.[41]

However, practical studies indicate the need to expand the definitions, develop guidelines for AI-based forensic electronic evidence, and improve inter-agency coordination to ensure the consistent application of criminal elements for deepfakes and the calculation of restitution.[42] Analytical studies and international NGOs addressing online gender-based violence have made the same recommendation.[43] This gap in substantive and procedural rules underscores the urgent need to formulate an integrative framework grounded in *maqāsid al-sharī'ah*, as proposed in this study.

Implications for the *maqāsid al-syarī'ah*

From the perspective of *maqāsid al-sharī'ah*, deepfake attacks on an individual's honor and reputation constitute a direct violation of the objective of protecting honor (*hifz al-'ird*). Audiovisual manipulation that depicts a person in humiliating or defamatory contexts not only damages the individual's reputation but also erodes the social fabric that sustains collective honor.[44] This harm is central to maintaining human dignity in the *maqāsid al-sharī'ah* literature.[45] Legal and policy studies indicate that such reputational harms can have long-term effects on victims' employment, community participation, and access to justice.[46] As Danielle K. Citron and Robert Chesney argue, deepfakes

---

Perspectives on Law and Justice 2, no. 1 (2026): 47–63, https://nayottamareswara.co.id/index.php/jhpa/article/view/27.

39 Santoso and Satria, "Sexual-Violence Offenses in Indonesia: Analysis of the Criminal Policy in the Law Number 12 of 2022."

40 Eva Khumairoh, Ishaq Ishaq, and Muhammad Faisol, "Marital Rape As A Crime Of Sexual Violence In Positive Law In Indonesia," *International Journal of Law, Crime and Justice* 1, no. 2 (2024): 51–66, https://doi.org/10.62951/ijlcj.v1i2.59.

41 Nasution, Suteki, and Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse."

42 Nasution, Suteki, and Lumbanraja.

43 Cristóbal Guerra et al., "Online Sexual Harassment and Depression in Chilean Adolescents: Variations Based on Gender and Age of the Offenders," *Child Abuse & Neglect* 120 (2021): 105219, https://doi.org/10.1016/j.chiabu.2021.105219; Selena Mariano, "The 'Double Bind' of Gender-Based Violence: Secondary Victimization in Courtroom Cross-Examinations," *Behavioral Sciences & the Law*, 2025, 1–13, https://doi.org/10.1002/bsl.70025.

44 Sahajuddin et al., "Beyond Regulation: Rethinking Deepfake Pornography Prevention Through Digital Literacy."

45 Ramadhani, Rachmawati, and Kurnikova, "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia."

46 Furizal et al., "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review"; Pamungkas, Sutarni,

require legal responses that are restorative and preventive as well as retributive;[47] accordingly, the protection of *hifz al-'ird* should be the starting point for formulating offences and remedial mechanisms consistent with *maqāsid al-sharī'ah*.

The effects of deepfakes extend to other *maqāsid al-sharī'ah*, particularly *hifz al-din* (protection of religion) and *hifz al-nafs* (protection of life). Manipulation of content targeting religious figures, religious messages, or worship events can provoke social unrest, exacerbate sectarian tensions, and disrupt safe religious practices, thereby threatening community stability and security.[48] Conversely, deepfakes used to induce panic, carry out periodic fraud, or perpetrate emotional deception can inflict severe psychological trauma on victims,[49] an issue that directly concerns the dimension of *hifz al-nafs*. Mika Westerlund's study also shows that improvements in deepfake quality accelerate the spread of disinformation and undermine the ability of communities and institutions to distinguish between authentic and fabricated information.[50]

The epistemic and cognitive effects of deepfakes implicate the *maqāsid al-sharī'ah*, particularly *hifz al-'aql* (protection of reason) and *hifz al-nasl* (protection of lineage). Erosion of public trust in audiovisual evidence undermines public rationality and decision making (core aspects of *hifz al-'aql*) because evidence-based arguments become susceptible to manipulation.[51] Moreover, deepfakes that falsify private messages or recordings can fracture family relationships, generate false accusations about lineage or sexual conduct, and thereby threaten *hifz al-nasl*.[52] These developments mean that standards of proof and verification mechanisms must account for broader cognitive and social harms, not merely the technical authenticity of files, in order to safeguard the right to truthful knowledge and the protection of lineage.

From the perspective of Islamic legal jurisprudence (*ijtihād*), the concepts of criminal offenses, evidence, and sanctions should be reformulated using the *maqāsid al-sharī'ah* as a normative guide.[53] This requires defining specific

---

and Pranawa, "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity."

47 Citron and Chesney, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics."

48 Hijriatu Sakinah, Arsy Shakila Putri, and Ainur Rofiq, "Islamic Ethical Analysis of Deepfakes and Religious Image Manipulation," *Jurnal Lentera Insani* 1, no. 2 (2025): 141–56, https://doi.org/10.65586/jli.v1i2.28.

