

Reconstructing Administrative Due Process in Algorithm-Based Government Decision-Making

Kurnia Arik Nugroho*

Faculty of Law, Universitas Dirgantara Marsekal Suryadarma, Indonesia

*Correspondence: arikkn7@gmail.com

Received: 17 August 2026

Accepted: 08 September 2026

Published: 21 September 2026

Abstrak

Penelitian ini mengkaji kecukupan kerangka hukum administrasi Indonesia dalam menjamin due process ketika keputusan pemerintahan dibuat atau dipengaruhi secara material oleh sistem algoritmik. Penelitian menggunakan metode hukum normatif preskriptif dengan pendekatan perundang-undangan, konseptual, kasus, dan perbandingan fungsional. Kerangka hukum dipetakan melalui 54 indikator dalam Six-Layer Administrative Due Process Model (DPA-6). Hasil pemetaan menunjukkan 19 indikator telah tersedia, 24 masih ambigu, dan 11 belum diatur secara khusus. Hukum Indonesia telah menyediakan dasar penting melalui asas legalitas, Asas-Asas Umum Pemerintahan yang Baik, perlindungan data pribadi, upaya administratif, alat bukti elektronik, mekanisme audit, Ombudsman, dan peradilan tata usaha negara. Kesenjangan utama terdapat pada meaningful human review, klasifikasi risiko, algorithmic impact assessment, pengujian bias, versioning sistem, penjelasan yang dapat dipersoalkan, dan audit trail pada tingkat keputusan. Penelitian ini mengusulkan DPA-6 sebagai model siklus terpadu yang menghubungkan legalitas dan risiko, kewajiban sebelum keputusan, pemberitahuan dan penjelasan, peninjauan manusia yang bermakna, upaya administratif yang efektif, serta audit, adjudikasi, dan pemulihan dengan prinsip proporsionalitas berdasarkan tingkat risiko keputusan.

Kata Kunci: keputusan algoritmik; due process administratif; peninjauan manusia yang bermakna; akuntabilitas algoritmik; upaya administratif

Abstract

This study examines the adequacy of Indonesia's administrative law framework in safeguarding due process when government decisions are made or materially influenced by algorithmic systems. Using prescriptive doctrinal legal research, the study integrates statutory, conceptual, case, and functional comparative approaches and maps the legal framework through 54 indicators within a Six-Layer Administrative Due Process Model (DPA-6). The mapping identifies 19 indicators as available, 24 as ambiguous, and 11 as not yet specifically regulated. Existing law provides important foundations through legality, the General Principles of Good Governance, personal data protection, administrative remedies, electronic evidence, audit mechanisms, the Ombudsman, and administrative adjudication. The principal gaps concern meaningful human review, risk classification, algorithmic impact assessment, bias testing, system versioning, contestable explanations, and decision-level audit trails. The study proposes DPA-6 as an integrated lifecycle model covering legality and risk, pre-decision duties, notice and explanation, meaningful human review, effective administrative remedies, and audit, adjudication, and remediation. The model links citizens' rights, official responsibility,

documentation, oversight, and remedies while preserving proportionality according to decision risk.

Keywords: *algorithmic decision-making; administrative due process; meaningful human review; algorithmic accountability; administrative remedies*

INTRODUCTION

Indonesia's digital transformation of government has moved from the digitization of procedures toward the integration of data, services, and decision-making. Presidential Regulation Number 95 of 2018 concerning the Electronic-Based Government System (SPBE) initially provided the framework for technology-based government administration. This direction was subsequently deepened through Presidential Regulation Number 132 of 2022 concerning the National SPBE Architecture and Presidential Regulation Number 82 of 2023 concerning the Acceleration of Digital Transformation and Integration of National Digital Services. At the next policy stage, the Government prepared a Draft Presidential Regulation on Digital Government to address service fragmentation, application duplication, limited data interoperability, and weak orientation toward service outcomes. Digital systems therefore no longer function merely as service-delivery channels. They increasingly operate as infrastructure that profiles individuals, verifies requirements, sets priorities, and influences decisions that directly affect citizens.¹

This transformation creates genuine opportunities to improve public services. Large-scale data processing and algorithm-based systems can reduce repetitive work, accelerate verification, detect inconsistencies, and generate more consistent recommendations. Kencono, Putri, and Handoko explain that digital government transformation can improve service efficiency and integration, although its success remains dependent on governance, institutional capacity, security, and interoperability. In decision-making, Heriansyah and Erliyana likewise show that artificial intelligence can reduce administrative burdens and support faster decisions. Efficiency, however, does not by itself establish legality or fairness. When system outputs are used to accept or reject applications, determine benefit eligibility, assign risk rankings, verify identities, or set service priorities, the issue shifts from a technical choice to the exercise of governmental power.²

In administrative law, the use of technology does not eliminate the duty of public officials to act on the basis of lawful authority, procedure, and substance. Law Number 30 of 2014 concerning Government Administration places legality and the General Principles of Good Governance (AUPB) at the center of assessing government decisions and actions. The principles of legal certainty, due care, transparency,

¹ Kementrian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, "Partisipasi Rancangan Peraturan Presiden Tentang Pemerintah Digital," 2026, <https://jdih.menpan.go.id/rancangan-puu/partisipasi-rancangan-puu>.

² F Heriansyah and A Erliyana, "Kecerdasan Buatan Menjadi Pemeran Pengganti Pejabat Pemerintahan," *Jurnal RechtsVinding: Media Pembinaan Hukum Nasional* 13, no. 2 (2024): 295–313, <https://rechtsvinding.bphn.go.id/ejournal/index.php/jrv/article/view/1801>; B D Kencono, H H Putri, and T W Handoko, "Transformasi Pemerintahan Digital: Tantangan Dalam Perkembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) Di Indonesia," *JlIP: Jurnal Ilmiah Ilmu Pendidikan* 7, no. 2 (2024): 1498–1506, <https://doi.org/10.54371/jljp.v7i2.3519>; Kencono, Putri, and Handoko, "Transformasi Pemerintahan Digital: Tantangan Dalam Perkembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) Di Indonesia."

impartiality, prohibition of abuse of authority, public interest, and good service remain applicable even when administrative processes are conducted through electronic systems. Algorithms therefore cannot be treated as neutral spaces outside the law. System design, data selection, weighting, eligibility thresholds, verification mechanisms, and the manner in which officials use system outputs form a chain of actions that can determine both the content of a decision and the quality of protection afforded to citizens' rights.

