PROCEEDINGS OF THE INTERNATIONAL CONFERENCE FOR INSTITUTE OF ADMINISTRATION (ICIA 2025)
AHMADU BELLO UNIVERSITY ZARIA - NIGERIA

Website: https://icia.org.ng **ISBN:** 978-978-695-265-9 **Volume II, 2025**

AN APPRAISAL OF THE LEGAL CONSEQUENCES OF AI-POWERED CUSTOMER DATA MANAGEMENT IN THE TRAVEL AND HOSPITALITY INDUSTRY

Lateefat Adeola Bello
Department of Commercial Law. Faculty of Law,
Ahmadu Bello University, Zaria
attorney4real@yahoo.com

ABSTRACT

Artificial Intelligence (AI) has emerged as a transformative force within the global travel and hospitality industry, redefining how customer data is collected, processed, and utilised for operational efficiency and personalised service delivery. As AI systems increasingly power data-driven functions ranging from predictive analytics and chatbots to dynamic pricing algorithms, the legal and ethical implications of such technologies have intensified. This paper appraises the legal consequences of AI-powered customer data management, focusing on privacy, consent, accountability, and liability concerns that arise from algorithmic processing within hospitality operations. Using a comparative doctrinal methodology, the study evaluates the European Union's General Data Protection Regulation (GDPR) and Nigeria's Data Protection Act (NDPA) 2023, highlighting their convergences and divergences in addressing AI-related challenges. While the GDPR offers a mature, procedurally grounded framework emphasising accountability and algorithmic transparency, Nigeria's NDPA remains largely principle-based and institutionally nascent. Through analysis of key jurisprudence. The paper illustrates how courts are shaping the contours of data protection and AI accountability. The findings reveal that Nigeria's NDPA, despite aligning conceptually with GDPR principles, lacks detailed provisions on automated decision-making, algorithmic bias, and cross-border data transfers. The paper concludes that effective AI regulation in hospitality requires a hybrid governance model integrating law, ethics, and institutional capacity. It recommends legislative amendments, sector-specific codes of conduct,

and enhanced regulatory oversight to ensure that AI innovation advances in harmony with privacy rights and consumer protection.

Keywords: *Artificial Intelligence, GDPR, NDPA 2023, Data Protection, Hospitality Law, Travel*

1.1 Introduction

The travel and hospitality sector is situated at the nexus of customer trust, customisation, and technology. The strategic driver of this change is now artificial intelligence (AI), which improves visitor interaction, forecasts demand, optimises pricing, and automates service delivery. In order to maintain competitiveness and enhance operational performance, hospitality firms are becoming more dependent on client data through the integration of machine learning, predictive analytics, and facial recognition technologies, but this data-driven innovation has raised difficult moral and legal issues. Concerns regarding the degradation of privacy and autonomy are raised by AI systems' reliance on enormous amounts of personal data, such as names, biometric identifiers, locations, financial information, and behavioural profiles. Additionally, when customer-facing systems make important decisions without significant human monitoring, algorithmic decision-making creates new concerns of bias, opacity, and liability. The General Data Protection Regulation (GDPR), which went into effect throughout the European Union in May 2018, is the most extensive attempt to govern such practices. The GDPR creates enforceable requirements for lawfulness, transparency, and responsibility while establishing data privacy as a basic right. Nigeria's Data Protection Act (NDPA) 2023, on the other hand, is still underdeveloped procedurally despite being a landmark in the country's data protection landscape. Although it provides guiding principles, it lacks the comprehensive operational methods, algorithmic safeguards, and oversight architecture included in the GDPR's Data Protection Impact Assessments (DPIAs).[3] Nigeria's hospitality sector, which handles massive amounts of client data via international booking engines, payment gateways, loyalty programs, and cross-border digital ecosystems, is especially vulnerable to this regulation gap. Nigerian clients' personal information is regularly transferred by these systems to foreign jurisdictions, creating compliance issues under both national and international law. By incorporating automated profiling and decision-making into service models, the inclusion of AI increases these dangers.[4]

1.2 Statement of Problem

Nigeria's regulatory readiness has not kept up with the rapid deployment of AI technologies, despite their promise of efficiency and customisation. Although it does not specifically address AI-driven processing or automated decision-making, the NDPA 2023 offers a legal framework for data protection. Because of this disparity, data controllers and AI suppliers operate in an accountability system that is fragmented and without a clear chain of accountability.[5]

Additionally, the Nigerian Data Protection Commission (NDPC), which is in charge of enforcement, has limited sector-specific guidelines and insufficient ability. Therefore, the inability of institutions and regulations to handle the intricate interactions between data innovation and privacy protection is the root of the issue. While customers are still unsure of their rights in algorithmic contexts, hospitality operators run the risk of being exposed to violations, discrimination claims, and international lawsuits.

