

Integrating Islamic Ethical Principles into Nigeria's AI Surveillance Policy: A Human Dignity Approach

Abubakar muhammad jibril¹, Sulaiman Dalha Ahmad²

¹ University of Indonesia, Indonesia

² Islamic University of Niger, Niger Republic

Histori Naskah

Diserahkan:
November 5, 2025

Direvisi:
May 3, 2026

Diterima:
October 12, 2026

ABSTRACT

In the era of hyper-digitalization, AI has exponentially expanded the size and scope of state surveillance globally, pushing fundamental ethical questions of privacy, discrimination, and human dignity to the forefront. In Nigeria, the rapid development of digital identity systems and compulsory SIM-to-ID registrations has established a significant real-time surveillance potential, yet AI-specific legal protections remain underdeveloped. Though the Nigerian Constitution and Nigerian Data Protection Act (NDPA) 2023 provide general rights to privacy, there is little incorporation of local religious and cultural frameworks in AI regulation. This article discusses how fundamental Islamic ethical principles, derived from maqāsid al-sharī'ah, i.e., protection of honor (ḥifẓ al-'ird), life (ḥifẓ al-nafs), intellect (ḥifẓ al-'aql), and public interest (maṣlaḥah), can be used to enhance Nigeria's AI surveillance law. Using doctrinal legal comparison, the research contrasts and compares classical Islamic sources and Nigerian statutory and constitutional law, the NDPA, and applicable digital identity law. The research demonstrates that while elements of Nigerian law are consistent with Islamic precepts of dignity and well-being, there remain lacunae under which bulk data harvesting, algorithmic profiling, and enforcement deficit erode privacy and autonomy. The paper concludes by recommending concrete measures to incorporate Islamic ethical imperatives in Nigeria's AI policy, including obligatory ethical audits, proportionality, and religion-based public control, in a bid to ensure that AI surveillance is solely for legitimate public interests and not at the cost of human dignity.

Keywords : Artificial Intelligence, Surveillance, Nigeria, Data Protection, Islamic Ethics.

ABSTRAK

Di era hiperdigitalisasi, AI telah memperluas ukuran dan cakupan pengawasan negara secara eksponensial di seluruh dunia, mendorong pertanyaan-pertanyaan etika mendasar tentang privasi, diskriminasi, dan martabat manusia ke permukaan. Di Nigeria, perkembangan pesat sistem identitas digital dan registrasi SIM-to-ID wajib telah menciptakan potensi pengawasan waktu nyata yang signifikan, namun perlindungan hukum khusus AI masih kurang berkembang. Meskipun Konstitusi Nigeria dan Undang-Undang Perlindungan Data Nigeria (NDPA) 2023 memberikan hak privasi secara umum, hanya terdapat sedikit penggabungan kerangka kerja agama dan budaya lokal dalam regulasi AI. Artikel ini membahas bagaimana prinsip-prinsip etika Islam fundamental, yang bersumber dari maqāsid al-sharī'ah, yaitu perlindungan kehormatan (ḥifẓ al-'ird), kehidupan (ḥifẓ al-nafs), akal (ḥifẓ al-'aql), dan kepentingan publik (maṣlaḥah), dapat digunakan untuk memperkuat hukum pengawasan AI di Nigeria. Dengan menggunakan perbandingan hukum doktrinal, penelitian ini mengontraskan dan membandingkan sumber-sumber Islam klasik dengan hukum perundang-undangan dan konstitusi Nigeria, Undang-Undang Dasar Nigeria (NDPA), dan hukum identitas digital yang berlaku. Penelitian ini menunjukkan bahwa meskipun unsur-unsur hukum Nigeria konsisten dengan ajaran Islam tentang martabat dan kesejahteraan, masih terdapat celah yang menyebabkan pengumpulan data massal, pembuatan profil algoritmik, dan defisit penegakan hukum mengikis privasi dan otonomi. Makalah ini diakhiri dengan rekomendasi langkah-langkah konkret untuk memasukkan keharusan etika Islam ke dalam kebijakan AI di Nigeria, termasuk audit etika wajib, proporsionalitas, dan kontrol publik berbasis agama, dalam upaya untuk memastikan bahwa pengawasan AI semata-mata untuk kepentingan publik yang sah dan tidak mengorbankan martabat manusia.

Kata Kunci : Kecerdasan Buatan, Pengawasan, Nigeria, Perlindungan Data, Etika Islam.

Corresponding Author : Abubakarmuhammadjibril9@gmail.com

INTRODUCTION

Artificial intelligence (AI) has tremendously increased the scope and intensity of surveillance technologies globally.(Ribeiro et al., 2024) Emerging tools such as facial recognition, biometric surveillance, and data mining permit an unparalleled accumulation of intimate details.(Mohanty et al., 2025) Innovation presents radical ethical dilemmas, such as bulk privacy violations, discrimination in algorithms, and loss of human agency. In Nigeria, fast advancements in digitalization, summed up by initiatives such as national identification programs and mobile telecommunication systems, have preceded the evolution of legal protections.(AlSuwaidi et al., 2023) Although the Nigerian Constitution provides for privacy ("the privacy of citizens... is hereby guaranteed and protected") and a new Data Protection Act creates rights over personal data, general AI-specific regulation is still in the process of taking shape.(NDPA, 2023) This is significant since Nigeria's digital identity schemes already encompass over 100 million citizens, and compulsory SIM-to-ID linkage programs essentially form a real-time tracking system. The scale of this monitoring requires serious ethical scrutiny.