The difficulty is that the prevailing administrative-law framework was largely designed on the assumption that assessment and reason-giving are performed by humans. In conventional decisions, citizens can identify the competent official, read the grounds for the decision, lodge an objection, and request correction. Algorithm-based decisions complicate this relationship. Adverse outcomes may result from outdated data, identity-matching errors, discriminatory proxy variables, non-explainable models, or the tendency of officials to accept machine recommendations without critical review. Williams warns that opacity, reliance on correlations, metric choices, and the scalability of error require more nuanced administrative-law controls over algorithmic decision-making. Responsibility may also be dispersed among the user agency, database administrator, system developer, vendor, and the official who formally signs the decision. Citizens then face three basic problems: they may not know that an algorithm was used, may not understand the reasons for the outcome, and may not know who should be held accountable.³

Existing digital regulation does not fully resolve this gap. Law Number 27 of 2022 concerning Personal Data Protection provides an important basis for data-subject rights, lawful processing, accuracy, security, and controller accountability. Data protection and the legality of administrative decisions, however, are distinct although related layers of legal concern. Correcting data does not necessarily restore a decision that has already harmed a citizen. Conversely, a formally lawful decision may remain problematic when it is produced through biased or non-auditable modelling. Data rights therefore need to be connected to the duty to give reasons, the opportunity to be heard, human review, administrative remedies, and review by the State Administrative Court.

Minister of Communication and Informatics Circular Number 9 of 2023 concerning Artificial Intelligence Ethics introduced the values of inclusiveness, humanity, security, accessibility, transparency, credibility and accountability, personal data protection, sustainability, and intellectual property. The circular also states that AI should support human activity and should not become the determinant of policy or the decision-maker in matters affecting humanity. These principles are important as ethical guidance, but they do not yet formulate procedural rights that citizens can enforce. There are still no detailed standards on when algorithmic use must be disclosed, what information must be explained, who is authorized to conduct reconsideration, how quickly objections must be decided, which technical documents must be retained, and what legal consequences follow from procedural violations.⁴

³ R Williams, "Rethinking Administrative Law for Algorithmic Decision Making," *Oxford Journal of Legal Studies* 42, no. 2 (2022): 468–494, <https://doi.org/10.1093/ojls/gqab032>.

⁴ Kementerian Komunikasi Informatika Republik Indonesia, "Surat Edaran Menteri Komunikasi Dan Informatika Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial," 2023, https://jdih.komdigi.go.id/produk_hukum/view/id/883/.

The urgency of regulation is increasing as Indonesia's national AI-governance agenda develops. In 2026, the Ministry of Communication and Digital Affairs stated that a Presidential Regulation on AI was being prepared as a foundation for national technology governance, while Digital Government was designed to consolidate cross-agency service transformation. This momentum should ensure that regulation addresses not only developers, system security, and ecosystem growth, but also constraints on the exercise of administrative power through algorithms. A framework focused solely on technological risk may overlook administrative justice, namely how citizens learn about, challenge, and obtain correction of state decisions affecting their rights or interests.⁵

Public-service oversight data show that the need for remedies is not hypothetical. The Ombudsman of the Republic of Indonesia continues to record public complaints concerning public-service delivery while service channels and systems become increasingly digital. Digitalization can broaden access to complaint mechanisms, but it can also generate new forms of maladministration, including automated rejection without adequate reasons, the absence of non-digital correction channels, responses that merely repeat system outputs, and uncertainty regarding the responsible actor. Citizens therefore require more than access to an application. They need a process through which errors can be understood, contested, and effectively corrected.⁶

Indonesian scholarship has begun to identify these problems from several perspectives. Heriansyah and Erliyana analyze the legitimacy of AI as a substitute for public officials and place ultimate responsibility on human officials through an analogy with mandates. Herawaty and Fitria examine potential legal responsibility of public officials for decisions influenced by generative-AI outputs. Al Fatihah and Utomo show that accountability problems in algorithm-based public services concern not only innovation but also transparency and the public's ability to scrutinize decisions. Yorman and Wahab develop the idea of algorithmic accountability in Indonesia's GovTech based on AUPB, including data validation, system audits, human oversight, a right to explanation, objections, data correction, and remedies. Suhardi and Wahab further propose an algorithmic rule-of-law framework for automated decision-making in local government, covering legal basis, risk classification, human oversight, understandable reasons, audit trails, administrative remedies, and external supervision. These studies show that Indonesian discourse has moved beyond the initial question of whether AI may be used in government.⁷

⁵ Kementerian Komunikasi Digital Republik Indonesia, "Sekjen Ismail: Perpres AI Fondasi Tata Kelola Teknologi Masa Depan Indonesia," 2026, <https://www.komdigi.go.id/berita/siaran-pers/detail/sekjen-ismail-perpres-ai-fondasi-tata-kelola-teknologi-masa-depan-indonesia>.

⁶ Ombudsman Republik Indonesia, "Laporan Tahunan Ombudsman Republik Indonesia Tahun 2025: Mengawasi Pelayanan Publik," 2025, https://ombudsman.go.id/produk/?c=19&s=SUB_LT_5a1ea951d55c4.

⁷ M Suhardi and A Wahab, "Algorithmic Rule of Law in Local Government: Administrative Law Challenges in Automated Public Decision-Making in Indonesia," *Journal of Governance* 11, no. 2 (2026): 327–341, <https://doi.org/10.62870/jog.v11i2.39854>; Yorman and A Wahab, "Akuntabilitas Algoritmik Dalam Penyelenggaraan Pelayanan Publik Digital Melalui GovTech Indonesia Ditinjau Dari Asas-Asas Umum Pemerintahan Yang Baik," *Jurnal Perlindungan Masyarakat: Bestuur Praesidium* 3, no. 1 (2026): 163–178, <https://ejournal.ipdn.ac.id/jpa/article/view/6428>; A Al-Fatihah and K A Utomo, "Tantangan Akuntabilitas Dalam Penggunaan Algoritma Pada Layanan Publik: Kajian Literatur Kritis Di Kalimantan Timur," *Jurnal Ilmu Hukum, Humaniora Dan Politik* 6, no. 2 (2026): 1771–1778, <https://doi.org/10.38035/jihhp.v6i2.7829>; R Herawaty and A Fitria, "Potensi Pertanggungjawaban

Nevertheless, an important analytical gap remains. Existing studies predominantly explain accountability principles, the legal position of AI, or general lists of safeguards. They do not yet systematically connect the full lifecycle of an individual decision, from establishing legal authority and risk classification, conducting impact assessment before deployment, notifying citizens, providing understandable reasons, and ensuring meaningful human review, to administrative objections, audit-trail retention, remedial standards, and review before the State Administrative Court. This gap matters because principles that are not translated into procedures, responsible officials, deadlines, mandatory evidence, and legal consequences are difficult for citizens and oversight bodies to use.

Conceptually, this study uses the term algorithm-based government decision to cover three forms of technology use. The first is a fully automated decision, in which an outcome is issued without substantive human assessment of the individual case. The second is an algorithm-assisted decision, in which an official formally decides but the system output significantly influences the result. The third is internal administrative automation that assists document management without determining rights or obligations. This distinction prevents legal duties from being imposed uniformly. The greater the system's effect on citizens' rights and the smaller the space for human evaluation, the stronger the safeguards that should be required.

In response to this gap, the study proposes the Six-Layer Administrative Due Process Model (DPA-6). The model consists of: (1) legal authority and risk classification; (2) algorithmic impact assessment before use; (3) notice of algorithmic use and identification of the responsible official; (4) a right to an understandable explanation; (5) meaningful human review and effective administrative remedies; and (6) audit trails, external oversight, evidence, and remediation. The novelty of the model does not lie in creating each principle separately, but in integrating them into Indonesia's administrative-law structure and specifying the function of each layer before, during, and after a decision is issued.

