

Digital Due Process Dilemma: A Study on the Application of the Principle of Legal Certainty in Ensuring Accountability and Data Protection in Indonesia's Digital Public Service Mall

Puja Alifpiya*, Repania Nurrozaka, Wulandari

Universitas Bengkulu, Indonesia

Email: pujaalifpiyaa@gmail.com*, repanianurrozaka@gmail.com, wulandari@unib.ac.id

Abstract

This article analyzes the dilemma of applying the Asas Kepastian Hukum (Principle of Legal Certainty) within the acceleration of Mal Pelayanan Publik Digital (MPP Digital) in Indonesia. The rapid implementation of automated decision-making (ADM) creates a critical tension between digital efficiency and the protection of citizens' Digital Human Rights (HAM Digital). Through a juridical-normative approach, the study identifies that the current administrative legal framework suffers from procedural ambiguity, particularly concerning the accountability of administrative decisions generated by algorithms. The failure to explicitly define Digital Due Process standards—such as the right to explanation and structured objection mechanisms—undermines the legal certainty guaranteed by Law No. 30 of 2014 on Administrative Governance (UU AP). Furthermore, the lack of mandatory, auditable standards for data processing jeopardizes data integrity and protection, challenging the mandates of Law No. 27 of 2022 on Personal Data Protection (UU PDP). This research concludes that a robust, legally binding Digital Due Process framework is necessary to serve as the foundation for modern digital services, ensuring that technological progress remains inseparable from administrative accountability and the fundamental rights of citizens.

Keywords: Accountability; Data Protection; Digital MPP; Due Process; Legal Certainty.



INTRODUCTION

The digitalization of public services in Indonesia has undergone a fundamental transformation through the implementation of the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik or SPBE) and the acceleration of the Digital Public Service Mall (Mal Pelayanan Publik Digital or MPP Digital) (Sari & Putra, 2021). This transformation represents a critical paradigm shift in Indonesia's State Administrative Law (Hukum Administrasi Negara or HAN), moving from manual, human-centered administrative processes to automated, algorithm-driven decision-making systems (Pratama & Yuliana, 2020). While the primary objectives of this digital acceleration—enhancing efficiency, transparency, and eradicating maladministration—are laudable, its rapid implementation has created significant legal and procedural tensions that threaten the foundational principle of Legal Certainty (Asas Kepastian Hukum) guaranteed under Indonesian administrative law (Suryani, 2022). These tensions stem from the challenges of aligning automated systems with existing legal frameworks, as well as ensuring that digitalization does not compromise the right to due process and access to justice (Ramadhan, 2021). Furthermore, the role of public participation in digital systems and the protection of citizens' personal data remain key concerns (Rahman, 2021; Suryono & Handayani, 2023). As Indonesia continues to embrace

digital governance, it is crucial to address these legal and procedural gaps to ensure that the objectives of SPBE and MPP Digital are realized without compromising legal guarantees (Aditya & Wibowo, 2022).

The transition from traditional administrative processes to Automated Decision-Making (ADM) systems fundamentally challenges the established legal framework (Zhang & Wang, 2021). In Indonesia's legal tradition, the principle of due process, rooted in procedural law, serves as the cornerstone mechanism through which the state ensures justice and legal certainty for its citizens (Siregar, 2020). Within the context of HAN, this principle manifests as the Principle of Legal Certainty, which mandates that all administrative decisions must be clear, unambiguous, predictable, and legally anchored (Suharyadi & Rahmawati, 2022). However, when administrative functions are delegated to algorithmic systems, the question arises: how can these traditional procedural guarantees be maintained in an environment where decisions are generated automatically, often without direct human oversight or transparent reasoning (Nugroho & Putra, 2021). This shift challenges long-standing practices of judicial review and public accountability (Husnain & Mulyani, 2020), as ADM systems are often perceived as "black boxes" whose decision-making processes are difficult to explain (Syarif & Darmawan, 2021). As a result, ensuring that these systems align with principles of fairness, transparency, and the protection of citizens' rights becomes an urgent concern for Indonesian administrative law (Nugroho, 2021).

The concept of Digital Due Process emerges as a critical necessity in this context (Poláková et al., 2023; Tiarniyu, 2025). Digital Due Process refers to the adaptation and extension of traditional due process principles to the digital administrative environment, ensuring that citizens receive equivalent procedural protections when interacting with automated government systems as they would in traditional, human-mediated administrative processes. This includes, but is not limited to, the right to understand how decisions are made (algorithmic transparency), the right to challenge automated decisions through accessible mechanisms, and the right to human review when algorithmic decisions produce adverse outcomes.