Recent scholarship on AI ethics has highlighted general principles (oversight, fairness, accountability) and the necessity of impact assessments.(Kannike & Fahm, 2025) However, there is limited work on how these issues intersect with Islamic ethical principles in Nigeria. Similarly, research on Islamic ethics in technology invokes concepts like *maqāṣid al-sharī'ah* (the purposes of Islamic law) and the classical prohibitions on eavesdropping, but it less often extends them to concrete AI policymaking in the world.(Thalgi, 2025) In Nigeria, scholarship on digital law is preoccupied with the new Data Protection regime that has been introduced and with public concerns over centralized identification programs; there is minimal conversation about how religious and cultural principles can inform policymaking.(Laguda, 2013) Specifically, although there has been some research on integrating artificial intelligence into Nigerian society from a developmental perspective and critiquing the nation's general digital policymaking, no targeted analysis of AI surveillance through the lens of Islamic ethics has been conducted.(Oloba & Blankenship, 2025) The paper fills this literature gap through its explorative endeavor to apply Islamic ethics based on *maqāṣid al-sharī'ah* to the Nigerian AI surveillance state. To this end, the study applies a human dignity-focused framework that is based on four goals: preservation of honor (*ḥifẓ al-ʿird*), preservation of life (*ḥifẓ al-naḥs*), preservation of intellect (*ḥifẓ al-ʿaql*), and preservation of public interests (*maṣlaḥah*), through a comparative and dogmatic methodology that translates and applies Islamic.

This paper is significant in that it advances a human dignity centered approach to AI surveillance governance grounded in core *maqāṣid al-sharī'ah* principles, offering a contextually resonant framework for Nigeria's legal and socio-religious landscape. Rather than advancing a general ethical alignment between Islamic values and artificial intelligence, the study adopts a normative operational orientation that examines how Islamic ethical reasoning can inform concrete regulatory standards governing state surveillance practices. Specifically, it explores how objectives such as *ḥifẓ al-ʿird* (protection of honor and dignity), *ḥifẓ al-naḥs* (protection of life), *ḥifẓ al-ʿaql* (protection of intellect), and *maṣlaḥah* (public welfare) may function as evaluative criteria for assessing the legitimacy, scope, and limits of AI-enabled surveillance within Nigeria's existing legal framework. Accordingly, the study is guided by the following research questions:

1. How can *maqāṣid al-sharī'ah* principles be translated into enforceable regulatory standards such as necessity, proportionality, transparency, and accountability within Nigeria's AI surveillance governance framework?
2. Which *maqāṣid al-sharī'ah* principles are most determinative in evaluating the legality and legitimacy of specific AI surveillance practices in Nigeria, particularly biometric identification systems and mandatory digital identity linkages?

By reframing Islamic ethical principles as operational governance tools rather than abstract moral values, this study seeks to contribute to Islamic legal scholarship and AI governance literature by demonstrating how culturally grounded normative frameworks can generate concrete, context-sensitive standards for regulating emerging surveillance technologies.

RESEARCH METHOD

This paper employs a strictly normative doctrinal legal research methodology. Its aim is not to produce or analyse empirical data on the social impact, magnitude and public perception of AI-enabled methods of surveillance in Nigeria, but to examine the normative adequacy of the existing and emerging legal frameworks faced with AI-enabled surveillance from a *maqāṣid al-sharīʿah* based ethical perspective. Accordingly, any claims that are made in the present article are set forth as legal-ethical assessments based on authoritative legal texts, doctrines, and scholarly literature.

The research proceeds through qualitative doctrinal analysis of two primary bodies of normative material. First, it examines Islamic legal and ethical sources, including the Qurʾān, relevant Prophetic traditions (*ḥadīth*), and classical and contemporary juristic scholarship on *maqāṣid al-sharīʿah*, particularly as articulated by al-Ghazālī, al-Shāṭibī, and Ibn ʿĀshūr. From this corpus, the study derives four normative principles *ḥifẓ al-ʿird* (protection of honor and dignity), *ḥifẓ al-nafs* (protection of life), *ḥifẓ al-ʿaql* (protection of intellect), and *maṣlaḥah* (public welfare) which function as evaluative standards rather than empirical descriptors. Second, the study examines Nigerian constitutional, statutory and regulatory instruments relevant to AI surveillance and data governance including the 1999 Constitution (as amended), the Nigeria Data Protection Act 2023, the Cybercrimes Act 2015 and related policy instruments such as draft national AI strategies and regulatory guidelines. These materials are analysed doctrinally to determine how legal concepts such as privacy, consent, proportionality, human oversight and accountability are formulated and limited.

The analysis takes place in two normative stages: firstly, to reconstruct the ethical content of the principles of the selected *maqasid shariah*; and secondly, to put them as normative evaluative criteria to Nigerian AI surveillance frameworks, especially biometric identification systems and linkages of digital identities. References to surveillance infrastructures or regulatory initiatives are for the sake of contextuality and are not empirical findings. This way, analytical coherence can be ensured while also providing for the systematic operationalization of Islamic ethical principles as governance standards for AI surveillance in Nigeria.