49 Fallis, "The Epistemic Threat of Deepfakes."

50 Westerlund, "The Emergence of Deepfake Technology: A Review."

51 John Twomey et al., "Do Deepfake Videos Undermine Our Epistemic Trust? A Thematic Analysis of Tweets That Discuss Deepfakes in the Russian Invasion of Ukraine," *PLOS ONE* 18, no. 10 (2023): e0291668, https://doi.org/10.1371/journal.pone.0291668; Habgood-Coote, "Deepfakes and the Epistemic Apocalypse."

52 Nasution, Suteki, and Lumbanraja, "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse."

53 Fauzan Arrasyid et al., "The Progressivity of Umar Ibn Al-Khattab's Ijtihad in Responding to Community Social Changes," *Al-Istinbath: Jurnal Hukum Islam* 8, no. 1 (2023): 21–36, https://doi.org/10.29240/jhi.v8i1.4872.

elements of offences that accommodate the technical characteristics of deepfakes. For example, intentional synthesis, intent to defame or degrade, and cross-platform distribution, while also establishing evidentiary standards that respect sharia principles yet adapt to the realities of digital proof.[54] Practical measures might include accredited forensic laboratory examination, a secure electronic chain-of-custody for digital artefacts, and rigorous evaluation and validation of detection methods. This framework opens space for a proportional *ta'zīr* sanction model and restorative justice mechanisms that prioritize restoring the victim's honour and social integrity rather than focusing solely on retribution, thereby aligning criminal responses with the demands of *maqāsid al-sharī'ah* without sacrificing procedural fairness.[55]

The practical policy implications of this *maqāsid al-sharī'ah*-based analysis must be transdisciplinary and operational. Normative recommendations include filling regulatory gaps by creating specific deepfake offences within technical regulations; developing AI-aware forensic evidence SOPs; accrediting laboratories and certifying digital-forensics workflows; and establishing recovery mechanisms such as compensation, takedown and correction orders, and reputational rehabilitation. Moreover, harmonization between *maqāsid al-sharī'ah*-informed sharia norms and positive law, achieved through collaborative mechanisms linking religious courts, civil courts, data regulators, and forensic institutions, will help ensure that policy implementation is both normatively legitimate and technically effective. Such a framework offers an integrative model that aligns the principles of *maqāsid al-sharī'ah* with adequate legal instruments and contemporary evidence mechanisms.

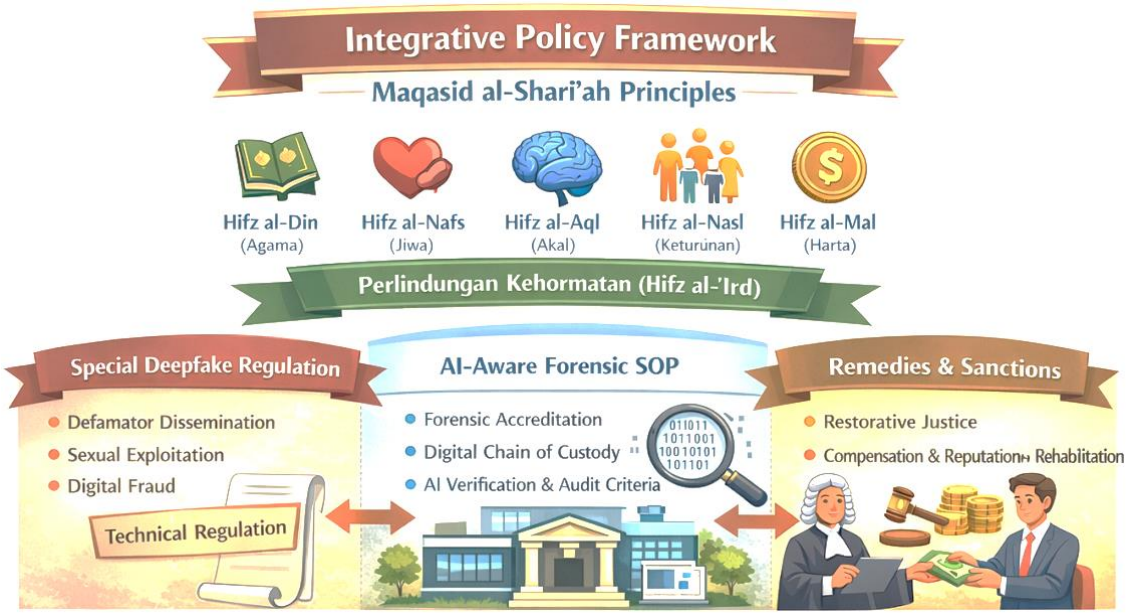

Figure 1. Integrative policy framework of *maqāsid al-sharī'ah*

[54] Sahajuddin et al., "Beyond Regulation: Rethinking Deepfake Pornography Prevention Through Digital Literacy."

[55] Djalaluddin et al., "The Implementation of Ta'zīr Punishment as an Educational Reinforcement in Islamic Law."