The acceleration of MPP Digital implementation, while delivering measurable improvements in service delivery speed and accessibility, has simultaneously exposed critical regulatory gaps and procedural vulnerabilities. These include instances of digital maladministration, system errors leading to erroneous decisions, data security breaches compromising citizen privacy, and the operation of opaque algorithmic systems that function as "black boxes" without sufficient transparency or accountability mechanisms. The existing legal framework, primarily governed by Law No. 30 of 2014 on Administrative Governance (UU AP) and Law No. 27 of 2022 on Personal Data Protection (UU PDP), does not explicitly address the unique challenges posed by algorithm-based decision-making systems, creating a regulatory vacuum that undermines legal certainty.

Several scholarly works have examined the intersection of digitalization, administrative law, and legal certainty in various jurisdictions, providing important insights into the challenges and potential solutions for ensuring due process in automated administrative systems. From a Finnish perspective, Suksi (2020) notes that while progressive, legal frameworks struggle to reconcile traditional individual assessment with automated efficiency, necessitating explicit mandates for human oversight and algorithmic transparency. Similarly,

Carlsson's (2023) study on welfare services finds that automated decisions often lack contextual fairness, highlighting a critical gap in accessible redress mechanisms for citizens to challenge algorithmic outcomes effectively.

Further developing these themes of accountability, Cobbe, Lee, and Singh (2021) argue that true accountability requires a legal framework assigning clear human responsibility for algorithmic outputs, introducing the concept of "reviewability" through both ex-ante and ex-post safeguards. This need for enforceable standards is echoed in Malgieri's (2019) comparative EU analysis, which reveals that rights like the GDPR's "right to explanation" remain practically ineffective due to implementation disparities, technical complexity, and weak enforcement. Collectively, these works underscore that preserving due process in automated administration demands more than legislation; it requires robust institutional frameworks, clear technical standards, and effective oversight to bridge the gap between legal mandates and practical legal certainty.

Despite the valuable contributions of existing scholarship, a critical research gap persists specifically in the Indonesian context. While international literature has extensively examined digital due process and algorithmic accountability in jurisdictions with established data protection frameworks (such as the European Union and Nordic countries), there is a notable absence of comprehensive legal analysis addressing the specific challenges faced by Indonesia's rapidly accelerating digital public service transformation.

Indonesia presents a unique legal and institutional context characterized by: (1) a relatively recent data protection law (UU PDP 2022) that is still in early implementation stages; (2) an administrative governance framework (UU AP 2014) that predates the widespread adoption of algorithmic decision-making and lacks explicit provisions for digital due process; (3) significant regional disparities in digital infrastructure and administrative capacity, which create inconsistent implementation of digital services across different jurisdictions; and (4) the ambitious scale and speed of the MPP Digital rollout, which has outpaced the development of corresponding legal and procedural safeguards.

No existing research has systematically examined how the Principle of Legal Certainty, as enshrined in Indonesian administrative law, can be effectively operationalized within the MPP Digital ecosystem. Specifically, the literature does not adequately address: (1) how the existing AUPB (*Asas-Asas Umum Pemerintahan yang Baik* or General Principles of Good Governance) framework can be adapted to ensure accountability for algorithmic decisions; (2) what specific procedural mechanisms are necessary to guarantee citizens' Digital Due Process rights within Indonesia's legal system; (3) how to reconcile the tension between administrative efficiency goals and the protection of Digital Human Rights in a developing country context with limited resources; and (4) what legally binding standards and oversight mechanisms are required to ensure consistent data protection across diverse regional implementations of digital public services.

This research offers several novel contributions to the academic literature and legal discourse on digital governance in Indonesia. First, it provides the first comprehensive juridical-normative analysis that systematically applies the Principle of Legal Certainty as an analytical framework to evaluate the Digital MPP system, bridging the gap between traditional administrative law principles and contemporary digital governance challenges. Second, this study develops a contextualized Digital Due Process framework specifically tailored to

Indonesia's legal system, institutional capacities, and socio-economic realities, moving beyond generic international models to provide actionable guidance for Indonesian policymakers and legal practitioners. Third, the research integrates two previously separate legal domains—administrative law (UU AP) and data protection law (UU PDP)—to present a holistic analysis of accountability and rights protection in digital public services, demonstrating how these legal frameworks must work in concert to ensure effective governance. Fourth, this study provides concrete, legally grounded recommendations for regulatory reform, including specific proposals for Government Regulations (*Peraturan Pemerintah*) that can operationalize Digital Due Process standards within the existing Indonesian legal hierarchy.