Table 1. Analytical Framework Linking Islamic and Nigerian Legal Sources

Source Type	Examples	Ethical Principle / Legal Concept	Application for AI Surveillance
Islamic Primary Texts	<i>Qurʾan, Ḥadīth</i>	<i>ḥifẓ al-ʿird (honor), ḥifẓ al-nafs (life)</i>	Prohibition of spying; permission for necessary protection
Islamic Jurisprudence	<i>al-Ghazālī, al-Shāṭibī, Ibn ʿĀshūr</i>	<i>maqāṣid al-sharīʿah</i>	Framework for public welfare and dignity
Nigerian Legal Sources	1999 Constitution, NDPA 2023, Cybercrimes Act	Right to Privacy; Consent	Protection of personal data and autonomy
Policy Sources	National AI Strategy (draft), NIMC Reports	AI oversight; data ethics	Implementation and governance of surveillance

Sources: Processed by the author 30/10/2025

RESULTS AND DISCUSSION

A. Operationalizing Maqāṣid al-Sharī'ah as Policy-Evaluation Criteria

To move beyond abstract ethical exposition, this study treats maqāṣid al-sharī'ah as operational evaluative instruments for assessing surveillance governance. Each relevant maqṣad is translated into concrete legal criteria against which AI surveillance policies may be normatively assessed. (Norman & Ruhullah, 2024) There are four derivative principles, which are directly relevant to AI surveillance.

a. *ḥifẓ al-ʿird* (Protection of Honor & Dignity): functions as a constraint on unjustified intrusion. As an evaluative criterion, it requires that surveillance measures be grounded in a clear legal authorization, demonstrate necessity for a legitimate aim, and incorporate procedural safeguards such as consent or its lawful substitution, data minimization, and access to remedies. (Abdullah et al., 2025) Surveillance practices lacking these elements constitute a *prima facie* violation of human dignity. (Hamid, 2018)

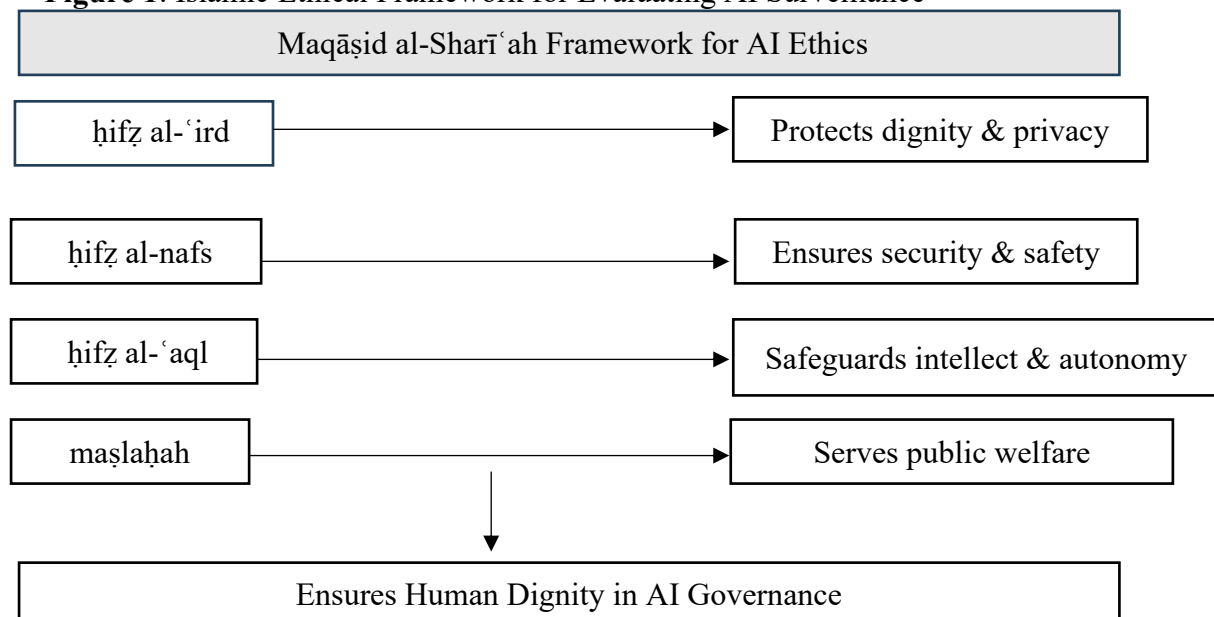
b. *ḥifẓ al-nafs* (Protection of Life): operates as a justification permitting surveillance only where it is demonstrably necessary to prevent serious harm. (Bawono et al., 2025) Normatively, this maqṣad demands a strict necessity test: surveillance may be justified only where less intrusive alternatives are unavailable and where safeguards exist to prevent wrongful harm, including erroneous targeting or arbitrary detention. (Dahlan et al., 2021)

c. *ḥifẓ al-ʿaql* (Protection of Intellect): functions as a safeguard against cognitive domination and psychological harm. (Ahmad et al., 2025) Applied to AI surveillance, it requires human oversight, transparency of automated processes, and protection against manipulative or fear-inducing practices that chill independent thought or distort perception. (Habib, 2025).

d. *Maṣlaḥah* (Public Welfare & Common Good): operates as a balancing principle, permitting limited surveillance only where a genuine and demonstrable public interest is established and where the benefits clearly outweigh the harms. (Mubarrak et al., 2025) Importantly, maṣlaḥah does not justify blanket or indiscriminate surveillance and must be applied consistently with dignity-preserving constraints.