An integrative Islamic legal framework

The proposed framework situates *maqāsid al-sharī'ah* as the primary normative principle guiding the formulation of offences, evidentiary standards, and sanctioning mechanismsi. The *maqāsid al-sharī'ah* should function not merely as a procedural guide but as a substantive benchmark for the legitimacy and finality of new norms: every novel rule must be evaluated by its capacity to protect *hifz al-'ird* (honour) alongside the other fundamental protections.[56] In practice, this requires that offences be defined with both elements of conduct (*actus reus*) and mental state (*mens rea*), and that remedial mechanisms be built in to restore victims' dignity and to prevent erosion of public trust.[57] The resulting integrative framework seeks balance—clearly proscribing harmful behaviour while preserving avenues for recovery that uphold *maqāsid al-sharī'ah* principles without compromising procedural rights.

First, the normative component: specific deepfake offences must identify concrete technical elements and culpable intent. For example, the creation or dissemination of synthetic audiovisual material intended to degrade a person's honour, to sexually exploit, or to deceive for profit should be an offence; cross-platform publication and repeated distribution can be treated as aggravating circumstances. This approach accords with policy arguments calling for new norms to counter systemic threats of disinformation and identity manipulation, as discussed by Danielle K. Citron and Robert Chesney.[58]

Second, the evidentiary component: adopt AI-aware admissibility rules and forensic practices. Because deepfake materials are artefactual and trivially reproducible, the framework proposes three integrated procedural mechanisms:

1. accreditation of forensic laboratories that validate detection algorithms;
2. implementation of an electronic chain-of-custody that records provenance, metadata, and cryptographic hashes across distribution channels; and
3. admissibility criteria that combine Sharia evidential principles (reliability, credibility, and fact-correlation) with contemporary forensic standards.

These requirements are supported by technical literature, including work by Mika Westerlund, which highlights the adaptive nature of generative methods and current limits of detection.[59]

Third, sanctions and remediation: a model of proportional *ta'zīr* coupled with restorative justice. Within a *maqāsid al-sharī'ah*, sanctions should be corrective and rehabilitative as well as proportional, prioritizing restoration of

---

[56] Mohammad Hashim Kamali, "Meaning and Definition of Maqasid," in *Goals and Purposes of Shariah: Maqasid in Theory and Practice* (Oxford, NY: Oxford University Press, 2025), 11–19, https://doi.org/10.1093/9780197786390.003.0003.

[57] Erica Beecher-Monas and Edgar Garcia-Rill, "Actus Reus, Mens Rea, and Brain Science: What Do Volition and Intent Really Mean?," *Kentucky Law Journal* 106, no. 2 (2017): 265–314, https://uknowledge.uky.edu/klj/vol106/iss2/5.

[58] Citron and Chesney, "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics."

[59] Westerlund, "The Emergence of Deepfake Technology: A Review."

the victim's dignity and prevention of recurrence.[60] The model therefore combines discretionary *ta'zīr* (scaled to severity and intent), mandatory corrections and takedown orders, a restorative compensation fund, and structured reputation-rehabilitation programs. This restorative orientation mirrors theories of justice applicable to non-material harms and supports the *maqāsid al-sharī'ah* objective of restoring social order rather than merely exacting punishment.[61]

Fourth, integration with statutory instruments and institutional architecture. The framework is designed for mainstreaming, via implementing regulations, technical guidelines, or inter-agency memoranda, into instruments such as the ITE Law, PDP Law, and TPKS Law. Operationalisation requires coordinated bodies: accredited forensic teams, specialised litigation units, and judicial panels with digital-forensics expertise to expedite evidentiary evaluation. Complementary measures—rapid takedown protocols, expedited compensation pathways, and clear referral mechanisms between religious and civil fora—are necessary to limit reputational harm before it proliferates.[62]

Fifth, safeguards and the principle of prudence. To avoid oversuppression, wrongful takedowns, and authoritarian misuse, the framework should adopt narrow mens rea elements for criminal liability, high evidentiary thresholds for criminal prosecution, prompt appeal remedies, and algorithmic transparency and auditability in forensic processes. Balancing *maqāsid al-sharī'ah*-based protections with human-rights norms requires adherence to proportionality, due process, and institutional independence. Empirical and theoretical studies on institutional legitimacy likewise underline the importance of these safeguards.[63] Maria Palewec's theoretical study on the impact of deepfakes on institutional legitimacy confirms the need for such safeguards to prevent policy side effects that undermine democracy and public trust.[64]

Mechanisms for implementation, governance, and evaluation

The proposed implementation plan is pilot-driven, multi-stakeholder, and phased. It engages ministries, technical agencies, law-enforcement bodies (for example, the Ministry of Law and Human Rights, the Supreme Court, the

---

60 Ibrahim et al., "Integration of Maqaṣid Al-Shari'ah in the Criminal Law Reform to Achieve Justice and Human Dignity."

61 Edi Rosman et al., "Tulou as a Customary Criminal Sanction in Mentawai: Convergensi of Customary and Islamic Law for Social Reconciliation," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 9, no. 3 (2025), https://doi.org/10.22373/sjhk.v9i3.30100.