The right to explanation in this model does not require disclosure of the entire source code. An administratively relevant explanation should at least enable citizens to understand the principal data used, decisive factors, legal basis, the relationship between those factors and the outcome, and available corrective steps. Human review likewise cannot be reduced to a formal signature. The reviewer must have competence, access to relevant data and logs, sufficient time, authority to depart from or overturn the system output, and responsibility to provide fresh reasons. Without these conditions, human review becomes only symbolic legitimation of a machine-generated decision.

The DPA-6 approach also reflects proportionality. A system that merely sorts an internal queue need not bear the same obligations as a system determining eligibility for benefits, permits, sanctions, or administrative status. A risk-based model allows innovation to continue while imposing stronger protection on high-impact decisions. Regulation (EU) 2024/1689 on Artificial Intelligence and the European framework for automated decision-making are used only to understand the functions of risk classification, human oversight, documentation, and rights of affected persons. The

Hukum Pejabat Publik Atas Keputusan Yang Dipengaruhi Output Kecerdasan Buatan (AI) Generatif," *Arus Jurnal Sosial Dan Humaniora* 5, no. 3 (2025): 4603–4616, <https://doi.org/10.57250/ajsh.v5i3.1966>; Heriansyah and Erliyana, "Kecerdasan Buatan Menjadi Pemeran Pengganti Pejabat Pemerintahan."

comparison is not a mechanical legal transplant. It is used to test safeguards that may be compatible with Indonesia's Government Administration Law, Public Service Law, Personal Data Protection Law, Ombudsman framework, and State Administrative Court system.

On this basis, the study addresses two research questions. First, to what extent is Indonesia's legal framework adequate to guarantee due process when government decisions are made or significantly influenced by algorithmic systems? Second, what model of administrative due process is appropriate to guarantee the rights to explanation, human review, administrative remedies, auditability, and remediation for affected citizens? The study maps vertical, horizontal, and operational gaps in the prevailing framework and formulates the DPA-6 Model together with compliance indicators, allocation of responsibility, and legal consequences of non-compliance. Theoretically, the study extends administrative due process to the human-data-algorithm chain. Practically, it is intended to provide a reference for policymakers, agencies using algorithmic systems, the Ombudsman, and administrative courts.

RESEARCH METHOD

This study is prescriptive normative legal research, or doctrinal legal research. This design follows from the study's purpose of assessing the adequacy of prevailing norms and formulating the legal model that should govern algorithm-based government decisions. The unit of analysis is not public acceptance of an application or the technical performance of a model, but norms of authority, decision-making procedures, citizens' rights, forms of accountability, and mechanisms of oversight and remediation. Institutional empirical data contained in policy documents and Ombudsman reports are used as contextual evidence rather than as a basis for measuring relationships among variables.

The study applies four complementary approaches. The statutory approach examines the relationship among the Government Administration Law, Public Service Law, Personal Data Protection Law, Electronic Information and Transactions Law, the SPBE Presidential Regulation, the National SPBE Architecture, the regulation accelerating digital transformation, and AI ethics policy. The conceptual approach constructs the concepts of algorithm-based decisions, procedural due process, meaningful human review, explainability, algorithmic accountability, and administrative justice. The case approach considers administrative-court decisions relating to electronic decisions, the duty to give reasons, procedural defects, AUPB, administrative remedies, and evidence. A functional comparative approach examines safeguards under the European Union AI Act and automated decision-making regime insofar as they address comparable problems in Indonesia.

Indonesian primary legal materials include Law Number 30 of 2014, Law Number 25 of 2009, Law Number 27 of 2022, the Electronic Information and Transactions Law and its amendments, Presidential Regulation Number 95 of 2018, Presidential Regulation Number 132 of 2022, Presidential Regulation Number 82 of 2023, Minister of Communication and Informatics Circular Number 9 of 2023, and official drafts and documents concerning Digital Government and AI governance. Primary materials also include relevant decisions of the State Administrative Courts and the Supreme Court. The principal comparative material is Regulation (EU) 2024/1689. Secondary legal materials consist of Indonesian and international journal articles addressing AI in public administration, AUPB, algorithmic accountability, the right to explanation, human oversight, and administrative remedies.

Materials were collected through a structured document study covering a principal publication period from January 2014 to August 2026. The year 2014 was selected because the Government Administration Law entered into force as an umbrella act for government decisions and actions, while August 2026 captures recent developments in the Digital Government proposal and AI policy. Pre-2014 sources are used only where necessary to explain foundational doctrines not displaced by more recent literature. Regulations were obtained from official legal-documentation networks or the BPK Regulation Database, judicial decisions from the Supreme Court Decision Directory, oversight documents from the Ombudsman, and literature from publisher journal portals, DOI records, or institutional repositories allowing full-text verification.

The search strategy used combinations of Indonesian and English keywords, including 'electronic decision', 'automated decision', 'algorithm-based decision', 'AI in government', 'artificial intelligence public officials', 'digital AUPB', 'algorithmic accountability', 'right to explanation', 'human review', 'administrative remedy', 'automated administrative decision', 'algorithmic decision-making', 'meaningful human review', and 'administrative remedy'. These keywords were combined with sectoral terms such as public services, social assistance, licensing, identity verification, and local government. The search process was recorded in a source register containing document identity, issuing authority, date, legal status, link, access date, relevant section, and analytical function.

Materials were purposively selected according to doctrinal relevance. A source was included where it had verifiable legal or academic authority, addressed government decisions or actions, algorithmic use in the public sector, procedural rights, data protection, or control mechanisms, was available in full text, and provided a testable concept, norm, finding, or argument. Sources were excluded where they consisted only of unsupported popular opinion, duplicates, unverifiable material, purely technical efficiency discussions without administrative implications, or metaphorical uses of the term AI. Additional materials were no longer added once each analytical dimension had sufficient primary and secondary grounding and no substantively new legal category emerged.

Selected materials were coded using the DPA-6 matrix. The first dimension, legality and risk classification, tests legal authority, decision type, level of impact, and limits of automation. The second, pre-decision obligations, examines impact assessment, data quality, bias testing, security, procurement, and system validation. The third, notice and explanation, assesses the information given to citizens and the adequacy of reasons. The fourth, human review, examines competence, information access, independence, authority to alter outcomes, and reviewer responsibility. The fifth, administrative remedies, examines channels, deadlines, accessibility, standards of review, and effectiveness of correction. The sixth, audit and adjudication, examines audit trails, external oversight, burden of proof, court access, and forms of remediation.

The analysis proceeded in five stages. First, legal materials were inventoried and their status validated to confirm hierarchy, amendment, and continuing force. Second, grammatical, systematic, and teleological interpretation was applied to norms governing authority, AUPB, electronic decisions, data protection, reasons for decisions, and administrative remedies. Historical interpretation was used only where needed to understand legislative purpose. Third, gap analysis identified legal vacuums,

ambiguity, normative conflict, and the absence of operational procedures. Fourth, functional comparison assessed how comparator jurisdictions address similar problems without disregarding differences in legal systems and institutional capacity. Fifth, the DPA-6 Model was constructed prescriptively, including compliance indicators and legal consequences of violation.