Together, these criteria transform maqāṣid al-sharī'ah from general moral values into a structured analytical framework for evaluating the legality and legitimacy of AI surveillance policies.

Figure 1: Islamic Ethical Framework for Evaluating AI Surveillance



Source: processed by the author 26/10/2025

Safeguarding honor and intellectual agency require that surveillance practices recognize individuals as rights-bearing subjects rather than objects of administrative control, while the preservation of life and public welfare may justify surveillance only within narrowly circumscribed limits. In Islamic legal theory, *karāmah insāniyyah* (human dignity) occupies a foundational normative position and is widely recognized as a core objective of the *Sharī'ah*. Accordingly, AI technologies must be designed and deployed in a manner that affirms human dignity, respects personal autonomy, and avoids instrumentalizing individuals through opaque or coercive monitoring practices. Any AI-enabled surveillance policy adopted in Nigeria is therefore normatively assessable against the extent to which it preserves, constrains, or undermines human dignity as articulated within Islamic ethical jurisprudence.

B. Nigeria's Data Privacy and AI Policies

Nigeria regulates AI-enabled surveillance primarily through general data protection, security, and telecommunications legislation rather than a dedicated AI or surveillance-specific legal framework. This regulatory choice shapes both the scope of state surveillance powers and the limits of rights-based safeguards, making Nigeria an appropriate case for normative evaluation through an ethical governance lens. (NDPA, 2023) It was signed into law in June 2023 and provides for the establishment of the Nigeria Data Protection Commission and enshrines the rights of data subjects into law. The NDPA establishes legal bases for processing (e.g., consent, public interest), data security requirements, and requires data controllers to carry out privacy impact assessments for high-risk processing. Note, Section 37 of the NDPA forbids entirely automated decision-making with legal or similar impacts on individuals without human intervention and explanation. (Mendelson, 2018) Section 29 also requires technical and organizational personal data protection measures. These provisions reflect accountability and protection concerns. The NDPA should help en-trench trust in digital initiatives: as one legal practitioner observed, its passage will "provide complete protection for the personal data of all individuals" and accelerate Nigeria's digital identity scheme.

In addition to the NDPA, Nigeria also has the NIMC Act, 2007 (regulating the National Identification Number, NIN), the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, and sectoral regulations (e.g., telecom regulations). Most importantly, Nigeria has established a huge digital ID infrastructure: more than 100 million citizens have been assigned a NIN as of mid-2023. (Akindipe et al., 2024) An ambitious scheme (backed by the World Bank and others) is rolling out eID cards with biometrics. The government also insisted on linking SIMs to NIN, so each mobile subscriber's SIM registration is tied to their national ID. Though these are measures of inclusion and security, they constitute the effect of an identity and communications-linked database. The Nigerian Communications Commission (NCC) has also produced studies on AI's social impact and inserted the term "AI" into policy papers, but there is no stand-alone law limiting the surveillance use of AI. (Idem, 2023) The National AI Strategy (draft 2024) mentions ethical and societal risks but does not directly limit surveillance activity. In practice, CCTV systems and metadata collection are administered by intelligence agencies and law enforcement under current legislation (e.g., they can use NDPA provisions and criminal code as grounds for authorization).

1. Structural Features and Regulatory Gaps in Nigeria's Surveillance Framework

Nigeria's current legal framework is open to the use of AI-enabled surveillance as a form of indirect authorization as opposed to explicit surveillance laws. The NDPA provides some important safeguards against abuse, such as consent, impact assessments, and restrictions on automated decisions, but it does not provide a complete regime for state surveillance, particularly when security or intelligence purposes are invoked. Surveillance rules are scattered throughout several different statutes and there is no uniformity in individualized judicial warrants or clear definitions on the requirement for necessity and proportionality. (Ekpo et al., 2025) Oversight is

similarly spread out. Although the authority for supervising the processing of personal data is with the Nigeria Data Protection Commission, the Commission's jurisdiction does not clearly extend to intelligence-led surveillance. Judicial review exists in principle, but there are no transparency obligations limiting people's ability to challenge surveillance or seek redress. The result is a regulatory regime that allows for widespread data collection with little pre-data collection authorization and minimal post data collection accountability. This structure provides a gap in ethical governance and provides a foundation for assessing the ethical practices of AI surveillance in Nigeria with maqāṣid criteria: Dignity, necessity, proportionate and public welfare. (Lateef et al., 2022)

This configuration marked by expansive surveillance capacity alongside limited normative constraints constitutes the legal context against which the following section applies a maqāṣid al-sharī'ah based evaluative framework to assess the legitimacy of Nigeria's AI surveillance practices.