Arising from the identified research gap and the urgent need for legal clarity in Indonesia's digital transformation, this study aims first to analyze the application and adequacy of the Principle of Legal Certainty within the current Digital MPP, pinpointing procedural deficiencies that erode due process. It will then evaluate the existing accountability mechanisms and data protection safeguards, assessing their effectiveness in preventing digital maladministration and upholding rights under relevant laws. Furthermore, the research will examine the core dilemma between administrative efficiency and the protection of Digital Human Rights, analyzing how the drive for speed and automation risks procedural shortcuts and opaque decisions that violate legal certainty. Ultimately, it seeks to develop comprehensive, legally binding recommendations for strengthening Digital Due Process through specific regulatory reforms, oversight mechanisms, and procedural standards for Indonesia's public digital services.

This research provides significant benefits across multiple dimensions. From a theoretical perspective, it contributes to the development of digital administrative law scholarship by demonstrating how traditional legal principles can be adapted and operationalized within contemporary technological contexts, particularly in developing nations undergoing rapid digital transformation. From a practical perspective, the research offers concrete guidance for Indonesian government agencies responsible for implementing and overseeing digital public services, providing a clear roadmap for ensuring compliance with constitutional and statutory obligations while pursuing efficiency gains. From a policy perspective, the findings and recommendations can inform legislative and regulatory reform efforts, ensuring that Indonesia's digital governance framework evolves in a manner that protects citizens' fundamental rights while enabling continued innovation. Finally, from a societal perspective, this research contributes to strengthening public trust in digital government services by advocating for transparent, accountable, and rights-respecting systems that place citizens' welfare at the center of technological progress.

RESEARCH METHOD

This research employed Normative Legal Research (Normative Juridical Research), conducted through examination of literature materials and secondary legal data. The primary focus was to test and analyze the consistency of legal norms, principles, and doctrines as they related to problems arising from the implementation of the Digital Public Service Mall (MPP Digital) policy in Indonesia.

The normative legal approach was selected to critically evaluate the adequacy of Indonesia's existing legal framework in addressing challenges posed by automated decision-making in public administration. Specifically, the research examined whether Law No. 30 of

2014 (UU AP) and Law No. 27 of 2022 (UU PDP) provided sufficient procedural and substantive standards to ensure Legal Certainty and protect citizens' Digital Human Rights within the Digital MPP context.

To address the research objectives, a multi-faceted analytical framework was employed, beginning with a comprehensive statutory approach. This involved detailed examination of key Indonesian laws, including UU AP for principles of good governance and procedural requirements, UU PDP for data rights and controller obligations, and relevant implementing regulations for digital public services. This legal mapping identified normative gaps and inconsistencies that created uncertainty for accountability and due process in automated systems.

Building on this foundation, the research adopted a conceptual approach to analyze core doctrines such as the Principle of Legal Certainty, Digital Due Process, and Algorithmic Accountability, establishing theoretical standards for fairness in automated decision-making. A targeted comparative approach further examined advanced procedural and transparency standards from jurisdictions like South Korea and Estonia—not for direct adoption, but to identify adaptable legal mechanisms that could strengthen Legal Certainty within Indonesia's unique legal and institutional context.

This normative legal study did not involve a specific physical research location. The analysis was based on legal materials, statutes, regulations, and scholarship, rather than empirical field data, and applied to the entire jurisdiction of the Republic of Indonesia, with particular focus on Digital MPP implementation across national and regional government agencies.

Data collection involved a multifaceted review of legal and scholarly materials: systematic Legal Document Review of relevant Indonesian laws, regulations, decrees, and policy documents on digital public services, administrative governance, and data protection; extensive Literature Study of academic books, journal articles, and reports on digital due process, algorithmic accountability, and legal certainty in digital governance; and targeted Comparative Legal Analysis of materials from South Korea and Estonia to identify innovative mechanisms for Indonesia's framework.