1.3 aim and objective of Research

Through comparative legal analysis, this paper aims to critically evaluate the legal ramifications of AI-powered data management within Nigeria's hospitality and travel industry. The goals are to:

a. Analyse the type and extent of AI-driven data management practices in the travel and hospitality sector; and b. Compare and assess the GDPR and NDPA 2023 regulatory frameworks.
b. Examine pertinent legal and judicial precedents that have an impact on the enforcement of data protection; and
c. Make recommendations for legislative and policy changes to improve Nigeria's governance of AI-based data management.

The following research questions are put forth to direct the analysis:

a. How does AI-driven customer data management function in the travel and hotel industry, and what particular legal concerns does it create?
b. Where do the GDPR and NDPA 2023 divide and coincide in terms of regulating AI-driven data processing?
c. What is the interpretation of accountability in AI-related data practices by courts and regulators?

d. What changes could bring Nigeria's data protection laws into compliance with global norms?

1.4 **Scope and Significance of the Study**

This study's focus is restricted to AI-powered data management in Nigeria's travel and hospitality sector, evaluated in light of the GDPR and NDPA 2023. This emphasis is a reflection of the industry's high reliance on personal data and its vulnerability to international data transfers. The study's dual contribution to research and policy is what makes it significant. Academically, it broadens the conversation around AI governance in the developing digital economies of Africa. Practically speaking, it offers legislators, regulators, and business executives practical insights for improving consumer protection, bolstering compliance, and promoting the ethical application of AI in the travel and hospitality industry.

2.1 Literature Review

2.1.1 Conceptual Overview of Artificial Intelligence and Data Governance

The term artificial intelligence (AI) describes computing systems that can carry out cognitive functions that are typically associated with human intelligence, including perception, reasoning, and learning. Machine learning (ML) and deep learning (DL) algorithms are used by AI technologies in data management to identify patterns, forecast behaviour, and make decisions automatically. AI is used in a variety of ways in the travel and hospitality sector, from recommendation engines and intelligent chatbots to facial recognition for visitor identification and sentiment analysis for better customer service.[6]

The use of AI in the hospitality industry depends on the availability of large volumes of customer data, which allows computers to forecast visitor preferences, optimise pricing, and customise experiences. However, increased vulnerability to privacy risks results from this same data reliance. There are significant accountability and transparency issues with AI's "black-box" architecture, which makes algorithmic judgments difficult to understand.

Floridi and Cowls claim that artificial intelligence (AI) significantly changes the information imbalance between service providers and customers, giving businesses disproportionate power to forecast, sway, and even control customer decisions[8]. Therefore, to ensure that automation does

not undermine individual rights or institutional accountability, effective governance of AI must strike a balance between innovation and ethical restraint. Therefore, data governance provides the ethical and legal foundation for the collection, processing, and security of personal data. According to Bygrave, data governance includes both the procedural accountability systems that guarantee compliance and the substantive standards of privacy law.[9].In order to ensure justice, explainability, and human oversight, governance in the AI era must transition from traditional data protection to algorithmic governance. [10]

2.2 Theoretical Foundations for Accountability, Risk-Based Regulation, and AI Ethics

The study of AI governance is underpinned by three interrelated theoretical frameworks: accountability theory, risk-based regulation, and AI ethics. Accountability theory posits that those who determine the purposes and means of data processing must bear responsibility for the outcomes of such processing. Under the GDPR, this principle is codified in Article 5(2), which obliges controllers to demonstrate compliance with data-protection principles[11]. Scholars such as Kuner (2020) and Lynskey (2015) argue that accountability represents the linchpin of modern data protection, transforming privacy from a reactive right into a proactive management duty.

Nigeria's NDPA 2023 similarly incorporates accountability as a guiding principle under Section 30, but lacks procedural instruments such as Data Protection Impact Assessments (DPIAs), auditable compliance records, or independent oversight mechanisms[12]. The absence of these tools renders accountability declarative rather than demonstrable.