Table 1 functions as an analytical audit instrument so that each normative conclusion can be traced to its question and sources. The matrix is not used to produce a quantitative score. Its function is to maintain consistency across documents and prevent the study from stopping at a mere inventory of regulations. Each cell records the relevant norm or argument, source, type of gap, and prescriptive implication. Where one source supports more than one dimension, it is recorded in each relevant dimension with a different explanation of its function.

Table 1. Six-Layer Administrative Due Process (DPA-6) Analytical Matrix

Dimension	Test Question	Analytical Output
1	Does the use of the algorithm have a clear legal basis, functional limits, and risk classification?	Legality test and limits of automation.
2	Does the agency assess impact, data quality, bias, security, and system validity before use?	Ex ante obligations and prerequisites for use.
3	Are citizens informed about system use and provided with understandable reasons?	Notification standard and minimum content of explanation.
4	Is the human reviewer competent, adequately informed and resourced, and authorized to change the outcome?	Test of meaningful human review.
5	Are objections or appeals accessible, timely, independent, and capable of restoring rights?	Design of effective administrative remedies.
6	Are logs available, auditable, subject to oversight, and usable for evidence and remediation?	Standards for audit trails, adjudication, and remediation.

The validity of the argument is maintained through triangulation of legal sources. No proposition is drawn solely from secondary literature. It is tested against regulations, official policy documents, judicial decisions, and relevant scholarship. Comparative analysis is not used as the sole basis for recommendations. Each safeguard is tested for coherence with the allocation of authority, AUPB, objection procedures, the Ombudsman, and the jurisdiction of Indonesia's State Administrative Courts. An audit trail of the analysis is maintained through the source register and coding matrix so that readers can examine the relationship among materials, interpretation, gaps, and recommendations.

The study establishes three limitations. First, the object is limited to individual administrative decisions producing legal consequences or significant effects on citizens. AI used for internal functions that do not affect individual outcomes is discussed only as a comparator. Second, the study does not evaluate the technical accuracy of a particular model because code, training data, and procurement documentation may not be publicly available. Third, where no Indonesian judgment

explicitly reviewing an algorithmic decision is found, analogous judgments are used only to explain doctrines concerning reasons, procedure, AUPB, and evidence, with the limits of analogy expressly acknowledged. These limitations prevent the recommendations from claiming evidence of practices that has not been established.

The analysis produces two outputs. The first is a map of legal adequacy distinguishing principles that are already available, norms that remain ambiguous, and procedures that have not yet been regulated. The second is the DPA-6 Model, identifying responsible actors, timing of obligations, information or documents that must be available, citizens' rights, oversight channels, and consequences of non-compliance. The model is then assessed against legality, rights protection, administrative effectiveness, risk proportionality, and feasibility within Indonesia's Digital Government governance framework.

RESULTS AND DISCUSSION

Normative mapping of 54 DPA-6 indicators shows that Indonesian law is not devoid of legal foundations, but protection remains fragmented and does not yet constitute an integrated cycle of algorithmic due process. Of the 54 indicators, 19 indicators (35.2%) were coded as available, 24 (44.4%) as ambiguous, and 11 (20.4%) as not yet regulated. These percentages describe only the distribution of normative coding and are not intended as a score of legal quality. The principal finding lies in the pattern across dimensions. Foundations for legality, data protection, administrative remedies, audit, and adjudication are present, but the relationships among system design, issuance of decisions, human review, objections, evidence, and remediation have not yet been organized into obligations traceable throughout the decision lifecycle.

Table 2. Map of the Adequacy of Indonesian Law Based on DPA-6 Dimensions

Dimension	Indicator Distribution	Dominant Status	Main Gap
D1 Legality & Risk Classification	Total: 7 Available: 2 Ambiguous: 3 Not regulated: 2	Ambiguous	Decision types, risk, limits of automation, and responsibility chains are not integrated.
D2 Pre-Decision Obligations	Total: 11 Available: 4 Ambiguous: 5 Not regulated: 2	Ambiguous	Data governance is more developed than bias testing, model validation, versioning, vendor audit, and AIA.
D3 Notice & Explanation	Total: 9 Available: 4 Ambiguous: 5 Not regulated: 0	Ambiguous	Reasons and data rights exist, but notice of algorithmic use and minimum explanatory content are not detailed.
D4 Human Review	Total: 8 Available: 0 Ambiguous: 3 Not regulated: 5	Not regulated	Competence, log access, independence, review time, override authority, and automation-bias safeguards remain unclear.
D5 Administrative Remedies	Total: 9 Available: 4 Ambiguous: 4 Not regulated: 1	Available*	General remedies exist but are not fully connected to objections to automated decisions and algorithmic scope of review.

Dimension	Indicator Distribution	Dominant Status	Main Gap
D6 Audit & Adjudication	Total: 10 Available: 5 Ambiguous: 4 Not regulated: 1	Available	Audit, Ombudsman, administrative courts, and electronic evidence exist, but decision-level audit trails and disclosure remain partial.
TOTAL	Total: 54 Available: 19 Ambiguous: 24 Not regulated: 11	Ambiguous	An integrated algorithmic due-process lifecycle has not yet been established.

*Note: *D5 contains an equal number of available and ambiguous indicators. It is classified as “available” because the general legal framework for administrative remedies is already established, although algorithm-specific procedures remain only partially regulated.*

Decision Legality Must Shift from the Official to the Human-Data-Algorithm Chain

The first dimension shows that Indonesia's foundation of administrative legality is relatively strong, but it is not sufficiently specific to distinguish the role of technology in individual decisions. Article 9 of Law Number 30 of 2014 requires every decision and action to have a basis of authority and to comply with legislation and AUPB. Article 10 places legal certainty, utility, impartiality, due care, prohibition of abuse of authority, transparency, public interest, and good service as standards of control. Article 52 also links the validity of decisions to authority, procedure, and substance. Under this construction, algorithmic use cannot create new authority. Authority must remain traceable to the body or official legally possessing attribution, delegation, or mandate.

The problem is that this framework does not yet provide a legal classification distinguishing fully automated decisions, decisions formally signed by humans but substantively dependent on algorithmic outputs, and internal administrative automation that does not determine citizens' rights or obligations. This is not merely terminological because the distinction determines the intensity of safeguards. Supreme Court Circular Number 1 of 2022 concerning OSS-based licensing illustrates an analogous principle: a digital platform does not replace the substantive source of authority. The same principle should prevent agencies from shifting responsibility to systems, vendors, or data managers when algorithmic output materially contributes to the reasons for a decision.