62 Dody Novizar Mardyansyah et al., "Harmonization of Personal Data Protection Principles With Electronic Justice Systems In Indonesia," *Yuridika* 40, no. 3 (2025): 343–68, https://doi.org/10.20473/ydk.v40i3.74179.

63 Tarmizi Tahir and Syeikh Hasan Abdel Hamid, "Maqasid Al-Syari'ah Transformation in Law Implementation for Humanity," *International Journal Ihya' 'Ulum Al-Din* 26, no. 1 (2024): 119–31, https://doi.org/10.21580/ihya.26.1.20248.

64 Maria Pawelec, "Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions," *Digital Society* 1, no. 2 (2022): 19, https://doi.org/10.1007/s44206-022-00010-6.

Ministry of Communication and Information Technology, and the Criminal Investigation Agency), and data-protection authorities. Initial stages should include drafting implementing regulations and technical SOPs, developing accredited forensic laboratories, and creating a rapid reporting channel. The pilot will be tested at the provincial level to observe technical, judicial, and policy effects before national adaptation. This phased approach is consistent with research by Alexander Romanishyn et al., which recommends policies that emphasize the need for testing AI-driven disinformation policies so that responses remain adaptive to technological evolution.[65]

Operational governance is to be delivered through an inter-agency steering committee for strategy, resource allocation, and pilot priorities, supported by technical working groups (forensics, law, victim protection, public communication). As argued by Isa Ismail and Khairul Akram Zainol Ariffin, courts should incorporate IT/forensic expert panels to accelerate admissibility decisions and reduce retrial burdens.[66] From a governance theory perspective, this type of vertical-horizontal coordination mechanism reduces policy fragmentation and promotes the synchronization of technical norms with judicial procedures.[67] This is also reflected in recent research by Khadiza Laskor et al., which recommends multi-stakeholder governance for issues related to digital and AI due to their cross-sectoral and cross-border nature.[68] As a normative-operational foundation, the establishment of MoUs and technical guidelines will facilitate inter-agency interoperability and rapid access to forensic resources.[69]

---

[65] Alexander Romanishyn, Olena Malytska, and Vitaliy Goncharuk, "AI-Driven Disinformation: Policy Recommendations for Democratic Resilience," *Frontiers in Artificial Intelligence* 8 (2025): 1569115, https://doi.org/10.3389/frai.2025.1569115.

[66] Isa Ismail and Khairul Akram Zainol Ariffin, "The Admissibility of Digital Evidence from Open-Source Forensic Tools: Development of a Framework for Legal Acceptance," *PLOS One* 20, no. 9 (2025): e0331683, https://doi.org/10.1371/journal.pone.0331683.

[67] Iveta Reinholde, Malvīne Stučka, and Ilze Auliciema, "Bridging Levels of Governance: The Dynamics of Vertical and Horizontal Intergovernmental Relations in Latvia," in *Horizontal Intergovernmental Coordination at Local and Regional Levels*, ed. Nathalie Behnke and Bettina Petersohn (Cham: Springer Nature Switzerland, 2025), 179–200, https://doi.org/10.1007/978-3-031-83567-4_10.

[68] Khadiza Laskor, Richard Owen, and Andrew Charlesworth, "Multi-Stakeholder Perspectives on Governing Innovation in the Digital Afterlife," *Journal of Responsible Technology* 25 (2026): 100150, https://doi.org/10.1016/j.jrt.2026.100150.

[69] Christian Kraetzer et al., "Process-Driven Modelling of Media Forensic Investigations-Considerations on the Example of DeepFake Detection," *Sensors* 22, no. 9 (2022): 3137, https://doi.org/10.3390/s22093137.