Risk-based regulation emphasises proportionality and preventive control. Rather than imposing uniform compliance duties, it requires regulators and organisations to assess and mitigate risks based on data sensitivity and processing scale[13]. The GDPR institutionalises this through DPIAs (Article 35), which obligate controllers to evaluate and minimise risks in high-impact processing, including automated decision-making and biometric analysis. Nigeria's NDPA lacks a parallel provision, leaving high-risk AI applications in hospitality largely unsupervised[14]

The third theoretical foundation—AI ethics—extends legal compliance into moral responsibility. Ethical AI frameworks, such as those proposed by UNESCO (2021) and the OECD AI Principles (2021), emphasise fairness, accountability, transparency, and human oversight. These frameworks urge developers and operators to embed ethics "by design," ensuring that AI systems reflect social

values and human rights[11]. Ethical governance is particularly crucial in hospitality, where trust, personalisation, and emotional intelligence underpin service quality[15]

2.3 AI and Data Protection in the Travel and Hospitality Industry

The hospitality and travel industries have become testing grounds for data-driven innovation. AI enables dynamic customer engagement, operational efficiency, and revenue optimisation. Yet, the same systems often blur the line between personalisation and surveillance.

Ivanov (2023) identifies hospitality as a "data-intensive ecosystem," where information flows are multidirectional—between guests, hotels, booking platforms, and analytics providers[16]. This interconnectedness amplifies privacy risks, as a single transaction may involve multiple processors across different jurisdictions. For example, an international hotel chain might collect data in Lagos, store it in Ireland, and analyse it using a U.S.-based AI vendor.

Buhalis and Yen (2022) demonstrate that while AI enhances guest experiences through real-time customisation, it also introduces risks of algorithmic discrimination, where automated systems unintentionally reproduce social biases in pricing or service eligibility[17]. This challenge has triggered legal scrutiny under GDPR's Article 22, which safeguards individuals from decisions made solely by automated means without human review.

In Nigeria, similar technological adoption is evident, though regulatory enforcement remains limited. Many hospitality operators utilise AI-driven marketing or reservation systems developed abroad, often without assessing compliance with NDPA or international data-transfer rules[15]. This underscores the regulatory asymmetry between technology diffusion and legal capacity.

2.4 **Comparative Perspectives on Data Protection: GDPR and NDPA 2023**

The GDPR's conceptual sophistication and procedural rigour have made it a global template for privacy regulation. It enshrines seven key principles—lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and accountability[18]

. These principles are reinforced by enforceable rights (access, rectification, erasure, objection) and obligations such as DPIAs, breach notification, and appointment of Data Protection Officers (DPOs).

The NDPA 2023 mirrors these principles but lacks operational depth. While Sections 24–30 outline data processing obligations, the Act omits explicit provisions on automated decision-making and AI-specific risk assessments. Unlike the GDPR's Article 22, the NDPA does not confer an individual's right to challenge or request human intervention in algorithmic decisions[17].

Furthermore, the NDPA's enforcement agency—the Nigeria Data Protection Commission (NDPC)—is still developing institutional expertise, funding, and regulatory instruments. The GDPR's enforcement is decentralised through independent Data Protection Authorities (DPAs) across the EU, which enjoy investigatory and sanctioning powers, including imposing fines up to 4% of annual turnover. In Nigeria, penalties remain modest, and enforcement is discretionary[18].

Despite these gaps, scholars such as Bello (2025) and Yakubu (2024) commend the NDPA for providing a foundational legal framework that can evolve toward global standards. They emphasise the need for subsidiary regulations—akin to the GDPR's Implementing Guidelines—to operationalise accountability and establish AI oversight mechanisms[19].

3.1 **Jurisprudential Developments and the Evolution of Data Rights**

Judicial interpretation has played a central role in defining the boundaries of data protection and AI accountability. In Digital Rights Ireland v Minister for Communications (CJEU, 2014), the Court of Justice of the European Union (CJEU) invalidated the Data Retention Directive for violating proportionality, holding that indiscriminate data retention breached Articles 7 and 8 of the EU Charter of Fundamental Rights[20]. Similarly, Schrems II (CJEU, 2020) invalidated the EU–US Privacy Shield, reaffirming that cross-border data transfers must ensure "essentially equivalent protection."[21]

In Nigeria, courts are gradually extending constitutional privacy guarantees to digital contexts. In Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (Court of Appeal, 2022), the court recognised data protection as an extension of the constitutional right to privacy under Section 37 of the 1999 Constitution[22]. Earlier, in Eneye v MTN Nigeria Communications Ltd (2019), unauthorised disclosure of subscriber data was held to contravene the same constitutional right[23].

These cases illustrate a growing judicial awareness of informational autonomy—the right of individuals to control their personal data in the digital era. They also reflect the courts' willingness

to bridge legislative gaps pending the full operationalisation of statutory protections. Three gaps emerge from the reviewed literature and jurisprudence there are;

a. Most studies on AI governance and data protection analyse general regulatory frameworks without contextualising implications for specific industries like hospitality.
b. Few Nigerian studies juxtapose local data-protection enforcement with EU precedents to derive actionable lessons.
c. Existing literature focuses heavily on privacy and consent, but under-theorises accountability, bias mitigation, and algorithmic explainability[24].