The judgment of the Court of Justice of the European Union in Case C-634/21 SCHUFA Holding provides a useful functional comparator. The Court held that the generation of a probability score may constitute automated individual decision-making where the score plays a determining role in a third party's decision that significantly affects an individual. This rule is not binding in Indonesia, but it demonstrates that legal control should not be triggered only by full automation. Where an algorithmic recommendation, score, or classification practically determines the outcome, it should be treated as significant algorithm-assisted decision-making and brought within a due-process framework.⁸

⁸ Court of Justice of the European Union, “Judgment in Case C-634/21, OQ v Land Hessen (SCHUFA Holding (Scoring),” 2025, ecli:EU:C:2023:957.

DPA-6 therefore proposes two additional duties at the first layer. Before deployment, an agency should classify system use as fully automated, significantly assisted, or internal automation. It should also classify risk according to the effect of the decision on rights and access to services, vulnerability of affected groups, reversibility of harm, and the degree of official dependence on system output. The greater the impact and the smaller the space for human evaluation, the stronger the obligations concerning impact assessment, explanation, human review, logging, and review.

Pre-Decision Obligations: DPIA Exists but Does Not Yet Constitute an Algorithmic Impact Assessment

Coding in the second dimension reveals an imbalance between data governance and model governance. Law Number 27 of 2022 provides a substantial foundation for lawful processing, transparency, accuracy, security, and data accountability. Article 16(2) establishes principles of lawful, transparent, accurate, up-to-date, secure, and accountable processing. Article 34 requires a personal data protection impact assessment for high-risk processing, including automated decision-making that has legal consequences or significant effects on data subjects. Presidential Regulation Number 39 of 2019 concerning One Data Indonesia also strengthens data standards, metadata, interoperability, and reference or master data, while Government Regulation Number 71 of 2019 and the SPBE framework provide a basis for the security and reliability of electronic systems.

These foundations are important, but a DPIA is not identical to an impact assessment of an administrative decision. A DPIA primarily addresses risks arising from personal-data processing. Algorithm-based government decisions require a broader assessment of whether the system corresponds to the legal basis of authority, whether the variables used have a lawful relationship with the purpose of the decision, whether there is a risk of discrimination or exclusion error, whether vulnerable groups are disproportionately affected, whether the outcome can be corrected, and whether remedies are available. The study therefore does not conclude that Indonesia has no impact assessment at all. The identified gap is the absence of an algorithmic or administrative impact assessment connecting data risks with decision legality and administrative justice.

The European Union provides functions that may be selectively adapted. Regulation (EU) 2024/1689 establishes lifecycle risk management for high-risk AI, regulates data governance and bias examination, logging, transparency, and human oversight, and in certain circumstances requires a fundamental-rights impact assessment before deployment by public bodies or public-service providers. DPA-6 uses these functions not as a mechanical transplant, but to demonstrate that legality review should begin before a system produces decisions.

Other significant gaps include the absence of specific obligations for pre-deployment bias testing, validation of a model or rule against legal purposes, versioning and revalidation after material changes, and minimum audit clauses where systems are supplied by third parties. Cobbe, Lee, and Singh show that reviewability requires socio-technical processes that can be reconstructed through record keeping, logging, and organizational documentation from the design stage. DPA-6 therefore requires a pre-decision evidence package including a legal-basis memorandum,

DPIA/AIA, data sheet, bias-test results, validation report, security records, vendor audit-access clauses, and system version and change logs.⁹

Two indicators that initially lacked explicit coding relationships can be anchored only partially in available primary and comparative sources. For D2.8, Government Regulation Number 71 of 2019 requires electronic systems to be reliable and secure and recognizes audits or conformity testing of reliability. Article 15 of the AI Act, as a comparator, requires appropriate levels of accuracy, robustness, and cybersecurity throughout the lifecycle. These sources support technical validation but do not yet establish an Indonesian duty to test whether a model or rule corresponds to the legal purpose and fairness of an administrative decision. For D2.11, Articles 25 and 26 of the Personal Data Protection Law regulate special processing of children's and persons with disabilities' data, while Article 5(1)(b) of the AI Act prohibits exploitation of vulnerabilities associated with age, disability, or socio-economic circumstances. These provisions show partial protection for vulnerable groups but do not yet constitute a cross-sector safeguard specifically governing algorithmic decision systems.

Notice and Explanation: Reasons for a Decision Are Not the Same as an Algorithmic Explanation

The third dimension does not reveal a complete legal vacuum. Article 55 of the Government Administration Law already requires a decision to contain the reasons forming the basis of consideration. The Personal Data Protection Law also provides rights to information regarding the identity and basis of processing, access to data, and correction of inaccurate data. Two important components of due process, reason-giving and informational control, are therefore already present.

Conventional administrative reasons, however, do not automatically answer the questions arising when an algorithm influences the result. Citizens need to know whether a system was used, the role of the system in the decision, the principal relevant data, decisive factors, how those factors relate to the outcome, the identity of the responsible official, and available corrective steps. Such an explanation does not require disclosure of all source code or trade secrets. Its focus is contestability. Minimum information must be sufficient for a citizen to identify possible data errors, misclassification, irrelevant variables, or excessive official dependence on the system output.

Wachter, Mittelstadt, and Floridi caution against reading the GDPR as a simple source of a general right to an explanation for every automated decision. Distinguishing information rights, safeguards, and explanations is necessary to avoid overclaiming. DPA-6 therefore uses a layered-explanation concept. The first layer is notice that an algorithm is used or significantly influences the decision. The second consists of administrative reasons explaining the legal basis and considerations. The third contains case-relevant algorithmic information, including principal data or data categories, decisive factors, the system's role, and the relationship between factors and

⁹ J Cobbe, M S A Lee, and J Singh, "Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21)* (Association for Computing Machinery, 2021), 598–609, <https://doi.org/10.1145/3442188.3445921>.

outcome. The fourth explains the objection route, deadlines, evidence that may be submitted, and the official or unit that may be contacted.¹⁰

Article 86 of the AI Act provides a comparator under which persons affected by certain decisions based on outputs of high-risk AI systems may obtain a clear and meaningful explanation of the system's role and the main elements of the decision. This is not Indonesian law, but its procedural function is compatible with the existing national duties to give reasons and allow correction. The required reconstruction is to operationalize those foundations into an explanation that can actually be used for correction and objection.

Indicator D3.7 likewise has only a partial legal basis. Articles 75 to 78 of the Government Administration Law provide objections, appeals, and filing and resolution deadlines. They do not require information on objection routes, deadlines, admissible evidence, and a responsible contact point to be delivered as one package when an algorithmic decision is notified. As an operational comparator, the Article 29 Data Protection Working Party recommends an accessible mechanism for human intervention, including a link to an appeal process when an automated decision is communicated, together with agreed timescales and a named contact point. D3.7 therefore remains appropriately classified as ambiguous rather than fully available.¹¹

Meaningful Human Review as the Largest Gap

Human review is the weakest dimension in the mapping. Of the eight D4 indicators, none is categorized as fully available. Three remain ambiguous and five are not specifically regulated. Indonesian law can attach responsibility to the competent official, and Minister of Communication and Informatics Circular Number 9 of 2023 positions AI as a support for human activity. Yet the presence of a human within an organizational chart does not establish that review of algorithmic output is substantively meaningful.