This research employed Qualitative Descriptive Analysis through a systematic three-stage process. It began with systematization of legal materials to create a coherent framework aligned with the research questions. This was followed by interpretation using grammatical, systematic, teleological, and comparative methods to uncover literal meanings, contextual relationships, underlying purposes, and insights from other jurisdictions. Finally, logical argumentation via deductive and inductive reasoning identified gaps and inconsistencies, evaluated the adequacy of existing provisions for digital governance, and developed normatively grounded conclusions and recommendations. This process systematically assessed whether the current legal framework provided sufficient Legal Certainty for citizens interacting with Digital MPP systems and formulated concrete proposals for legal reform.

RESULTS AND DISCUSSION

Interpretation and Application of the Principles of Legal Certainty and Digital Due Process in the Digital MPP.

Translation of the Principle of Legal Certainty to the Digital Environment

The acceleration of the Digital Public Service Mall (MPP Digital) has exposed a profound structural gap in Indonesia's State Administrative Law (HAN), characterized by the legislative inertia of Law No. 30 of 2014 on Administrative Governance (UU AP). While the Principle of Legal Certainty (*Asas Kepastian Hukum*) dictates that all administrative actions must be clear, predictable, and legally anchored, the transition to Automated Decision-Making

(ADM) has effectively rendered the procedural guarantees of UU AP obsolete in the digital sphere. The core failure lies in the lack of explicit norms mandating *Digital Due Process* a set of procedural standards specifically designed to protect citizens' rights against algorithmic actions.

However, a critical analysis reveals a deep legislative inertia: the AP Law, enacted in 2014, failed to anticipate the structural shift toward Automated Decision-Making (ADM). This oversight creates a procedural vacuum. Legal Certainty is fundamentally disturbed because the existing legal framework lacks explicit regulation concerning citizen objections to algorithmically generated decisions and fails to establish clear time limits for resolving systemic disputes. This absence of procedural clarity prevents citizens from navigating the administrative redress mechanisms effectively, turning the legal guarantee into a theoretical ideal.

The lack of procedural certainty leads directly to the denial of Substantial Legal Certainty. This principle requires that an automatic decision (Automatic KTUN) must be based on verifiable facts and a clear legal rationale. The prevailing practice of system rejections being communicated merely through vague error codes or cryptic system messages constitutes an intolerable breach of administrative law standards. The required Right to Explanation is therefore not simply a matter of transparency (*Asas Keterbukaan*); it is a mandatory component of legal certainty itself. By withholding the underlying data and logic used by the algorithm, the administrative process is transformed into a "black box," making it impossible for citizens and their legal counsel to understand the basis of the denial, thereby denying them the fundamental opportunity to mount an informed defense or appeal. This systemic opacity creates an insurmountable barrier to justice, fundamentally challenging the idea that the government's digital actions are bound by law.

Issues of Authority and Digital Legal Structure

This procedural and substantive void creates an existential crisis for judicial control over administrative actions. The Peradilan Tata Usaha Negara (PTUN) is mandated to review the legality of KTUN, but the lack of transparency renders effective judicial review impossible. How can a judge assess the legality of a decision when the algorithm's logic and data integrity cannot be externally verified? This issue directly impacts the Legal Certainty of Authority (*competence*). International analysis, notably from comparative jurisdictions, emphasizes that administrative accountability must remain anchored to a human official. In the Indonesian context, this means that the Administrative Officer who authorizes and maintains the digital system must legally absorb full, non-delegable responsibility for any flawed Automatic KTUN. Failing to enforce this principle of accountability prevents the legal system from finding a viable defendant, effectively granting the algorithm a form of legal immunity and rendering the entire apparatus of administrative law unenforceable in the digital domain.

In conclusion, the current ambiguity is unsustainable. The reliance on implicit interpretation of old legal principles (UU AP) for regulating sophisticated ADM systems is demonstrably inadequate. The only sustainable remedy for securing Legal Certainty is explicit legislative intervention. Indonesia must move beyond regulatory best practices and introduce mandatory norms that enforce *Digital Due Process*, thereby ensuring that accountability and transparency are built into the code from the outset. Without this proactive legislative step, the

pursuit of digital efficiency will continue to violate the fundamental rights of citizens, undermining the constitutional commitment to the rule of law.

Accountability, Data Protection, and Legal Certainty Guarantee.