This paper addresses these gaps by providing a contextualised, comparative, and doctrinally grounded analysis of AI's legal consequences in hospitality, bridging normative theory with practical enforcement realities. This paper adopts a doctrinal and comparative legal research design, which is best suited to analysing the legal and institutional dimensions of AI governance. The doctrinal method involves a systematic examination of primary and secondary legal sources, including statutes, regulations, case law, and policy instruments to identify, interpret, and synthesise the applicable legal principles[25]. It is essentially a library-based approach that emphasises textual analysis and legal reasoning rather than empirical fieldwork.

Through this approach, the paper explores how the General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDPA) 2023 conceptualise and regulate the challenges of AI-powered customer data management. The comparative dimension is used to highlight the convergence and divergence between these two regimes in terms of substantive protections, procedural mechanisms, and enforcement capacity[26].

This paper relies on Primary Legal Sources, which include constitutional provisions, statutes, judicial decisions, and regulatory instruments. The paper also draws extensively on peer-reviewed academic articles, legal commentaries, and institutional reports.

This analytical framework evaluates how both GDPR and NDPA assign legal responsibility to controllers, processors, and AI system operators. Under the GDPR, accountability is an enforceable duty; controllers must not only comply with legal principles but also demonstrate such compliance through records, DPIAs, and independent audits[27]. The NDPA adopts accountability

as a guiding principle but lacks corresponding procedural mechanisms. The analysis, therefore, focuses on the normative and operational consequences of this disparity**.**

3.2 Risk-Based Regulatory Framework:

This framework examines the proportionality of regulatory interventions relative to the risks posed by AI-driven data processing. The GDPR's Article 35 on Data Protection Impact Assessments (DPIAs) serves as a benchmark, representing a dynamic model of anticipatory governance. The NDPA's absence of a risk-based oversight tool exposes high-risk AI applications—such as biometric recognition and automated pricingto legal ambiguity[28].

3.3 Comparative Doctrinal Framework:

This interpretive lens enables the juxtaposition of EU and Nigerian legal systems to reveal structural, procedural, and normative differences. Through doctrinal reasoning, the paper assesses how each jurisdiction translates abstract principles (like transparency and fairness) into actionable obligations. It also evaluates the institutional capacity of enforcement bodies (e.g., the NDPC in Nigeria versus EU national Data Protection Authorities) and how that capacity influences compliance outcomes[29].

3.4 Justification for the Methodology

The choice of a doctrinal-comparative method is justified by both the nature of the research question and the character of AI regulation. Empirical methods, while valuable, would be insufficient for this study's objectives because AI governance is primarily a legal and normative issue, rather than a quantitative one. By applying doctrinal analysis, the research can engage in a critical exegesis of legal texts—interpreting statutory language, judicial reasoning, and policy intent. This approach allows for the systematic exposition of:

a. The extent to which AI-related risks are addressed by existing legal provisions.
b. The conceptual coherence of those provisions with broader human-rights standards, and
c. The implications of gaps and ambiguities for accountability in the hospitality industry[30].

Comparative methodology further enables policy learning and transnational dialogue. As both the GDPR and NDPA aim to safeguard personal data in digital environments, comparing them reveals best practices that Nigeria can adapt to its socio-economic context. This aligns with Kamba's

(1974) classical justification for comparative law: to harmonise legal development by borrowing "functional equivalents" across jurisdictions[31].

Like any doctrinal analysis, this study faces certain limitations. First, it relies on existing legal materials rather than empirical data from industry practice. Consequently, it cannot quantify the actual rate of compliance or the practical efficacy of NDPA enforcement in hospitality businesses. Second, AI regulation is a rapidly evolving field; legislative amendments or new case law could modify the analysis over time. Third, while the comparative focus provides valuable insights, it may not fully capture jurisdiction-specific socio-economic constraints influencing implementation[32]. Nonetheless, these limitations do not undermine the study's objectives. Instead, they highlight the dynamic nature of AI governance and the ongoing need for continuous legal and policy adaptation.

4.1 Discussion and Analysis

4. 1.1 Comparative Legal Frameworks of GDPR and NDPA 2023

The General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDPA) 2023 share a common normative ambition: to safeguard the rights of individuals whose personal data are processed by public or private entities. However, their divergence lies in the depth of procedural integration and institutional maturity. The GDPR represents a fully developed supranational framework with a risk-based architecture, while the NDPA remains principle-oriented but operationally shallow[33].