Meaningful human review requires at least five capacities. A reviewer must understand the system's functions and limitations, have access to relevant data, logs, and model or rule versions, possess sufficient time and independence, have authority to reject, alter, or suspend an output, and be required to provide fresh reasons after review. Without these elements, a human-in-the-loop arrangement can become mere rubber-stamping. Williams emphasizes that opacity, correlation, metric choices, and scalable errors require administrative controls more detailed than formal procedural involvement.¹²

Article 14 of the AI Act and the Article 29 Working Party guidance on automated decision-making provide comparative standards for effective and competent human oversight capable of understanding and intervening in system outputs. The guidance also stresses that human involvement is not meaningful where the reviewer lacks genuine authority or routinely accepts system recommendations. DPA-6 therefore

¹⁰ S Wachter, B Mittelstadt, and L Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law* 7, no. 2 (2017): 76–99, <https://doi.org/10.1093/idpl/ixp005>.

¹¹ "Article 29 Data Protection Working Party. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)," 2018.

¹² Williams, "Rethinking Administrative Law for Algorithmic Decision Making."

treats human review as an independent layer rather than an additional phrase in the decision.¹³

The prescriptive consequence is that agencies need a clearly defined reviewer role, competence standards, conflict-of-interest declarations, minimum access to the decision record, and a documented override mechanism. High-impact decisions should not be finalized before the reviewer completes substantive examination. At the objection stage, the review should be conducted afresh with the ability to correct both data and outcomes, rather than merely verifying that the system operated according to its technical configuration.

The normative basis for D4.4 and D4.5 is also limited. The principle of impartiality in Article 10(1)(c) of the Government Administration Law provides a general basis for review to remain free from irrelevant interests, but it does not regulate separation of duties, conflict declarations, or special independence for algorithmic reviewers. The Article 29 Working Party guidance requires meaningful involvement by a person with the authority and competence to change a decision and a thorough assessment of all relevant data. It also provides examples of agreed timescales for review. Indonesian law, however, has not been identified as establishing minimum time or adequate time capacity for substantive algorithmic review. D4.4 and D4.5 therefore remain categorized as not specifically regulated, with these sources serving only as analogical and prescriptive comparators.

Administrative Remedies Must Connect Personal Data Rights with Decision Correction

Unlike human review, administrative remedies have a comparatively stronger legal foundation. Article 75 of the Government Administration Law gives adversely affected citizens the right to pursue administrative remedies through objections and appeals, while Articles 76 to 78 regulate the process and deadlines. Supreme Court Regulation Number 6 of 2018 and the Administrative Chamber formulations clarify the relationship between administrative remedies and access to administrative courts. The Public Service Law also provides complaint channels, while Article 10 of the Personal Data Protection Law adds a particularly relevant right: data subjects may object to decisions based solely on automated processing, including profiling, where those decisions have legal consequences or significant effects.

The principal weakness lies in the relationship among legal regimes. An objection under the Personal Data Protection Law centers on the rights of the data subject, whereas an administrative remedy under the Government Administration Law is directed toward correcting a government decision or action. If the two operate separately, a citizen may obtain data correction without restoration of the decision, or a decision may be reviewed without access to the data and logs explaining why the outcome occurred. DPA-6 proposes procedural integration. A single objection to an algorithmic decision should be capable of examining the legality of data processing, the data used, the version of the rule or model, the way the output was used by the official, the reasons for the decision, and the need for human review.

The Pangkal Pinang State Administrative Court Decision Number 4/PLW/2019/PTUN-PGP and Semarang State Administrative Court Decision Number 2/G/2019/PTUN.SMG are used analogically to emphasize sequencing between

¹³ "Article 29 Data Protection Working Party. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01)."

administrative remedies and access to the State Administrative Court. The analogy is limited because neither case concerns algorithms. Their doctrinal value lies in the need for a clear remedy chain. Chamber formulations concerning incorrect filing routes and deadlines likewise show that digital design should not create new procedural traps for citizens.

An effective remedy must extend beyond an administrative response that simply repeats the system output. Depending on the defect, review may result in data correction, a new decision supported by fresh reasons, annulment or revocation, temporary suspension to prevent irreparable harm, or correction of the use of a model or rule. Assisted and non-digital channels remain necessary for vulnerable groups so that digitalization does not transform access to administrative remedies into a new barrier.

The Auditability-to-Remedy Chain: From Technical Logs to Testable Evidence

The sixth dimension shows a more developed foundation for audit and adjudication, but it is not yet fully directed toward reconstructing individual decisions. The Electronic Information and Transactions Law and Government Regulation Number 71 of 2019 recognize and regulate electronic information and documents and system reliability. The SPBE Presidential Regulation provides for information-technology audits, the Public Service Law regulates internal and external oversight, the Ombudsman Law authorizes maladministration examinations, and administrative law provides access to the State Administrative Court after relevant procedures have been pursued. These foundations permit oversight, but a general system audit is not the same as a decision-level audit trail.

To test an algorithmic decision, logs should reconstruct at least the inputs used, processing time, system or rule version, output, human intervention, changes or overrides, and the identity of the responsible unit. Log retention should correspond to the time limits for objections, Ombudsman examinations, and litigation. Cobbe et al. describe reviewability as the need to create record keeping that enables a socio-technical process to be reviewed comprehensively rather than merely explaining a model at a single point.¹⁴

A more difficult gap concerns disclosure and the burden of proof where technical documents are controlled entirely by an agency or vendor. Without proportionate access to the decision record, objection rights and access to the State Administrative Court may be formally available but ineffective. DPA-6 therefore connects logging with disclosure. Mandatory evidence must be retained and capable of being requested by internal reviewers, the Ombudsman, or courts within their respective authority. The absence of evidence caused by the agency's own failure should produce proportionate procedural consequences. The study does not assume that all logs must be publicly disclosed. Security, confidentiality, and intellectual-property protection may still be maintained through layered access.

Remediation must also move from the individual to the systemic level. Supreme Court Decision Number 455 K/TUN/2021 is used analogically to show that AUPB and service quality remain relevant to reviewing the legality of decisions, while Bandung State Administrative Court Decision Number 133/G/2020/PTUN.BDG illustrates variation in administrative remedies. In an algorithmic context, where an audit

¹⁴ Cobbe, Lee, and Singh, "Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems."

identifies a recurring error pattern, remediation should not stop with a single decision. Agencies should undertake incident response, revalidation, correction of data or models, and review of the affected group of decisions.

Functional Comparison: European Union Safeguards as a Testing Tool, Not a Transplantation Model

Comparison with the European Union shows functional similarities between safeguards developed there and Indonesian legal principles, although their normative structures differ. GDPR Article 22 focuses on decisions based solely on automated processing that produce legal effects or similarly significant impacts, while the AI Act establishes lifecycle, risk-based obligations for systems. Indonesian law, by contrast, places the Government Administration Law at the center of decision legality, the Personal Data Protection Law at the center of data-processing protection, and distributes public-service, electronic-system, Ombudsman, and State Administrative Court mechanisms across separate regimes.