Table 2: Convergence between Islamic Ethical Principles and Nigerian Data Law

Nigerian Legal Provision / Practice	Maqāṣid-Derived Evaluative Criterion	Normative Assessment
Section 37 of the Constitution (Right to Privacy)	ḥifẓ al-'ird (protection of dignity and personal autonomy)	Establishes a constitutional baseline against unjustified intrusion but lacks detailed standards governing state surveillance authorization and proportionality.
NDPA 2023, Section 37 (Restriction on Fully Automated Decision-Making)	ḥifẓ al-'aql (protection of intellect and human agency)	Aligns with maqāṣid by requiring human intervention and intelligibility in consequential decisions; however, its limited application to security-based surveillance constrains its protective scope.
Statutory Allowances for Data Use in Security and Public Interest Contexts	ḥifẓ al-nafs (protection of life) and maṣlaḥah (public welfare)	Normatively permissible only where necessity and proportionality are clearly established; the absence of explicit thresholds risks over-extension beyond legitimate protective aims.
Absence of Explicit Prohibitions on Algorithmic Profiling or Biometric Surveillance	ḥifẓ al-'ird (dignity) and ḥifẓ al-'aql (agency)	Constitutes a significant governance gap, enabling discriminatory or dehumanizing practices inconsistent with dignity-based maqāṣid constraints.
Lack of Dedicated Surveillance Oversight and Remedies	maṣlaḥah (public welfare) conditioned by justice ('adl)	Weakens accountability and undermines claims of public interest, as maqāṣid require enforceable safeguards to prevent abuse and ensure fairness.

Source: processed by the author based on the analysis 05/01/2025

C. Islamic Ethical Analysis of Nigeria's Policies

This section uses the operationalized framework of *maqaaasid* (plural of *maqaaasid*) to assess the AI-enabled surveillance policies in Nigeria based on authorization, necessity, proportionality, oversight, and accountability. From the point of view of the protection of the privacy interest in the case of the NDPA and mandatory linkage of SIM and NIN, and the use of biometric registration on a large scale, the two issues are not fully related to the protection of dignity, but are less intrusion. (Baharuddin et al., 2019) . Under the concept of security-based surveillance or the concept of *hifaz al-nafs*, security-based surveillance may be justified only if strictly necessary; blanket data retention goes beyond that. Regarding the issue of "*hifZ al-`aql*" [limited transparency and human supervision], the lack of intellectual autonomy is encouraged in the process. Finally, appeals to *ma'slahah* are also normatively deficient in that there are not strong oversight and anti-profiling protections. (Muhsin, 2022).

The rest is targeted at *hifz al-nafs*: the state argues that the adoption of digital ID and AI is in the interest of public safety and national security. The linking of SIMs to NIN can be understood as enabling the quick tracing of terrorists or criminals, supposedly saving lives in line with public welfare (*maṣlaḥah*). Similarly, Nigeria's anti-cybercrime initiatives are meant to protect citizens from fraud and online harm. In emergencies (e.g., tracking missing individuals through phone records), this surveillance might save lives, meeting Islamic justifications of necessity. (Almutairi, 2020) The Islamic legal maxim "*la ḍarara wa lā ḍirār*" (no harm shall be done or reciprocated) would permit intrusion only to the degree required to avert harm. The NDPA itself allows for the utilization of data in "public interest" (e.g., law enforcement), which mirrors this balance. Here, some level of surveillance is not necessarily anti-Islamic *per se*; where proportionality and transparency are maintained, it can be compatible with *maṣlaḥah*.

But serious concerns are raised when the dignity principle of Islam is in question. Nigeria's bulk surveillance system threatens to infringe *hifz al-`ird* unless tightly circumscribed. Mandatory SIM registration, though security justified, constitutes coercing citizens into providing personal information "without stress," a utilitarian bypass of informed consent. (Gorian & Osman, 2024) Forcing privacy invasion is abhorrent to Islam, as Prophet Muhammad ﷺ had cautioned, "Do not spy on one another." According to this perspective, bulk data collection (SIM linking and NIN registration) is susceptible to abuse, i.e., if the state uses the register to track peaceful religious assemblies or political opposition, individuals' dignity would be infringed upon under the pretext of security. (Anyia, 2017) Even without malicious intent, knowledge of widespread surveillance might chill society and interfere with mental well-being, including the protection of *hifz al-`aql*. The Quranic ethic of privacy argues that individuals ought to be "safe from glance and prying eye" within their domain, an immunity that should not easily be overridden by Nigeria's policy.