The GDPR's core philosophy rests on accountability, which extends beyond compliance into demonstrable responsibility. Controllers must not only adhere to principles such as lawfulness, fairness, and transparency but must also prove compliance through verifiable documentation and independent audit mechanisms[34]. Under Article 5(2), accountability becomes both a substantive and procedural obligation, enforced by powerful supervisory authorities across the EU.

In contrast, Section 30 of the NDPA 2023 acknowledges accountability as a principle but lacks corresponding enforcement tools such as Data Protection Impact Assessments (DPIAs) or mandatory recordkeeping. The NDPA's approach therefore remains reactive rather than preventive, depending heavily on post-breach enforcement by the Nigeria Data Protection Commission (NDPC) rather than risk-based oversight[35].

Another major divergence lies in the regulation of automated decision-making and profiling. Article 22 of the GDPR explicitly provides that individuals shall not be subjected to decisions based solely on automated processing that significantly affects them, including profiling, unless specific conditions are met—such as explicit consent or necessity for contract performance[36]. The provision further guarantees the right to obtain human intervention and to challenge such decisions. The NDPA contains no equivalent clause. This omission is particularly concerning for industries like hospitality, where AI-driven personalisation directly influences pricing, service eligibility, and consumer treatment.

The GDPR also mandates Data Protection Officers (DPOs) for organisations engaging in large-scale data processing (Article 37), establishing a direct link between internal compliance and regulatory supervision. Although the NDPA requires controllers to designate compliance officers, the Act offers no detailed description of their functions or reporting obligations[37]. This lack of institutional clarity undermines accountability and weakens consumer confidence.

A further point of contrast lies in cross-border data transfers. The GDPR allows transfers only to jurisdictions that ensure an "adequate level of protection," codified under Articles 44–50. Transfers without such adequacy require additional safeguards, including Standard Contractual Clauses (SCCs) or **Binding Corporate Rules (BCRs)**[38]. The NDPA's Section 41 permits transfers where adequate safeguards exist, but does not guide what constitutes "adequacy." This vagueness has left Nigerian hospitality companies—especially multinational hotel chains—operating in regulatory uncertainty when transferring customer data to non-Nigerian servers[39].

Thus, while the GDPR exemplifies procedural robustness, the NDPA still reflects a transitional framework in need of secondary legislation, sector-specific codes, and capacity-building to operationalise its principles[40].

4.2 Case Law and Regulatory Precedents

Judicial decisions play a central role in shaping data-protection norms and clarifying ambiguities in statutory provisions. In the EU, landmark decisions such as *Digital Rights Ireland Ltd v Minister for Communications (2014) and Schrems II (2020)* illustrate the judiciary's commitment to upholding data rights as fundamental constitutional guarantees[41].

In Digital Rights Ireland, the Court of Justice of the European Union (CJEU) invalidated the EU Data Retention Directive, emphasising that indiscriminate retention of telecommunications data violated privacy and proportionality. Similarly, in Schrems II, the CJEU struck down the EU–US Privacy Shield, ruling that transfers to the United States failed to ensure "essentially equivalent protection."[42] These rulings have had profound implications for AI and data management. By recognising privacy as an element of human dignity, the CJEU set a global precedent that algorithmic processing must respect proportionality and purpose limitation. Furthermore, they demonstrate judicial willingness to invalidate regulatory frameworks that fail to meet minimum human-rights standards.

Nigeria's jurisprudence, though still developing, has begun to mirror this rights-based approach. In *Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (CA/L/722/2021),* the Court of Appeal affirmed that personal data protection is implicit within the constitutional right to privacy (Section 37 of the 1999 Constitution)[43]. The court emphasised that the government's duty to protect citizens' personal data extends to digital and automated contexts. Similarly, in Godfrey Eneye v MTN Nigeria Communications Ltd (2019), the High Court found that unauthorised disclosure of subscriber data constituted a violation of the right to privacy[44].

Collectively, these cases signify a doctrinal shift in Nigerian law—from treating privacy as a peripheral interest to recognising it as a justiciable right enforceable through constitutional and statutory mechanisms. However, courts have yet to articulate explicit standards for AI accountability, algorithmic bias, or automated profiling. This remains a significant jurisprudential gap.

At the regulatory level, the Nigeria Data Protection Commission (NDPC) has issued Advisories on High-Risk Data Processing (2024) and Strategic Guidelines for Data Compliance (2025), both emphasising the need for proactive risk management in AI applications[45]. Yet, these instruments lack binding force, illustrating the NDPC's evolving, rather than fully mature, authority.

4.3 **Consent, Transparency, and Fairness in AI Data Processing**

The concept of consent lies at the heart of data protection. Under both GDPR and NDPA, processing must be based on the data subject's explicit, informed consent unless justified by anotherlawful basis[46]. However, the advent of AI complicates this principle.