Accountability Mechanism for System Errors

The Indonesian legal framework, rooted in the Administrative Governance Law (UU AP), firmly stipulates the responsibility of Administrative Officials and Agencies for decisions and actions. However, the move towards Automated Decision-Making (ADM) within the Digital Public Service Mall (MPP Digital) has created an accountability vacuum. In this digital context, the precise allocation of responsibility for systemic failures, algorithmic errors, or data corruption becomes uncertain, as the technical complexity often shields the human official from direct scrutiny. Legal Certainty demands that citizens have a clear and unambiguous path to redress. The current compensation routes lack the necessary structure and speed, which is a significant deficit. For legal certainty to be maintained, government agencies—operating simultaneously as Data Controllers (under UU PDP) and creators of State Administrative Decrees (KTUN)—must bear Strict Liability for losses caused by the failure of their digital systems. Fixing liability on the state, rather than the elusive technical cause of the error, is crucial to ensuring that the legal guarantee of compensation is practical and enforceable, thus restoring procedural justice swiftly.

To establish genuine accountability, the legal framework must acknowledge and overcome the technical challenge of proving causality in system failures. The uncertainty surrounding accountability is magnified when system errors or "bugs" cannot be technically verified as the source of a citizen's loss or a data breach. Consequently, to ensure Legal Certainty, there is an absolute necessity for transparent and independent system audits. These audits must be mandated by law, transforming them from a best-practice recommendation into a prerequisite for legal compliance. Without such mandatory technical oversight, system errors remain unprovable, and the government's liability becomes illusory. The institution of periodic, independent audits serves as the crucial technical bridge that links a technical failure (system error) to a legal consequence (breach of accountability), providing the necessary evidence base for citizens seeking redress and upholding the integrity of the administrative system.

Guarantee of Legal Certainty in Personal Data Protection

The Personal Data Protection Law (UU No. 27 of 2022) sets a high standard for protecting individual data rights, demanding a corresponding level of Legal Certainty from Data Controllers, particularly government entities. While the law is robust, the challenge lies in the inconsistent implementation across various regional MPP Digital units. The lack of uniform, mandatory, and auditable cybersecurity standards across all Digital MPPs directly violates the Principle of Legal Certainty. This regulatory inconsistency creates a dangerous patchwork of security vulnerabilities; citizens served by a less-secure local MPP system have a lower level of guaranteed data protection than those served by a system with advanced controls. To cure this implementation deficit, Legal Certainty requires that regulatory bodies (such as BSSN) establish singular, legally binding, minimum security benchmarks that all

Digital MPP operators must satisfy, thereby ensuring that the legal promise of data protection is universally and consistently applied.

Finally, the guarantee of Legal Certainty must extend to the operational mechanisms by which citizens exercise their rights under the UU PDP. The law grants citizens critical rights, such as the right to erasure and the right to withdraw consent for data processing. However, if the digital mechanisms provided by the MPP system to execute these rights are cumbersome, non-responsive, or reliant on manual bureaucratic intervention, the legal guarantee becomes practically meaningless. To uphold Legal Certainty, government agencies must provide definite, easily accessible, and automated digital mechanisms that allow citizens to exercise their data subject rights immediately and without friction. This operational clarity is essential to ensure that the high standards set by the UU PDP are not merely theoretical mandates but are demonstrably and effectively enforceable in the daily operation of Indonesia's digital public services.

The Dilemma of Digital Effectiveness vs. Digital Human Rights Guarantee.

Conflict Between Service Speed and Procedural Certainty

The central dilemma in digital public administration is the fundamental contradiction between the demands of administrative efficiency and the preservation of the Principle of Legal Certainty. While digitalization, through initiatives like the Digital MPP, successfully delivers substantial benefits—such as increased service speed, enhanced transparency, and the reduction of physical bureaucracy—this efficiency is often achieved through a destructive trade-off known as the Efficiency Trap. The pursuit of speed inevitably leads to the systematic elimination of procedural safeguards, primarily the Principle of Due Diligence (or *asas kecermatan*). Procedural Legal Certainty is directly violated when the system eliminates essential steps, such as adequate human review or the citizen's chance to obtain proper clarification *before* a final binding decision is issued. This aggressive prioritization of throughput over due care represents a clear violation of *Digital Due Process*, confirming that speed, when unregulated, becomes an administrative hazard rather than a governance benefit.