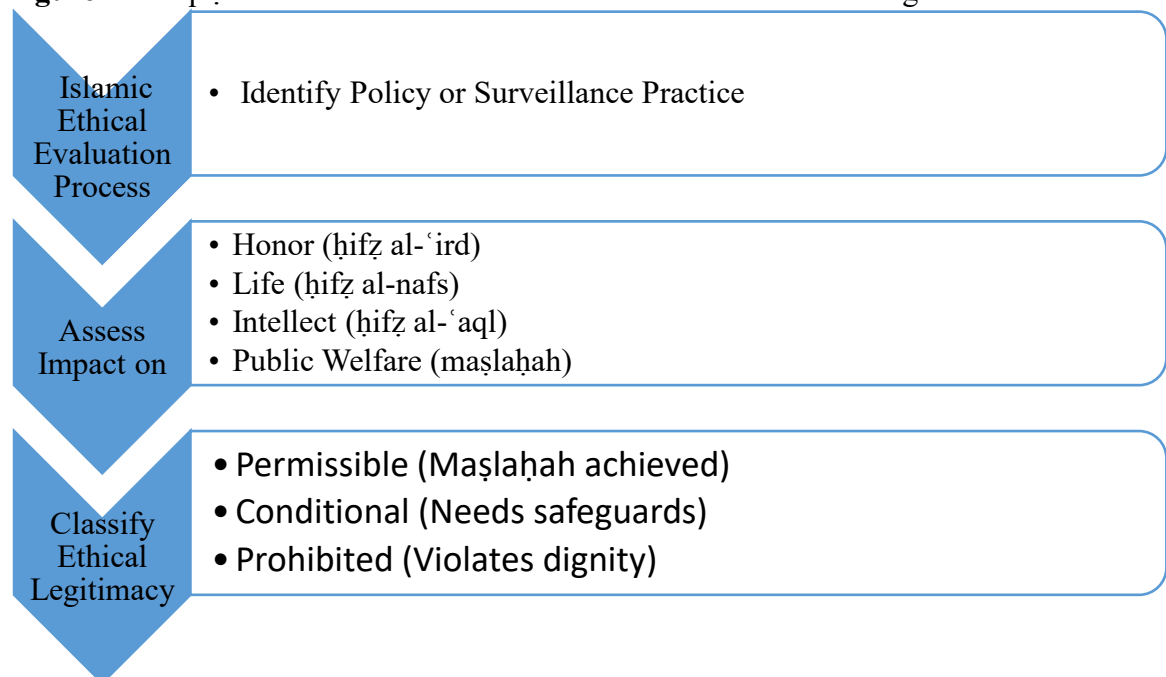
There are also criticisms on the grounds of consistency and justice. Nigeria's data law is great on paper but light on enforcement. Islamic values require that the application of laws should be implemented with fairness (justice) and mercy. The new NDPA has contemporary safeguards but has not yet demonstrated effectiveness in practice. Researchers observe broad distrust of the ID program because of previous data breaches; promise-keeping (*amānah*) and privacy in Islam are moral obligations. (Maruf, 2025) In the absence of public enforcement, data privacy breaches would constitute a breach of Islamic accountability (*dhimmah*). Nigeria is also a signatory to global AI ethics statements and necessitates human oversight, which speaks to Islam's focus on accountability. However, if they are nothing more than paper promises, then the spirit of *hifz al-nafs* and *hifz al-`aql* (i.e., not cheating or processing people illegally) is not truly honored.

Notably, the *maṣlaḥah* doctrine instructs that any surveillance should be for the common good in an Islamic society. Policies in Nigeria habitually quote development and security as benefits. Indeed, based on one analysis of workshops, an issue like predictive policing or hospital surveillance could be framed as in the public interest. However, *maṣlaḥah* also requires reducing

negative impacts. For instance, facial recognition technology – a powerful AI surveillance tool – is mentioned as being especially objectionable. Islamic ethics concur: the use of AI to recognize people in public spaces without their consent "should not be used in ways that infringe human rights or dignity". (Adam et al., 2018) Under Shari'ah, this would mean that such technology would only be used if required to fulfill an established public safety requirement, under rigorous anti-discrimination protections. Nigeria does not have any AI-surveillance specifics beyond the general data legislation. An Islamic critique would call for definite boundaries: e.g., prohibit racial profiling, insist on the immediate removal of irrelevant data, and provide redress for citizens who are unfairly targeted.

Overall, Islamic ethics offers guidance and critique of the Nigerian practice. It guides by supporting rightful ends (security, welfare) that can be served by surveillance (*ḥifẓ al-nafs*, *maṣlaḥah*), life-enhancing, and safety-enhancing technologies. It critiques by demanding priority for individual dignity and justice (*ḥifẓ al-ʿird*, *ḥifẓ al-ʿaql*) in any such system. Where Nigeria's digital policies already safeguard certain rights (e.g., constitutional privacy), they supplement Shari'ah values. Where they are lacking (e.g., extensive data demands without sufficient ethical guidance), Islamic norms would have to be bolstered. Applying this prism necessitates scrutinizing every surveillance practice: Does it maintain the dignity of the surveilled? Is it truly indispensable to save lives? Does it advance an actual public interest without eroding trust? These are the standards that an Islamic dignity approach introduces into AI policy in Nigeria.

Figure 2: Maqāṣid-Based Evaluation Model for AI Surveillance in Nigeria



Source: processed by the author 31/10/2025

CONCLUSION

This study has demonstrated that four maqāṣid al-sharīʿah principles *ḥifẓ al-ʿird* (protection of honor and dignity), *ḥifẓ al-nafs* (protection of life), *ḥifẓ al-ʿaql* (protection of intellect), and *maṣlaḥah* (public welfare) can function as a normative evaluative framework for assessing AI-enabled surveillance governance in Nigeria. Rather than claiming that Islamic ethics can, in themselves, ensure the protection of human dignity, the analysis shows that these principles illuminate specific points of convergence and tension within Nigeria's existing legal architecture, particularly constitutional privacy guarantees and the Nigeria Data Protection Act 2023. In this sense, maqāṣid do not replace positive law, but operate as a critical lens for evaluating its adequacy and limits.