AI systems often engage in secondary data processing, deriving insights beyond the scope of initial consent—such as inferring preferences or predicting behaviours from seemingly neutral data[47]. In the hospitality industry, this might involve an AI system analysing a guest's social media activity or historical bookings to predict purchasing intent. Such inferences fall into a grey area: the guest may have consented to data use for booking but not for behavioural profiling.

The GDPR mitigates this risk through stringent transparency obligations (Articles 12–14), requiring controllers to disclose not only data categories and purposes but also the logic involved in automated decision-making[48]. Nigerian law lacks an equivalent mandate. NDPA Section 26 merely requires controllers to process data lawfully and fairly, without defining transparency in operational terms.

Moreover, AI explainability—a key tenet of GDPR's transparency principle—remains largely absent from Nigeria's regulatory vocabulary. Explainability ensures that individuals can understand how an algorithm reached a particular decision, especially when that decision affects their economic or legal rights. Its absence in NDPA leaves individuals powerless to contest algorithmic outcomes[49].

In practice, many Nigerian hospitality operators rely on third-party vendors to provide AI-based customer management systems. Contracts rarely specify data ownership, liability, or audit rights, creating accountability gaps[50]. Under GDPR's Article 28, processors must act only on documented instructions from controllers, who remain ultimately responsible. The NDPA's silence on such detailed controller–processor relationships creates uncertainty about legal responsibility when breaches occur.

4.3Accountability and Liability in AI-Driven Data Management

Accountability and liability form the normative backbone of data governance. Under the GDPR, accountability encompasses both compliance responsibility and liability for non-compliance. Controllers and processors are jointly and severally liable for damages caused by unlawful processing (Article 82)[51].

In AI contexts, liability becomes particularly challenging because decision-making is distributed and opaque. An algorithm's outcome may result from multiple actors—data suppliers, software developers, or hospitality operators—making causation difficult to establish[52]. Scholars like Mittelstadt (2022) and Wachter et al. (2017) describe this as the "problem of many hands," where accountability is diluted across the AI value chain.

The GDPR addresses this challenge by imposing strict, joint liability unless the processor proves it was not responsible for the event giving rise to damage. The NDPA, however, does not specify shared liability for controllers and processors. Instead, Section 38 vaguely refers to "responsibility of the controller," leaving unclear whether third-party vendors can be held directly liable for AI malfunctions[53].

This ambiguity presents a tangible risk for Nigeria's hospitality operators, many of whom integrate AI tools developed by external providers. Without contractual clauses allocating liability, disputes may lead to protracted litigation and reputational harm. Additionally, the NDPA lacks an explicit remedy mechanism akin to GDPR's Articles 77–82, which guarantees the right to lodge complaints with supervisory authorities and seek judicial redress. While Nigerian courts recognise fundamental rights actions, procedural access remains cumbersome, limiting consumer empowerment[54].

4.4 **Cross-Border Data Transfers and International Compliance**

The hospitality and travel sectors are inherently global. Cross-border data transfers are routine, as hotel chains and online booking platforms operate across jurisdictions. This raises critical issues of jurisdictional adequacy and extraterritorial compliance.

The GDPR asserts extraterritorial applicability under Article 3, extending its obligations to non-EU entities processing data of EU residents. Nigerian hospitality companies serving EU guests via online channels are thus indirectly bound by GDPR standards[55]. By contrast, the NDPA's Section 41 restricts transfers of personal data outside Nigeria unless "adequate safeguards" exist, but provides no methodology for determining adequacy or recognising foreign jurisdictions. This legal vacuum complicates Nigeria's participation in international tourism and digital commerce. A Nigerian hotel using a U.S.-based AI analytics tool, for instance, risks violating foreign data laws if transfers occur without explicit contractual or regulatory authorization[56].This deficiency also

undermines investor confidence. International travel brands operating in Nigeria must often duplicate compliance efforts—adhering to GDPR for EU customers and improving NDPA compliance locally. Such fragmentation hampers Nigeria's integration into global digital value chains[57].

4.5.Implications for the Travel and Hospitality Industry

The legal consequences of AI-powered data management in hospitality are multifaceted. For operators, non-compliance risks range from financial penalties and contractual liability to reputational damage and loss of consumer trust. For regulators, inadequate oversight erodes the legitimacy of data protection law itself.

AI's integration has blurred the traditional boundaries between data controllers and processors, necessitating a paradigm shift in compliance culture. Hospitality organisations must adopt privacy-by-design and ethics-by-design approaches to integrate legal compliance into technological architecture[58]. This involves early-stage risk assessments, algorithmic audits, and human oversight protocols.