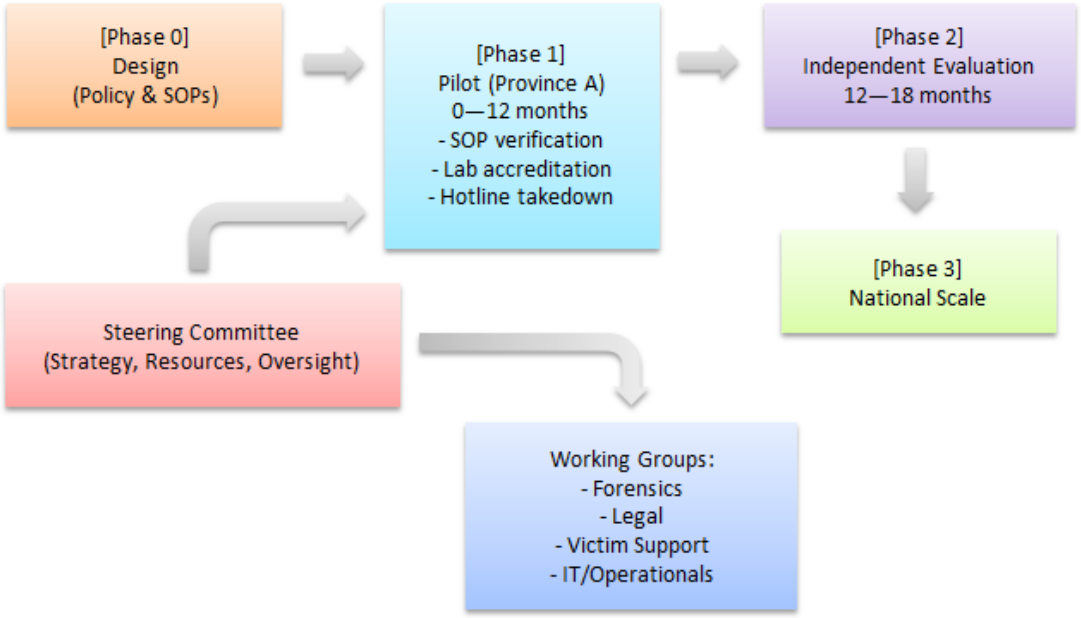

Figure 2. Implementation roadmap: pilot-driven multi-stakeholder flow

The illustration above explains the implementation flow: design of norms or SOPs (Phase 0), controlled field testing (Phase 1) with clear operational indicators, independent evaluation (Phase 2) to assess effectiveness and cost-benefit, and adaptation before national scale (Phase 3). This explanation emphasizes that digital evidence verification SOPs (electronic chain-of-custody, laboratory accreditation, and rapid takedown protocols) must be tested in conjunction with victim remediation mechanisms (restorative compensation, correction publication) so that policies can balance technical responses and *maqāsid al-sharī'ah* protection. Technical and policy studies show that without a measurable trial phase, takedown and verification initiatives tend to fail to meet standards of admissibility and legitimacy in court.

The evaluation mechanism is designed based on pragmatic measurable indicators, including:

1. the level of SOP adoption by courts and law enforcement agencies;
2. the ratio of reports that lead to legal proceedings versus reports that are taken down;
3. average time taken to implement a takedown since reporting;
4. victim satisfaction and recovery index (victim surveys on reputation rehabilitation and compensation); and
5. forensic laboratory performance metrics (analysis time, detection accuracy, and model audit)

Independent evaluations during the first 12–18 months serve to validate pilot assumptions (technical, legal, and cost-effectiveness) and provide empirical evidence for legislative decision-making and broader budget allocation. Empirical evidence from Indonesia on the surge in deepfake

incidents reinforces the urgency of time-sensitive and outcome-oriented indicators.

The sustainability and legitimacy of the policy depend on safeguards and financing strategies. Safeguards include narrow limits on the definition of offenses so as not to restrict freedom of expression, high standards of mens rea for criminal offenses, rapid appeal mechanisms to review takedowns, and independent audits of algorithms and forensic laboratories to prevent errors and bias. In terms of financing, priority is initially given to reallocating existing training and forensic program budgets, supplemented by public-private partnerships for accreditation, so that new funding requirements are minimal and politically more acceptable. This framework also fulfills the research objective: to design recommendations that are operational, evidence-based, and compatible with *maqāsid al-sharī'ah*, prioritizing the restoration of honor and protection of victims while maintaining the principle of procedural justice.

Conclusion

This study concludes that the threat posed by deepfakes transcends technical challenges and strikes directly at the realization of *maqāsid al-sharī'ah*, most immediately the protection of honour (*hifz al-'ird*), while also imperiling the protections of religion, life, reason, lineage, and property. Doctrinal analysis, statutory review, and empirical inquiry reveal normative gaps and shortfalls in forensic capacity that render existing legal instruments ill-suited to the distinct features of deepfakes—synthetic manipulation, cross-platform distribution chains, and the necessity for AI-aware evidentiary practices.

In response, the study proposes an integrative Islamic-legal framework that combines narrowly defined criminal offences tailored to technical elements and intent, validated forensic evidence standards, and proportional *ta'zīr* sanctions integrated with restorative-justice remedies. Framed by *maqāsid al-sharī'ah* principles, the model emphasizes remediation of victims' dignity alongside accountability, so that legal responses are corrective and restorative rather than merely repressive.

For practical implementation, the study recommends a pilot-driven, multi-stakeholder rollout and cross-institutional governance that prioritize: accredited forensic laboratories, secure electronic chains-of-custody, AI-aware verification SOPs, rapid reporting and takedown channels, and measurable evaluation indicators to assess effectiveness before national scale-up. Essential normative safeguards—narrow *mens rea* requirements to avoid overbreadth, high evidentiary standards for criminal enforcement, rapid appeal and counter-notice procedures, and independent audits of forensic tools—are necessary to preserve fundamental freedoms while protecting *maqāsid al-sharī'ah* goals. Finally, while this research provides a conceptual and operational blueprint for policymakers and courts, its long-term effectiveness depends on empirical pilot testing, independent monitoring, iterative refinement, and continual adaptation to technological evolution.

Acknowledgements

The authors express their sincere gratitude to the editor and the anonymous reviewers for their careful reading and constructive suggestions, which materially improved the quality of this manuscript.