The findings indicate that while Nigeria's data protection framework reflects partial alignment with dignity- and accountability-oriented values, significant gaps remain especially regarding authorization standards, oversight mechanisms, and safeguards against disproportionate or bulk surveillance. Islamic ethical reasoning underscores the importance of categorical boundaries: surveillance must not devolve into reputational harm, coercion, or cognitive domination, even when justified in the name of security or development. At the same time, the maqāṣid framework acknowledges that carefully circumscribed surveillance may be normatively permissible where it is demonstrably necessary to protect life and genuine public interests.

The policy implications advanced in this article are therefore normative and interpretive, not prescriptive mandates. Proposals such as ethical impact assessments, enhanced proportionality requirements, and strengthened oversight mechanisms are grounded in principles already familiar to constitutional and data protection law, with Islamic ethics offering context-sensitive justification rather than religious enforcement. In a multireligious constitutional order such as Nigeria's, maqāṣid-based reasoning should be understood as a complementary ethical resource, capable of informing inclusive governance debates without displacing secular legal authority.

This study is limited by its strict doctrinal methodology and does not assess the empirical operation or societal reception of surveillance practices. Future research could therefore pursue comparative analyses of surveillance regulation in Muslim-majority jurisdictions, examine judicial engagement with dignity-based claims in data protection litigation, or explore how Islamic ethical reasoning interacts with international human rights standards in digital governance. Such work would further clarify the practical role of maqāṣid al-sharī'ah in contemporary AI regulation.

REFERENCES

- Abdullah, H., Mohd Zain, F. A., Juahir, H., Che Haron, H. I., Ismail, A., Islam, T., & Sheikh Ahmad Tajuddin, S. A. F. (2025). Developing Tahfiz empowerment index based on Maqasid Shariah. *International Journal of Islamic and Middle Eastern Finance and Management*. <https://doi.org/10.1108/IMEFM-06-2024-0317>
- Adam, S. B., Al-Aidaros, A. M. H., & Ishak, S. B. (2018). The moderating effect of Islamic work ethics on the relationship between corporate governance and performance of Islamic financial institutions in Nigeria: A proposed framework. *Journal of Social Sciences Research*, 2018(Special Issue 6), 1041–1048. <https://doi.org/10.32861/jssr.spi6.1041.1048>
- Ahmad, N., Ahmad, S. H., & Rahim, F. (2025). Islamic Ethical Principles for Addressing Obesity: A Public Policy Perspective. *Legal Transformation in Muslim Societies*, 2(2), 1–19. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-105014285321&partnerID=40&md5=e940cceb835258462aeae31b3038e8c7>
- Akindipe, D. O., Lalude, O. M., Bamgbose, O. T., & Gbenga-Fabusiwa, L. (2024). Appraisal of the Legal Framework on Emerging Cybercrimes and Virtual Disruption in Nigeria. *IEEE International Conference on Emerging and Sustainable Technologies for Power and ICT in a Developing Society, NIGERCON*, 2024. <https://doi.org/10.1109/NIGERCON62786.2024.10927149>
- Almutairi, S. E. (2020). The Shari'a approach to contemporary problems of mass surveillance. *Muslim World Journal of Human Rights*, 17(1), 1–44. <https://doi.org/10.1515/mwjhr-2020-0007>
- AlSuwaidi, H. A., Harous, S., & Serhani, M. A. (2023). Review of Visual AI Applications in Smart Surveillance for Crime Detection and Prevention: A Survey. *IET Conference Proceedings*, 2023(39), 307–320. <https://doi.org/10.1049/icp.2024.0502>
- Anyia, A. (2017). Muslim Organisation and the Mobilisations for Sharia Law in northern