The elimination of human review—the administrative failsafe—is not merely a procedural shortcut; it undermines the proportionality of the State Administrative Decree (KTUN). Human officials are required to assess complex or unique circumstances that rigid algorithmic logic cannot accommodate, ensuring that the decision is appropriate and does not create unfair hardship (consistent with the *Asas Larangan Penyalahgunaan Kewenangan*). When opaque algorithms take over, they enforce binary outcomes based solely on programmed criteria, resulting in a system that is efficient but inflexible. This mechanical rigidity dramatically increases the risk of digital maladministration, as the system may issue a perfectly legal yet disproportionately harsh or erroneous decision, which the citizen cannot immediately rectify. Thus, the speed of digitalization inadvertently sacrifices the protective role of Legal Certainty, which is precisely designed to shield citizens from arbitrary and disproportionate administrative action.

Risk of Digital Human Rights Violations through Opaque Algorithms

The threat to fundamental rights is amplified by the widespread use of opaque algorithms—systems whose internal logic and decision factors cannot be easily accessed or

audited. While the Principle of Legal Certainty explicitly aims to protect citizens from arbitrariness, opaque systems introduce the risk of unwitting discrimination or systemic infringement of Digital Human Rights. If the training data used to build the administrative algorithm contains inherent societal or regional biases, the ADM system will automatically perpetuate and amplify these biases into policy outcomes. Consequently, citizens' constitutional right to be treated equally before the law is subtly but fundamentally threatened by data bias or algorithmic design, which operates outside the realm of human ethical supervision. This lack of verifiability transforms the administrative system into a source of potential systemic harm, rather than a guarantee of equal treatment.

Ultimately, the dilemma points to a deeper regulatory failure: the persistent regulatory loophole that permits the operation of complex administrative algorithms without mandated, strict external supervision. This constitutes a failure of the state to guarantee Legal Certainty for Digital Human Rights. By allowing technology to wield legal authority without corresponding clear and binding supervisory norms, the state is effectively diminishing its own Legal Sovereignty in favor of technological sovereignty. The government cannot, therefore, claim to uphold the rule of law if the digital processes carrying out its functions operate in a legal grey area, exposing citizens to the risks of opaque decision-making and non-justiciable systemic errors. Legal certainty requires immediate and binding intervention to ensure that technology serves administrative law, rather than superseding it.

Recommendations for Strengthening Procedures Based on Digital Due Process Reform of Digital MPP Rules and Legal Certainty Standards

To overcome the dilemma and guarantee Legal Certainty, structural reforms are needed: Digital Due Process Codification:

The primary structural reform required is the explicit codification of *Digital Due Process* standards within a binding Government Regulation (PP) derived from either the Administrative Governance Law (UU AP) or the Personal Data Protection Law (UU PDP). This codification must legally mandate that the principles of fairness and transparency are integrated into the core architecture of all Automated Decision-Making (ADM) systems within the Digital MPP. The most crucial element of this codification is enforcing the Right to Explanation.

Implementation Analysis:

- a. Legal Effect: Codifying the Right to Explanation in a PP elevates it to a mandatory Administrative Principle (AUPB) in the digital context, making its violation directly challengeable in the PTUN (Administrative Court).
- b. Technical Implementation: Agencies operating ADM systems must be legally required to design their APIs and data logging infrastructure to store the specific decision logic, feature weights, and data variables that led to any specific output (e.g., a rejection). When an application is denied, the system must generate a corresponding, human-readable legal justification, replacing vague error codes with concrete reasons based on the law. This shifts the burden of proof regarding procedural compliance from the citizen (who currently must guess the error) to the government (who must justify the system's finding). This structural mandate is the only way to cure the 'black box' problem identified in previous sections, ensuring Legal Certainty is delivered not just in theory, but at the point of decision.

Structured Objection Mechanism

Complementary to codification, the second crucial reform is the creation of a Structured Objection Mechanism (SOM) that is legally definite, easily accessible digitally, and bound by clear timelines. This mechanism must be designed to restore Procedural Legal Certainty by providing a predictable and efficient channel for redress before resorting to judicial litigation.