Disclosure Statement

Certain sections of this manuscript were edited using Grammarly to enhance grammar and clarity, and one figure was generated with the assistance of ChatGPT. All material produced with the aid of these artificial-intelligence tools was critically reviewed, validated, and approved by the authors, who accept full responsibility for the final content. The authors also declare no financial, personal, or professional conflicts of interest in relation to this work.

Author Contributions

Conceptualization was undertaken by D.R.N.F. and R.D.; methodology was developed by N.D.L. and R.D.; validation was performed by T.A.S. and D.R.N.F.; supervision was provided by N.D.L. and A.I.L.; the initial draft was prepared by D.R.N.F., R.D., and T.A.S.; and all authors participated in the review and editing of the manuscript. All authors have read and approved the final version.

References

'Aisy, Firsta Rahadatul, Muhammad Azil Maskur, and A.M Adzkiya' Amiruddin. "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore." *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431–82. https://doi.org/10.15294/jils.v10i1.13755.

Amerini, Irene, Mauro Barni, Sebastiano Battiato, Paolo Bestagini, Giulia Boato, Vittoria Bruni, Roberto Caldelli, et al. "Deepfake Media Forensics: Status and Future Challenges." *Journal of Imaging* 11, no. 3 (2025): 73. https://doi.org/10.3390/jimaging11030073.

Arrasyid, Fauzan, Pagar Pagar, Dhiauddin Tanjung, and Mohd Roslan Mohd Nor. "The Progressivity of Umar Ibn Al-Khattab's Ijtihad in Responding to Community Social Changes." *Al-Istinbath: Jurnal Hukum Islam* 8, no. 1 (2023): 21–36. https://doi.org/10.29240/jhi.v8i1.4872.

Beecher-Monas, Erica, and Edgar Garcia-Rill. "Actus Reus, Mens Rea, and Brain Science: What Do Volition and Intent Really Mean?" *Kentucky Law Journal* 106, no. 2 (2017): 265–314. https://uknowledge.uky.edu/klj/vol106/iss2/5.

Citron, Danielle K., and Robert Chesney. "Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics." *Foreign Affairs*, January 2019. https://perma.cc/TW6Z-Q97D.

Dinas Kominfo Provinsi Jawa Timur. "Polda Jatim Ungkap Kasus Penipuan Deepfake AI Kepala Daerah, Pelaku Kantongi Keuntungan Hingga Rp87 Juta." Dinas Kominfo Provinsi Jawa Timur, April 28, 2025. https://kominfo.jatimprov.go.id/berita/polda-jatim-ungkap-kasus-penipuan-deepfake-ai-kepala-daerah-pelaku-kantongi-keuntungan-hingga-rp87-juta.

Djalaluddin, Muhammad Mawardi, Bulqia Mas'ud, Dedy Sumardi, Isnawardatul Bararah, and Kamus Kamus. "The Implementation of Ta'zīr Punishment as an Educational Reinforcement in Islamic Law." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 7, no. 1 (2023): 399–417. https://doi.org/10.22373/sjhk.v7i1.15101.

Fallis, Don. "The Epistemic Threat of Deepfakes." *Philosophy & Technology* 34, no. 4 (2021): 623–43. https://doi.org/10.1007/s13347-020-00419-2.

Furizal, Alfian Ma'arif, Hari Maghfiroh, Iswanto Suwarno, Denis Prayogi, Kariyamin, Syahrani Lonang, and Abdel-Nasser Sharkawy. "Social, Legal, and Ethical Implications of AI-Generated Deepfake Pornography on Digital Platforms: A Systematic Literature Review." *Social Sciences & Humanities Open* 12 (2025): 101882. https://doi.org/10.1016/j.ssaho.2025.101882.

Guerra, Cristóbal, Cristián Pinto-Cortez, Edgardo Toro, Erifili Efthymiadou, and Ethel Quayle. "Online Sexual Harassment and Depression in Chilean Adolescents: Variations Based on Gender and Age of the Offenders." *Child Abuse & Neglect* 120 (2021): 105219. https://doi.org/10.1016/j.chiabu.2021.105219.

Habgood-Coote, Joshua. "Deepfakes and the Epistemic Apocalypse." *Synthese* 201, no. 3 (2023): 103. https://doi.org/10.1007/s11229-023-04097-3.

Ibrahim, Zumiyati Sanu, Suud Sarim Karimullah, Andi Istiqlal Assaad, Rina Septiani, and Huseyin Okur. "Integration of Maqaṣid Al-Shari'ah in the Criminal Law Reform to Achieve Justice and Human Dignity." *Jurnal Hukum Islam* 23, no. 1 (2025): 105–44. https://doi.org/10.28918/jhi.v23i1.04.

Ismail, Isa, and Khairul Akram Zainol Ariffin. "The Admissibility of Digital Evidence from Open-Source Forensic Tools: Development of a Framework for Legal Acceptance." *PLOS One* 20, no. 9 (2025): e0331683. https://doi.org/10.1371/journal.pone.0331683.