The Nigerian hospitality sector, still developing its digital infrastructure, faces the dual challenge of technological dependency and regulatory immaturity. Without proactive reforms, the sector risks entrenching systemic vulnerabilities—algorithmic bias, discriminatory pricing, and cross-border data insecurity—that could undermine both consumer protection and international competitiveness[59].

5.1 Findings

This study identifies five principal findings regarding the legal, institutional, and ethical dimensions of AI-powered customer data management in Nigeria's travel and hospitality industry.

First, the Nigeria Data Protection Act 2023 (NDPA) provides an essential legal foundation for data protection but lacks explicit and enforceable provisions governing AI-driven automated decision-making, profiling, and algorithmic bias. Unlike the European Union's General Data Protection Regulation (GDPR), which explicitly protects individuals against fully automated decisions, the NDPA remains silent on the right to human intervention or contestation of algorithmic outcomes. This gap weakens consumer protection and limits the accountability of data controllers.

Second, the Nigeria Data Protection Commission (NDPC), though established as the national supervisory authority, still faces institutional and operational constraints. Insufficient technical expertise, limited funding, and a lack of sector-specific regulatory instruments have hindered its ability to monitor AI-based data processing proactively. Enforcement remains reactive, largely dependent on post-breach investigations rather than risk-based oversight.

Third, the study finds persistent ambiguity in accountability and liability allocation among controllers, processors, and AI vendors. The NDPA attributes general responsibility to controllers without defining how liability should be shared when decisions are made by autonomous or semi-autonomous systems. By contrast, the GDPR's concept of joint and several liability under Article 82 offers a clearer framework for assigning responsibility.

Fourth, cross-border data transfers continue to occur without a defined adequacy framework or standard contractual mechanisms. Given the global nature of the hospitality industry, Nigerian businesses that rely on international booking or analytics platforms risk violating foreign privacy laws and losing consumer trust due to inconsistent safeguards.

Finally, there is a notable ethical and transparency deficit in AI adoption. Hospitality organisations frequently employ personalisation and predictive analytics without disclosing data-processing logic or obtaining explicit, informed consent. The absence of algorithmic explainability and independent auditing mechanisms increases the risk of discrimination and privacy violations.

Overall, these findings demonstrate that while the NDPA 2023 marks a historic advancement in Nigeria's data-protection landscape, its procedural, institutional, and ethical gaps must be addressed to achieve effective and accountable AI governance comparable to international best practice.

5.2 Conclusion

Artificial Intelligence (AI) continues to redefine customer data management within the travel and hospitality industry, offering remarkable operational and experiential advantages while introducing significant legal and ethical challenges. This paper concludes that Nigeria's Data Protection Act 2023 (NDPA) provides a critical foundation for safeguarding data rights but lacks the procedural, institutional, and AI-specific mechanisms required for robust accountability. Comparative analysis with the European Union's General Data Protection Regulation (GDPR)

reveals that the NDPA's gaps in automated decision-making, cross-border data transfers, and enforcement capacity expose both consumers and businesses to regulatory uncertainty.

To ensure responsible innovation, Nigeria must evolve toward a risk-based, ethically grounded AI governance model—one that integrates transparency, accountability, and fairness into every layer of data processing. Legislative amendments, institutional strengthening, and cross-sector collaboration are vital to aligning national law with global standards. Ultimately, embedding privacy- and ethics-by-design within AI systems will protect consumer rights, promote business confidence, and position Nigeria's hospitality industry as a credible and competitive player in the global digital economy.

5.3 Recommendations

This study recommends a series of legislative, institutional, and ethical reforms to strengthen Nigeria's data governance framework for AI-powered customer data management in the travel and hospitality industry. Legislatively, the Nigeria Data Protection Act 2023 (NDPA) should be amended to include explicit provisions on automated decision-making, profiling, and algorithmic accountability, aligned with Article 22 of the GDPR. The Act should also mandate Data Protection Impact Assessments (DPIAs) for high-risk AI processing and define adequacy standards for cross-border data transfers.

Institutionally, the Nigeria Data Protection Commission (NDPC) must be empowered through greater autonomy, funding, and technical capacity to conduct audits, enforce sanctions, and coordinate with other regulatory agencies.

At the industry level, hospitality organisations should implement comprehensive data-protection policies, appoint compliance officers, and adopt transparent redress mechanisms for algorithmic decisions.

Ethically, a National AI Ethics and Governance Board should be established to ensure algorithmic fairness, transparency, and explainability.

Finally, regional integration through ECOWAS and the African Union should be pursued to harmonise data-protection standards and promote secure cross-border digital trade.