The relevant comparative function is therefore not to copy European categories or terminology, but to test whether Indonesia has functional equivalents for risk classification, impact assessment, data governance, logging, notice, explanation, human oversight, and remedies. The mapping shows that some equivalents already exist, including legality, AUPB, DPIA, data access and correction rights, administrative remedies, audit, and adjudication, but their operational relationships remain undefined. The CJEU's SCHUFA judgment further supports the proposition that legal categories should consider the factual influence of algorithmic output, not merely the identity of the person formally signing the decision.

This functional approach preserves two objectives. Low-risk digital functions are not burdened by disproportionate duties, while high-impact decisions cannot avoid safeguards merely by claiming that the system only provides a recommendation. Where a recommendation practically determines the outcome, due process should follow its substantive influence.

Prescriptive Reconstruction of the DPA-6 Model

Based on the adequacy map, gap analysis, analogous decisions, and functional comparison, DPA-6 is formulated as a six-layer cycle. The model's novelty lies in integrating safeguards that were previously dispersed and specifying who is responsible, when duties arise, which documents must be available, which rights citizens may exercise, and what forms of oversight and remediation apply. The model is prescriptive. The following table does not claim that every proposed obligation already exists as positive law.

Table 3. Reconstruction of the Six-Layer Administrative Due Process Model (DPA-6)

Layer	Core Obligation	Actor & Timing	Minimum Documents/Evidence	Citizen Rights & Remedial Direction
D1 Legality & Risk	Legal basis, function and risk classification, limits of automation, responsibility map.	Agency holding authority and decision official, before use and when risk changes.	Legal-basis memorandum, risk classification, responsibility map, automation limits.	Know the legal basis and responsible actor. Defects of authority or procedure may trigger correction or annulment.
D2 Pre-Decision	DPIA/AIA, data quality, bias testing, validation, security, vendor audit, versioning/revalidation.	Deployer, data controller, system owner, vendor, before deployment and after material changes.	DPIA/AIA, data sheet, bias test, validation report, security test, audit clause, change log.	Accurate data and lawful processing. Risky deployment may be suspended until correction or validation is completed.
D3 Notice & Explanation	Notice of algorithmic use, reasons, principal factors/data, responsible actor, objection route.	Issuing official, service unit, data controller, at or before notification of the decision.	Algorithm-use notice, decision reasons, explanation record, remedy notice.	Notice, understandable reasons, data access/correction. Decisions should be reviewed where they are not contestable.
D4 Human Review	Competent reviewer, data/log access, independence, sufficient time, override authority, fresh reasons.	Authorized human reviewer, before finalization of high-impact decisions and during review.	Review checklist, data/log/model version, conflict declaration, override/review record.	Genuine human examination. Rubber-stamping requires renewed substantive review.
D5 Administrative Remedy	Integrated objection/appeal, review of data-log-model, routing, suspension, integrated remedy.	Official/superior, complaint unit, data controller, after the decision within legal time limits.	Objection file, data/log/model snapshot, routing record, review record, remedy decision.	Objection, data correction, human review, suspension, new decision or annulment. Procedural traps must not eliminate rights.
D6 Audit & Adjudication	Decision-level audit trail, retention, audit, disclosure, Ombudsman/court review, individual and systemic remediation.	Log manager, internal auditor, Ombudsman, litigation official, throughout the lifecycle and during disputes/incidents.	Audit trail, retention policy, audit report, evidence package, incident/remediation record.	Access to evidence and oversight. Failure to preserve evidence should trigger proportionate procedural consequences and remediation.

Temporally, the six layers form three zones of protection. D1 and D2 operate before an individual decision is issued. D3 and D4 operate when the system influences

or generates the decision. D5 and D6 operate after a citizen is affected or when a pattern of failure is identified. This division is important because due process should not emerge only after a dispute. Many algorithmic errors are systemic and can be replicated at scale, making prevention through legal basis, impact assessment, validation, and logging as important as objections and annulment.

DPA-6 also distinguishes minimum standards from standards that increase with risk. For internal automation that does not affect individual rights, obligations may focus on security, accuracy, and audit. Significant algorithm-assisted decisions require additional notice, explanation, human review, and audit trails. High-impact or fully automated decisions require the strongest ex ante duties, human review, access to remedies, and evidence retention. This proportionality allows innovation to continue without sacrificing citizens' rights.

From the perspective of legal consequences, DPA-6 does not independently create new sanctions. It connects violations with consequences already recognized in administrative law and related regimes, including defects of authority, procedure, or substance, correction or annulment of decisions, data correction, suspension or restriction of processing, Ombudsman examination, and review before the State Administrative Court. New duties such as bias testing, override authority, or decision-level logging require further normative regulation before the consequences of violation can be applied consistently.

The evidentiary strength of the mapping must be read with one triangulation limitation. The initial worksheet audit showed that 49 of 54 indicators had source-coding relationships, while five indicators, D2.8, D2.11, D3.7, D4.4, and D4.5, lacked explicit relationships in the coding register. In addition, only 15 indicators were categorized as ready for results and discussion in the triangulation audit, while 39 still required stronger sourcing. Re-examination of available sources enabled those five indicators to receive limited normative or comparative anchors as described above, but this did not transform them into complete legal norms or remove the need for further triangulation. The distribution of 19 available, 24 ambiguous, and 11 unregulated indicators is therefore treated as normative coding, not as a quantitative measure of evidentiary strength or Indonesian legal compliance.

CONCLUSION

This study shows that Indonesia's legal framework contains important foundations for controlling algorithm-based government decisions, but it has not yet formed an integrated due-process framework throughout the decision lifecycle. Of 54 DPA-6 indicators, 19 were categorized as available, 24 as ambiguous, and 11 as not yet regulated. This does not mean that 35.2% of Indonesian law is quantitatively 'adequate'. It indicates the distribution of normative positions. The clearest foundations concern decision legality, AUPB, data protection, correction and access rights, administrative remedies, system audits, the Ombudsman, electronic evidence, and adjudication. The largest gaps concern meaningful human review, classification of algorithmic decision types and risks, algorithmic impact assessment, bias testing, versioning, explanations capable of supporting contestation, and decision-level audit trails.

The first research question is therefore answered by finding that Indonesian law provides a sufficient starting point but remains insufficient to guarantee due process where individual outcomes are produced or heavily influenced by algorithms. The principal problem is not the total absence of norms but vertical, horizontal, and

operational fragmentation. The Government Administration Law, Personal Data Protection Law, electronic-system regime, public-service regime, SPBE, Ombudsman framework, and State Administrative Courts operate on different objects and stages, while an algorithmic decision is a socio-technical process crossing all of them.

The second research question is answered through the DPA-6 Model: (1) legality and risk classification, (2) pre-decision obligations, (3) notice and explanation, (4) meaningful human review, (5) effective administrative remedies, and (6) audit, adjudication, and remediation. The model places citizens' rights, official responsibility, mandatory documents, timing of compliance, oversight, and remediation within a single traceable chain. A right to explanation is not equivalent to disclosure of source code, and human review is not equivalent to a formal signature. Both must be designed to enable substantive correction.