Kamali, Mohammad Hashim. "Meaning and Definition of Maqasid." In *Goals and Purposes of Shariah: Maqasid in Theory and Practice*, 11–19. Oxford, NY: Oxford University Press, 2025. https://doi.org/10.1093/9780197786390.003.0003.

Khumairoh, Eva, Ishaq Ishaq, and Muhammad Faisol. "Marital Rape As A Crime Of Sexual Violence In Positive Law In Indonesia." *International Journal of Law, Crime and Justice* 1, no. 2 (2024): 51–66. https://doi.org/10.62951/ijlcj.v1i2.59.

Kraetzer, Christian, Dennis Siegel, Stefan Seidlitz, and Jana Dittmann. "Process-Driven Modelling of Media Forensic Investigations-Considerations on the Example of DeepFake Detection." *Sensors* 22, no. 9 (2022): 3137. https://doi.org/10.3390/s22093137.

Laskor, Khadiza, Richard Owen, and Andrew Charlesworth. "Multi-Stakeholder Perspectives on Governing Innovation in the Digital Afterlife." *Journal of Responsible Technology* 25 (2026): 100150. https://doi.org/10.1016/j.jrt.2026.100150.

Loovens, Jenifer, and Hasan Tinmaz. "A Systematic Literature Review of Deepfakes in Forensic Science." *Forensic Imaging* 43 (2025): 200647. https://doi.org/10.1016/j.fri.2025.200647.

Lundberg, Ebba, and Peter Mozelius. "The Potential Effects of Deepfakes on News Media and Entertainment." *AI & SOCIETY* 40, no. 4 (2025): 2159–70. https://doi.org/10.1007/s00146-024-02072-1.

Mahrina, Mahrina, Joko Sasmito, and Candra Zonyfar. "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation." *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 21, no. 2 (2023): 345–62. https://doi.org/10.31941/pj.v21i2.2680.

Mardyansyah, Dody Novizar, Sukarmi Sukarmi, Adi Kusumaningrum, and Yenny Eta Widyanti. "Harmonization of Personal Data Protection Principles With Electronic Justice Systems In Indonesia." *Yuridika* 40, no. 3 (2025): 343–68. https://doi.org/10.20473/ydk.v40i3.74179.

Mariano, Selena. "The 'Double Bind' of Gender-Based Violence: Secondary Victimization in Courtroom Cross-Examinations." *Behavioral Sciences & the Law*, 2025, 1–13. https://doi.org/10.1002/bsl.70025.

Mustak, Mekhail, Joni Salminen, Matti Mäntymäki, Arafat Rahman, and Yogesh K. Dwivedi. "Deepfakes: Deceptions, Mitigations, and Opportunities." *Journal of Business Research* 154 (2023): 113368. https://doi.org/10.1016/j.jbusres.2022.113368.

Nasution, Angelica Vanessa Audrey, Suteki, and Anggita Doramia Lumbanraja. "Addressing Deepfake Pornography and the Right to Be Forgotten in Indonesia: Legal Challenges in the Era of AI-Driven Sexual Abuse." *International Journal for the Semiotics of Law* 38, no. 7 (2025): 2489–2517. https://doi.org/10.1007/s11196-025-10265-0.

Nur, Iffatin, Syahrul Adam, and M. Ngizzul Muttaqien. "Maqāṣid Al-Sharī'at: The Main Reference and Ethical-Spiritual Foundation for the Dynamization Process of Islamic Law." *Ahkam: Jurnal Ilmu Syariah* 20, no. 2 (2020): 331–60. https://doi.org/10.15408/ajis.v20i2.18333.

Pamungkas, Abdul Aziz, Nanik Sutarni, and Burham Pranawa. "Legal Analysis of Deepfake Technology in Indonesia from the Perspective of Fair and Civilized Humanity." *Pena Justisia: Media Komunikasi Dan Kajian Hukum* 24,

no. 1 (2025): 4562–74. https://doi.org/10.31941/pj.v24i2.6311.

Pawelec, Maria. "Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions." *Digital Society* 1, no. 2 (2022): 19. https://doi.org/10.1007/s44206-022-00010-6.

Qofifah, Wanda Iqwatul, Muhammad Dirgantara, Fadhlan Maulana, and Zul Fahmi. "Organizational Communication Ethics and Personal Data Protection: A Review of the Personal Data Protection Law." *SHISHYA: Studies and Perspectives on Law and Justice* 2, no. 1 (2026): 47–63. https://nayottamareswara.co.id/index.php/jhpa/article/view/27.

Ramadhani, Evyta Rosiyanti, Ayudya Rizqi Rachmawati, and Roro Hera Kurnikova. "Integrating Islamic Values with the Right to Be Forgotten: A Legal Approach to Addressing Deepfake Pornography in Indonesia." *De Jure: Jurnal Hukum Dan Syar'iah* 17, no. 1 (2025): 112–31. https://doi.org/10.18860/j-fsh.v17i1.28880.