Together, these reforms would align Nigeria's legal framework with global standards, ensuring responsible, fair, and innovation-friendly AI deployment across the hospitality sector.

References

1. Buhalis, D., & Yen, E.C.W. (2022). Hospitality and Tourism 4.0: The Convergence of AI, IoT, and Big Data for Service Innovation.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.
3. Nigeria Data Protection Act (NDPA), 2023.
4. Ivanov, S. (2023). The Future of Hotel Technology: AI, Robotics, and Automation.
5. Akinola, S., & Oyeniran, C.I. (2024). Regulatory Lag and AI Deployment in Nigeria's Digital Economy.
6. Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.).
7. Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information.
8. L., & Cowls, J. (2022). The Ethics of AI in Human Contexts: A Unified Framework.
9. Bygrave, L.A. (2020). Data Privacy Law: An International Perspective.
10. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.
11. Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding Regulation: Theory, Strategy, and Practice.
12. EDPB (European Data Protection Board). (2021). Guidelines on Data Protection Impact Assessment (DPIA).
13. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence.
14. Ivanov, S. (2023). AI and robotics in the hospitality industry: Current applications and future trends. International Journal of Hospitality Management, 103, 103273.
15. Buhalis, D., & Yen, C. (2022). Customer data management and personalisation in hospitality: The role of AI. Journal of Hospitality and Tourism Technology, 13(1), 78–98.

16. Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1).
17. Bygrave, L. A. (2021). Data protection by design and by default. Oxford University Press.
18. Floridi, L. (2023). The ethics of artificial intelligence: Human rights and regulatory accountability. AI & Society, 38(2), 357–372.
19. Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press.
20. Yakubu, A. (2024). Nigeria's Data Protection Act 2023: Emerging issues in AI governance. Nigerian Journal of Technology Law, 7(1), 25–46.
21. Kuner, C. (2020). Transborder data flows and data privacy law. Oxford University Press.
22. OECD. (2021). OECD AI Principles. Paris: Organisation for Economic Co-operation and Development.
23. Bello, A. (2025). Institutional capacity in Nigeria's data protection ecosystem. African Journal of Law and Technology, 9(1), 56–78.
24. European Data Protection Board (EDPB). (2020). *Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default.* Brussels: EDPB.
25. Mittelstadt, B. D. (2022). Algorithmic accountability and transparency: The limits of explainability. Big Data & Society, 9(2), 1–15.
26. Tassi, A., & Recchi, E. (2023). Privacy by design and by default in AI environments: Challenges and compliance. Computer Law & Security Review, 49, 105794.
27. Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Transparent, explainable, and accountable AI for law and policy. Philosophy & Technology, 31(4), 611–627.
28. Court of Justice of the European Union (CJEU). (2014). Digital Rights Ireland Ltd v Minister for Communications (Joined Cases C-293/12 and C-594/12).
29. Court of Justice of the European Union (CJEU). (2020). Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II) (Case C-311/18).
30. Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (CA/L/722/2021) [2022] NGCA 31.
31. Godfrey Nya Eneye v MTN Nigeria Communications Ltd (FCT High Court, Suit No. CV/1365/2017, judgment delivered 2019).
32. Nigeria Data Protection Commission (NDPC). (2024). Advisory on High-Risk Data Processing Activities. Abuja: NDPC Publications.

33. Nigeria Data Protection Commission (NDPC). (2025). Strategic Guidelines for Data Compliance and AI Risk Management. Abuja: NDPC.
34. ECOWAS Commission. (2023). Regional framework for data protection and digital trade. Abuja: ECOWAS Secretariat.
35. African Union. (2022). Data Policy Framework. Addis Ababa: African Union Commission.
36. Kamba, W. J. (1974). Comparative law: A theoretical framework. International and Comparative Law Quarterly, 23(3), 485–519
37. Solove, D. J., & Schwartz, P. M. (2022). Information privacy law (7th ed.). Wolters Kluwer.
38. Cavoukian, A. (2020). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario.
39. Adadi, A., & Berrada, M. (2018). Peeking inside the black box: A survey on explainable artificial intelligence (XAI). IEEE Access, 6, 52138–52160.
40. ECOWAS Commission. (2022). Policy harmonisation for the digital economy and data protection in West Africa. Abuja: ECOWAS Secretariat.
41. World Travel & Tourism Council (WTTC). (2024). AI and the future of responsible tourism. London: WTTC Publications.
42. Federal Ministry of Communications and Digital Economy (FMoCDE). (2020). National Digital Economy Policy and Strategy (2020–2030). Abuja: FMoCDE.
43. Hospitality and Tourism Council of Nigeria (HTCN). (2025). Proposed Code of Conduct for AI in Hospitality. Draft Policy Paper.