At the policy level, reconstruction can proceed incrementally. Existing norms should be operationalized through guidance on algorithmic decisions. Emerging AI-governance and Digital Government frameworks should incorporate administrative decision and risk categories. Agencies using high-impact systems should be required to prepare impact assessments and decision records. Objection procedures should integrate rights under the Personal Data Protection Law with administrative remedies under the Government Administration Law. SPBE audits should be extended so that they can reconstruct individual decisions. Future research should test DPA-6 in concrete sectors such as social assistance, licensing, identity verification, taxation, education, and local government, and examine how the State Administrative Courts and Ombudsman handle algorithmic evidence as such disputes begin to arise.

REFERENCE

- Al-Fatihah, A, and K A Utomo. "Tantangan Akuntabilitas Dalam Penggunaan Algoritma Pada Layanan Publik: Kajian Literatur Kritis Di Kalimantan Timur." *Jurnal Ilmu Hukum, Humaniora Dan Politik* 6, no. 2 (2026): 1771–1778. <https://doi.org/10.38035/jihhp.v6i2.7829>.
- Article 29 Data Protection Working Party. Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (WP251rev.01), 2018.
- Cobbe, J, M S A Lee, and J Singh. "Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems." In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21)*, 598–609. Association for Computing Machinery, 2021. <https://doi.org/10.1145/3442188.3445921>.
- Court of Justice of the European Union. "Judgment in Case C-634/21, OQ v Land Hessen (SCHUFA Holding (Scoring)," 2025. ecli:EU:C:2023:957.
- Herawaty, R, and A Fitria. "Potensi Pertanggungjawaban Hukum Pejabat Publik Atas Keputusan Yang Dipengaruhi Output Kecerdasan Buatan (AI) Generatif." *Arus Jurnal Sosial Dan Humaniora* 5, no. 3 (2025): 4603–4616. <https://doi.org/10.57250/ajsh.v5i3.1966>.
- Heriansyah, F, and A Erliyana. "Kecerdasan Buatan Menjadi Pemeran Pengganti Pejabat Pemerintahan." *Jurnal RechtsVinding: Media Pembinaan Hukum Nasional* 13, no. 2 (2024): 295–313. <https://rechtsvinding.bphn.go.id/ejournal/index.php/jrv/article/view/1801>.
- Kementerian Komunikasi Digital Republik Indonesia. "Sekjen Ismail: Perpres AI Fondasi Tata Kelola Teknologi Masa Depan Indonesia," 2026.

- <https://www.komdigi.go.id/berita/siaran-pers/detail/sekjen-ismail-perpres-ai-fondasi-tata-kelola-teknologi-masa-depan-indonesia>.
- Kementerian Komunikasi Informatika Republik Indonesia. "Surat Edaran Menteri Komunikasi Dan Informatika Nomor 9 Tahun 2023 Tentang Etika Kecerdasan Artifisial," 2023. https://jdih.komdigi.go.id/produk_hukum/view/id/883/.
- Kementrian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia. "Partisipasi Rancangan Peraturan Presiden Tentang Pemerintah Digital," 2026. <https://jdih.menpan.go.id/rancangan-puu/partisipasi-rancangan-puu>.
- Kencono, B D, H H Putri, and T W Handoko. "Transformasi Pemerintahan Digital: Tantangan Dalam Perkembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) Di Indonesia." *JlIP: Jurnal Ilmiah Ilmu Pendidikan* 7, no. 2 (2024): 1498–1506. <https://doi.org/10.54371/jiip.v7i2.3519>.
- Ombudsman Republik Indonesia. "Laporan Tahunan Ombudsman Republik Indonesia Tahun 2025: Mengawasi Pelayanan Publik," 2025. https://ombudsman.go.id/produk/?c=19&s=SUB_LT_5a1ea951d55c4.
- Peraturan Mahkamah Agung Republik Indonesia Nomor 2 Tahun 2019 tentang Pedoman Penyelesaian Sengketa Tindakan Pemerintahan and Kewenangan Mengadili Perbuatan Melanggar Hukum oleh Badan dan/atau Pejabat Pemerintahan.
- Peraturan Mahkamah Agung Republik Indonesia Nomor 6 Tahun 2018 tentang Pedoman Penyelesaian Sengketa Administrasi Pemerintahan Setelah Menempuh Upaya Administratif.
- Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem and Transaksi Elektronik.
- Peraturan Presiden Republik Indonesia Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional.
- Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia.
- Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital and Keterpaduan Layanan Digital Nasional.
- Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
- Putusan Mahkamah Agung Republik Indonesia Nomor 455 K/TUN/2021, 30 November 2021.
- Putusan Pengadilan Tata Usaha Negara Bandung Nomor 133/G/2020/PTUN.BDG, 23 Maret 2021.
- Putusan Pengadilan Tata Usaha Negara Pangkal Pinang Nomor 4/PLW/2019/PTUN-PGP, 13 Maret 2019.
- Putusan Pengadilan Tata Usaha Negara Semarang Nomor 2/G/2019/PTUN.SMG, 14 Maret 2019.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
- Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

- Surat Edaran Mahkamah Agung Republik Indonesia Nomor 1 Tahun 2022 tentang Pemberlakuan Rumusan Hasil Rapat Pleno Kamar Mahkamah Agung Tahun 2022 sebagai Pedoman Pelaksanaan Tugas bagi Pengadilan.
- Surat Edaran Mahkamah Agung Republik Indonesia Nomor 5 Tahun 2021 tentang Pemberlakuan Rumusan Hasil Rapat Pleno Kamar Mahkamah Agung Tahun 2021 sebagai Pedoman Pelaksanaan Tugas bagi Pengadilan.
- Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi and Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
- Undang-Undang Republik Indonesia Nomor 25 Tahun 2009 tentang Pelayanan Publik.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
- Undang-Undang Republik Indonesia Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan.
- Undang-Undang Republik Indonesia Nomor 37 Tahun 2008 tentang Ombudsman Republik Indonesia.
- Suhardi, M, and A Wahab. "Algorithmic Rule of Law in Local Government: Administrative Law Challenges in Automated Public Decision-Making in Indonesia." *Journal of Governance* 11, no. 2 (2026): 327–341. <https://doi.org/10.62870/jog.v11i2.39854>.
- Wachter, S, B Mittelstadt, and L Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7, no. 2 (2017): 76–99. <https://doi.org/10.1093/idpl/ix005>.
- Williams, R. "Rethinking Administrative Law for Algorithmic Decision Making." *Oxford Journal of Legal Studies* 42, no. 2 (2022): 468–494. <https://doi.org/10.1093/ojls/gqab032>.
- Yorman, and A Wahab. "Akuntabilitas Algoritmik Dalam Penyelenggaraan Pelayanan Publik Digital Melalui GovTech Indonesia Ditinjau Dari Asas-Asas Umum Pemerintahan Yang Baik." *Jurnal Perlindungan Masyarakat: Bestuur Praesidium* 3, no. 1 (2026): 163–178. <https://ejournal.ipdn.ac.id/jpa/article/view/6428>.