Reinholde, Iveta, Malvīne Stučka, and Ilze Auliciema. "Bridging Levels of Governance: The Dynamics of Vertical and Horizontal Intergovernmental Relations in Latvia." In *Horizontal Intergovernmental Coordination at Local and Regional Levels*, edited by Nathalie Behnke and Bettina Petersohn, 179–200. Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-83567-4_10.

Romanishyn, Alexander, Olena Malytska, and Vitaliy Goncharuk. "AI-Driven Disinformation: Policy Recommendations for Democratic Resilience." *Frontiers in Artificial Intelligence* 8 (2025): 1569115. https://doi.org/10.3389/frai.2025.1569115.

Romero-Moreno, Felipe. "Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content." *International Review of Law, Computers & Technology* 38, no. 3 (2024): 297–326. https://doi.org/10.1080/13600869.2024.2324540.

Rosman, Edi, Elfiani Elfiani, Hidayatul Azizah, and Ferdi Yufriadi. "Tulou as a Customary Criminal Sanction in Mentawai: Convergensi of Customary and Islamic Law for Social Reconciliation." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 9, no. 3 (2025). https://doi.org/10.22373/sjhk.v9i3.30100.

Ruhtiani, Maya, Yuris Tri Naili, Astika Nurul Hidayah, and Hyun Kyung Park. "Generative AI and Copyright Law: A Rule of Law Comparison between Indonesia and South Korea." *Kosmik Hukum* 25, no. 3 (2025): 428–49. https://doi.org/10.30595/kosmikhukum.v25i3.26268.

Rushagama, Faraji M. "Combined Doctrinal and Qualitative Approach in Legal Researches: An over View." *International Journal of Innovative Science and Research Technology* 9, no. 1 (2024): 1780–85. https://doi.org/10.5281/zenodo.10634265.

Sahajuddin, Ansaar, Abdul Hafid, Erlita Tantri, Entis Sutisna, and Sri Najiyati. "Beyond Regulation: Rethinking Deepfake Pornography Prevention Through Digital Literacy." *JURIS (Jurnal Ilmiah Syariah)* 24, no. 2 (2025): 357–67. https://doi.org/10.31958/juris.v24i2.15775.

Sakinah, Hijriatu, Arsy Shakila Putri, and Ainur Rofiq. "Islamic Ethical Analysis of Deepfakes and Religious Image Manipulation." *Jurnal Lentera Insani* 1, no. 2 (2025): 141–56. https://doi.org/10.65586/jli.v1i2.28.

Santoso, Topo, and Hariman Satria. "Sexual-Violence Offenses in Indonesia: Analysis of the Criminal Policy in the Law Number 12 of 2022." *Padjadjaran Jurnal Ilmu Hukum* 10, no. 1 (2023): 59–79. https://doi.org/10.22304/pjih.v10n1.a4.

Sodiqin, Ali. "Legal, Moral, and Spiritual Dialectics in The Islamic Restorative Justice System." *Ahkam: Jurnal Ilmu Syariah* 21, no. 2 (2021): 357–78. https://doi.org/10.15408/ajis.v21i2.22675.

Supeno, Supeno, Rosmidah Rosmidah, and Syed Mohd Uzair Iqbal. "Personal Data Protection in Review of Legal Theories and Principles." *Journal of Law and Legal Reform* 6, no. 3 (2025): 1349–76. https://doi.org/10.15294/jllr.v6i3.10252.

Tahir, Tarmizi, and Syeikh Hasan Abdel Hamid. "Maqasid Al-Syari'ah Transformation in Law Implementation for Humanity." *International Journal Ihya' 'Ulum Al-Din* 26, no. 1 (2024): 119–31. https://doi.org/10.21580/ihya.26.1.20248.

Twomey, John, Didier Ching, Matthew Peter Aylett, Michael Quayle, Conor Linehan, and Gillian Murphy. "Do Deepfake Videos Undermine Our Epistemic Trust? A Thematic Analysis of Tweets That Discuss Deepfakes in the Russian Invasion of Ukraine." *PLOS ONE* 18, no. 10 (2023): e0291668. https://doi.org/10.1371/journal.pone.0291668.

VIDA. "Penipuan Deepfake Indonesia Melonjak 1550%: Begini Cara VIDA Memeranginya." VIDA, October 28, 2024. https://vida.id/id/pressrelease/penipuan-deepfake-indonesia-melonjak-1550-begini-cara-vida-memeranginya.

Wang, Tianyi, Xin Liao, Kam Pui Chow, Xiaodong Lin, and Yinglong Wang. "Deepfake Detection: A Comprehensive Survey from the Reliability Perspective." *ACM Computing Surveys* 57, no. 3 (2025): 1–35. https://doi.org/10.1145/3699710.

Westerlund, Mika. "The Emergence of Deepfake Technology: A Review." *Technology Innovation Management Review* 9, no. 11 (2019): 39–52. https://doi.org/10.22215/timreview/1282.

Yadav, Drishti. "Criteria for Good Qualitative Research: A Comprehensive Review." *The Asia-Pacific Education Researcher* 31, no. 6 (2022): 679–89. https://doi.org/10.1007/s40299-021-00619-0.