- Nigeria: The JNI and The NSCIA. *Journal of Asian and African Studies*, 52(1), 82–102. <https://doi.org/10.1177/0021909614560246>
- Baharuddin, A. S., Ismail, W. A. F. W., Mutalib, L. A., Ahmad, M. H., Razak, R., Saharudin, N. S., & Rahim, A. A. (2019). An Appraisal of Maqāsid Al-Shari‘ah Classic and Recent Literature: Systematic Analysis. *Library Philosophy and Practice*, 2019. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85100643530&partnerID=40&md5=484fe35f51b6bce7a312162176143a37>
- Bawono, B. T., Huda, M. N., Prayitno, A. H., & Siswanto, M. A. (2025). Human Trafficking and the Relevance of Hifz al-nafs and Hifz al-’ird in Contemporary Islamic Legal Ethics. *MILRev: Metro Islamic Law Review*, 4(1), 597–618. <https://doi.org/10.32332/milrev.v4i1.10694>
- Dahlan, M., Bustami, M. R., & Mas’ulah, S. (2021). The Islamic principle of ḥifẓ al-nafs (protection of life) and COVID-19 in Indonesia: A case study of nurul iman mosque of Bengkulu city. *Heliyon*, 7(7). <https://doi.org/10.1016/j.heliyon.2021.e07541>
- Ekpo, O., Okokon, A., & Akpakpan, M. (2025). Data Protection in the Digital Age: A Comparative Analysis of Nigeria’s NDPA and the EU’s GDPR. *ICTD 2024 - Proceedings of the 2024 International Conference on Information and Communication Technologies and Development*, 48–56. <https://doi.org/10.1145/3700794.3700799>
- Gorian, E., & Osman, N. D. (2024). DIGITAL ETHICS OF ARTIFICIAL INTELLIGENCE (AI) IN SAUDI ARABIA AND UNITED ARAB EMIRATES. *Malaysian Journal of Syariah and Law*, 12(3), 583–597. <https://doi.org/10.33102/mjssl.vol12no3.798>
- Government, N. (2023). *NIGERIA DATA PROTECTION ACT, 2023*. <https://lawcarenigeria.com/nigeria-data-protection-act-2023/>
- Habib, Z. (2025). Ethics of Artificial Intelligence in Maqāsid Al-Sharī‘a’s Perspective. *KARSA*, 33(1), 105–134. <https://doi.org/10.19105/karsa.v33i1.19617>
- Hamid, S. (2018). Drawing a Synergy between Theory and Practice – A Move towards a More Stakeholder-Oriented Regulatory Framework for Modern Islamic Finance Institutions: A Comparative Analysis. In *Asian Yearbook of Human Rights and Humanitarian Law* (Vol. 2, pp. 117–147). https://doi.org/10.1163/9789004346888_005
- Idem, U. J. (2023). The Legal Approach for Fighting Cybercrimes in Nigeria: Some Lessons from the United States and the United Kingdom. *2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, 191–198. <https://doi.org/10.1109/CyMaEn57228.2023.10050983>
- Kannike, U. M. M., & Fahm, A. O. (2025). EXPLORING THE ETHICAL GOVERNANCE OF ARTIFICIAL INTELLIGENCE FROM AN ISLAMIC ETHICAL PERSPECTIVE. *Jurnal Fiqh*, 22(1), 134–161. <https://doi.org/10.22452/fiqh.vol22no1.5>
- Laguda, D. O. (2013). Religion and government policy formulations: A study of the responses of Muslims to the coroner law system in Lagos, Nigeria. *Politics and Religion Journal*, 7(2), 399–412. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067376609&partnerID=40&md5=fc033416add09daedde1c30c43357ab5>
- Lateef, M. A., Taiwo, L. O., & Adeyoju, A. (2022). Examining the Powers of the NITDA to Enforce Data Protection Laws in Nigeria. *Global Privacy Law Review*, 3(2), 89–97. <https://doi.org/10.54648/gplr2022009>
- Maruf, A. O. (2025). Comparative Study of Islamic and Secular Economic Law in Nigeria: Implications for Policy Making. *Jurnal Ilmiah Mizani*, 12(1), 33–49. <https://doi.org/10.29300/mzn.v12i1.5340>
- Mendelson, D. (2018). The european union general data protection regulation (EU 2016/679) and the Australian my health record scheme - A comparative study of consent to data processing provisions. *Journal of Law and Medicine*, 26(1), 23–38. <https://www.scopus.com/inward/record.uri?eid=2-s2.0->

- 85062487706&partnerID=40&md5=849ec75737e2371fef8bc55025adfad
- Mohanty, P., Manu, S. R., Shreyas, M., Uttam, V., Navada, B. R., Sravani, V., & Santhosh, K. V. (2025). Integrating Multi-Sensors and AI to Develop Improved Surveillance Systems. *Journal of Robotics and Control (JRC)*, 6(2), 980–994. <https://doi.org/10.18196/jrc.v6i2.25596>
- Mubarrak, Z., Bakar, I. A., & Hamdani, M. (2025). The Urgency of the Islamic Law and Contemporary Societal Challenges: The Flexibility of al-Maslahah in Determining the Hierarchy of Maqāsid al-Sharī‘ah. *El-Usrah*, 8(1), 344–365. <https://doi.org/10.22373/pxydd884>
- Muhsin, S. M. (2022). Medical Confidentiality Ethics: The Genesis of an Islamic Juristic Perspective. *Journal of Religion and Health*, 61(4), 3219–3232. <https://doi.org/10.1007/s10943-021-01313-7>
- National Identity Management Commission, 5182 (2007). <http://www.nimc.gov.ng/>
- Nigeria Data Protection Act, Federal Republic of Nigeria Official Gazette A719 (2023). <https://placng.org/i/wp-content/uploads/2023/06/Nigeria-Data-Protection-Act-2023.pdf>
- Norman, N. A., & Ruhullah, M. E. (2024). EXPLORING THE ETHICAL DIMENSIONS OF FIQH: THE ROLE OF THE SOUL IN ACHIEVING MAQĀSID AL-SHARĪ‘AH. *Al-Shajarah*, 29(1), 47–77. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85199269891&partnerID=40&md5=f2fb61b953cc6160816d4114baee56a0>
- Oloba, B. L., & Blankenship, A. M. (2025). Gender Dynamics in Online Religious Leadership in Nigeria: Investigating How Digital Platforms Shape Communication, Authority, and Influence. *Religions*, 16(1). <https://doi.org/10.3390/rel16010005>
- Ribeiro, T., Oliveira, P., & Rodrigues, M. (2024). Next-Generation Surveillance: Exploring the Intersection of Artificial Intelligence and Security. *Lecture Notes in Networks and Systems*, 1066 LNNS, 522–535. https://doi.org/10.1007/978-3-031-66428-1_33
- Thalgi, M. (2025). AI Ethics in Islamic Contents: Applications Per UNESCO Recommendations. In *Studies in Systems, Decision and Control* (Vol. 234, pp. 333–346). https://doi.org/10.1007/978-3-031-84636-6_28