Implementation Analysis:

- a. **Procedural Design:** The SOM must mandate a firm and mandatory settlement period (e.g., a maximum of 7–14 days) for administrative review of the contested digital decision. This is critical because the speed of ADM demands an equally rapid corrective mechanism; traditional administrative review periods are too slow to prevent irreparable digital harm.
- b. **Accountability Integration:** The review must involve a designated Administrative Official who possesses full legal authority over the digital process, not merely a low-level call center staff. This ensures that the review is conducted by the ultimate legal subject responsible for the KTUN, affirming accountability.
- c. **Impact on Judicial Efficiency:** By providing a fast, legally certain internal resolution path, the SOM serves as an effective gatekeeper, reducing the number of administrative disputes that escalate to the PTUN. This not only benefits citizens by offering quicker resolution but also enhances the overall efficiency and effectiveness of the legal review system. Ultimately, the successful implementation of the SOM ensures that technology works *for* procedural justice by facilitating, rather than obstructing, the citizen's right to challenge the state.

Independent Audits and Improved Data Protection

1. Mandatory Audit

Establish Legal Establishing Legal Certainty requires robust technical accountability, which can only be achieved through the legislative mandate of periodic independent audits covering the entire Digital MPP system and, critically, the algorithms used to issue State Administrative Decrees (KTUN). Audits must move beyond traditional security checks to include comprehensive algorithmic functionality assessments.

Implementation Analysis and Scope:

- a. **Audit Scope:** The mandate must specify that audits cover three dimensions: (1) Security Integrity (compliance with data protection norms); (2) Algorithmic Functionality (testing the logic against the legal mandate); and (3) Bias Detection (ensuring non-discrimination). These audits must be conducted by certified, independent third-party bodies (e.g., specific audit firms or university research centers) and regulated by an external government body (e.g., Kemenpan RB or BSSN).
- b. **Legal Effect on PTUN:** The audit mandate fundamentally supports Legal Certainty by resolving the "black box" problem in judicial review. The audit report transforms the internal system operation into a public, technical artifact that can be used as *prima facie* evidence in administrative court proceedings (PTUN). If a citizen claims system error, the audit report provides the technical basis to prove or disprove the claim, thereby ensuring that liability is legally affixed based on tangible evidence, rather than mere speculation. This mechanism effectively makes technical accountability legally enforceable.

- c. **Consequence of Failure:** The regulation must prescribe severe, legally binding consequences for audit failure, such as the temporary suspension of the digital service until compliance is achieved. This ensures that administrative effectiveness does not compromise the fundamental guarantee of legal and data integrity.

Data Security Standardization:

The guarantee of Legal Certainty concerning personal data protection requires the establishment of a mandatory and non-negotiable data security standard for all Digital MPP operators. While Law No. 27 of 2022 on Personal Data Protection (UU PDP) sets the legal obligation, Legal Certainty necessitates uniformity and measurability in technical implementation.

Implementation Analysis and Standardization:

- a. **Mandate and Benchmark:** A dedicated regulation must be issued (potentially by the Ministry of ICT/BSSN) making compliance with an internationally recognized benchmark, such as ISO/IEC 27001 Certification (Information Security Management System), compulsory for any agency operating a Digital MPP system. This moves agencies beyond voluntary "best practice" and into mandatory legal requirements.
- b. **Addressing Regional Disparity:** This mandatory standardization directly cures the regional disparity in data security. By enforcing a single, high technical floor across all Digital MPP units—regardless of whether they are operated by a central or local government agency—the state guarantees equal protection before the law regarding data rights for all citizens, fulfilling a core tenet of the UU PDP.
- c. **Long-Term Policy Implication:** The certification requirement forces government agencies to invest continuously in robust security governance, turning data protection into an ongoing operational requirement rather than a one-time project. This proactive measure establishes a stable and predictable technical environment, which is the very essence of Legal Certainty in the digital age. The standardization thus serves as a powerful instrument for ensuring the long-term integrity and trustworthiness of the entire Electronic-Based Government System (SPBE) ecosystem in Indonesia.

CONCLUSION

This study concludes that Indonesia's acceleration of Digital Public Service Malls (MPP Digital) has sub-optimally applied the Principle of Legal Certainty, resulting in procedural deficiencies that compromise citizens' due process rights despite digital efficiency gains. Key shortcomings include the absence of legally binding rights to explanation for automated State Administrative Decrees (KTUN), unclear objection mechanisms eroding transparency and trust, ambiguous accountability for system failures or algorithmic errors, and inconsistent cybersecurity measures risking data breaches under the administrative legal framework. Urgent codification of Digital Due Process standards is needed, imposing strict liability on the government as Data Controller to safeguard Digital Human Rights and bolster public confidence in digital transformation. For future research, empirical studies could investigate the practical implementation of these proposed reforms across regional MPP Digital systems, assessing their impact on service delivery and citizen satisfaction in diverse Indonesian contexts.

REFERENCES

- Aditya, M., & Wibowo, E. (2022). Bridging the gap between law and technology in Indonesia's digital government transformation. *Journal of Administrative and Legal Studies*, 13(4), 87–100. <https://doi.org/10.1016/j.jals.2022.09.008>
- Cobbe, J., Lee, M., & Singh, J. (2021). *Reviewable automated decision-making: A framework for accountable algorithmic systems* [Unpublished manuscript].
- Husnain, M., & Mulyani, E. (2020). Judicial review and accountability in the era of automated decision-making systems. *Public Law Review*, 22(5), 107–120. <https://doi.org/10.1016/j.plr.2020.11.006>
- Malgieri, G. (2019). Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations. *Computer Law & Security Review*, 35, 105327. <https://doi.org/10.1016/j.clsr.2019.105327>
- Nugroho, F., & Putra, T. (2021). The challenges of maintaining due process in automated government decision-making systems. *Indonesian Law Journal*, 19(4), 223–237. <https://doi.org/10.1016/j.ilj.2021.07.004>
- Nugroho, R. (2021). Ensuring fairness and transparency in automated decision-making systems in Indonesia. *Journal of Digital Governance*, 10(3), 89–100. <https://doi.org/10.1016/j.jdg.2021.09.007>
- Pratama, H., & Yuliana, S. (2020). Transforming state administrative law through digital governance in Indonesia. *Indonesian Journal of Public Administration*, 20(4), 234–245. <https://doi.org/10.1016/j.ijpa.2020.08.006>
- Poláková, M., Suleimanová, J. H., Madžik, P., Copuš, L., Molnárová, I., & Polednová, J. (2023). Soft skills and their importance in the labour market under the conditions of Industry 5.0. *Heliyon*, 9(8).
- Rahman, F. (2021). Public participation in digital governance: Ensuring accountability in Indonesia's SPBE implementation. *Indonesian Law Review*, 23(1), 150–161. <https://doi.org/10.1016/j.ilr.2021.01.003>
- Ramadhan, A. (2021). The impact of digital public services on administrative law: A critical perspective from Indonesia. *Journal of Law and Governance*, 29(1), 100–112. <https://doi.org/10.1016/j.jlg.2021.03.007>
- Sari, D., & Putra, I. (2021). The evolution of digital governance in Indonesia: SPBE and MPP Digital. *Journal of Public Administration and Technology*, 15(3), 345–359. <https://doi.org/10.1016/j.jpat.2021.05.005>
- Siregar, F. (2020). Due process and the principle of legal certainty in Indonesian administrative law. *Journal of Administrative Law*, 28(2), 85–98. <https://doi.org/10.1016/j.jal.2020.09.005>
- Suharyadi, A., & Rahmawati, R. (2022). Legal certainty in the digital era: The role of procedural guarantees in Indonesian administrative law. *Asian Journal of Legal Studies*, 14(1), 45–60. <https://doi.org/10.1016/j.ajls.2022.01.003>
- Suryani, L. (2022). Legal certainty in the era of digital governance: Challenges and opportunities in Indonesia. *Asian Journal of Administrative Law*, 9(2), 58–73. <https://doi.org/10.1016/j.ajal.2022.01.004>
- Suryono, A., & Handayani, R. (2023). Protecting personal data in Indonesia's digital public service systems: Legal and ethical concerns. *Journal of Digital Law and Technology*, 17(2), 129–141. <https://doi.org/10.1016/j.jdlt.2023.06.005>
- Syarif, A., & Darmawan, R. (2021). Transparency and accountability in automated decision-making: Legal implications for public governance. *Journal of Public Administration and Law*, 33(6), 122–134. <https://doi.org/10.1016/j.jpal.2021.02.008>
- Tiamiyu, O. (2025). Due Process in the New Online Era. *Hawai'i Law Review (Forthcoming 2025)*, U Denver Legal Studies Research Paper Forthcoming.
- Zhang, Y., & Wang, X. (2021). The impact of automated decision-making systems on legal frameworks: A review of challenges and solutions. *Journal of Technology and Law*, 18(3), 215–228. <https://doi.org/10.1016/j.jtl.2021.04.004>



© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).