IJLR: International Journal of Law Reconstruction
Volume 10, Number 1, March 2026
DOI: https://dx.doi.org/10.26242/ijlr.v10i1.

ACCOUNTABILITY OF THE DIRECTORATE GENERAL OF TAXES AS THE CONTROLLER OF PERSONAL DATA IN THE CORETAX SYSTEM ACCORDING TO CYBER LAW

Antin Okfitasari
Universitas Duta Bangsa, Surakarta, Indonesia
antin_okfitasari@udb.ac.id

Femmy Silaswaty Faried
Universitas Islam Batik, Surakarta, Indonesia
femmysilaswaty@gmail.com

Hafid Zakariya
Universitas Islam Batik, Surakarta, Indonesia
hafidzakariya@gmail.com

Abstract

This study aims to analyze the accountability of the Directorate General of Taxes as a personal data controller within the Coretax System from a cyber law perspective and to assess its compliance with personal data protection regulations in Indonesia. The study employs a normative legal research method utilizing statutory, conceptual, and analytical approaches. Legal materials were gathered through a literature review of relevant legislation, legal doctrines, and scholarly works. The findings indicate that the accountability of the Directorate General of Taxes encompasses not only compliance with obligations under personal data protection regulations but also the implementation of electronic system security principles, transparency in data management, cyber risk mitigation, and accountability mechanisms regarding data breaches or leaks. Strengthening data governance and the oversight of electronic systems is a fundamental prerequisite for ensuring the protection of taxpayers' rights in the era of digital tax administration. This study is expected to contribute to the body of knowledge regarding the modernization of tax governance within electronic systems and the protection of personal data.

Keywords: *Cyber Law; Personal Data; Tax;*

A. INTRODUCTION

Digital transformation in governance has become the mainstream of public policy in various countries. The development of information technology is no longer merely understood as an administrative tool, but rather as a new foundation for governance that influences how the state makes decisions, provides services, and enforces the law. Recent literature shows that e-government has evolved into a more complex form, namely

the use of data-based systems, process automation, and the use of algorithms in administrative decision-making. [1] This development is often referred to as *algorithmic governance* or *automated decision-making in public administration* , which marks a shift from a conventional bureaucratic model to a more integrated and technology-based digital governance model.

In the tax sector, digitalization plays a very strategic role. Taxes are the backbone of state finances and the primary instrument for realizing the state's redistributive function. Therefore, efficiency, accuracy, and legitimacy in tax administration are crucial issues. Research by Linda Santioso and Andreas B. Daryatno [2] shows that modernization of tax administration and digitalization contribute positively to increased taxpayer compliance. Digital systems facilitate tax reporting and payment, thus encouraging better compliance. Furthermore, data integration and process automation are also seen as strengthening the state's capacity to conduct tax oversight and enforcement more effectively.

Earlier empirical research on electronic public services demonstrates that performance and institutional legitimacy cannot be measured by transaction speed alone. A public-value analysis of developing-country e-government evaluates benefits from the perspective of service users and state capacity.[3] Indonesian research on digital government transformation associates sustained trust with the experience of public services.[4]

Indonesia is at the forefront of this transformation through the development and implementation of Coretax, a core electronic-based tax administration system. Coretax is designed to integrate various tax business processes, from registration and reporting to tax assessment, to monitoring and collection, within a single, centralized digital platform. Policy-wise, this step aligns with the government's bureaucratic reform and digital transformation agenda. From a governance perspective, Coretax promises efficiency, consistent regulatory implementation, and increased transparency in the relationship between tax authorities and taxpayers. The digitalization of the tax system has been ongoing since 2002, with the launch of e-SPT, the introduction of e-Registration, the implementation of e-Billing, e-Invoice, and e-Bupot, leading to the implementation of Coretax in 2025. The electronic/digitalized tax administration system is clearly regulated by law.

The constitutional justification for a digital tax system begins with the rule of law and the state’s obligation to protect individuals when it exercises compulsory public powers. Because taxpayers generally cannot opt out of

[1] H. T. Wu., "Regulation of Automated Administration via Technical Due Process in the Context of Algorithmic Black Box," *Advances in Law* 8, no. 2 (2026): 33–44,

[2] Linda Santioso and Andreas B. Daryatno., "The Effect of Digitalization of Taxation, Tax Morale and Modernization of the Administrative System on Taxpayer Compliance," *International Journal of Application on Economics and Business* 3, no. 2 (2025): 682–695.

[3] H. Deng, K. Karunasena, and W. Xu., "Evaluating the Performance of e-Government in Developing Countries: A Public Value Perspective," *Internet Research* 28, no. 1 (2018): 169–190.

[4] Sose Raeinaldo Virnandes, Jun Shen, and Elena Vlahu-Gjorgievska., "Building Public Trust through Digital Government Transformation: A Qualitative Study of Indonesian Civil Service Agency," *Procedia Computer Science* 234 (2024): 1183–1191, https://doi.org/10.1016/j.procs.2024.03.114.

legally required reporting, their position differs from that of users choosing a private online service; this makes the procedural protection of financial and identifying data a condition of legitimate tax administration. Comparative legal research on public-sector automation establishes that administrative safeguards must evolve with the technology used to exercise state authority.[5] Analysis of accountable artificial intelligence likewise emphasizes that deploying an algorithm does not eliminate the public authority's duty to answer for the decision.[6]

The philosophical relationship between efficiency and rights is particularly visible when public authorities collect information for a lawful purpose but process it through interconnected databases. Studies of privacy rights and Indonesian personal-data legislation explain why information handling must be linked to legal protection rather than treated solely as a matter of administrative speed.[7] Research on controllers' legal certainty points to the need for identifiable duties and implementing arrangements.[8] A comparative analysis of Indonesian personal-data rules and the GDPR further underlines the relevance of supervision and enforcement for the operation of formal rights.[9]

However, the digitalization of public administration cannot be understood solely as a technical process. The use of electronic systems, especially those involving automation and algorithms, carries significant legal, ethical, and governance implications, even leading to administrative decisions. Smuha, in line with his opinion, explains [10]that the application of AI and algorithms in government administration is not only related to technical efficiency, but also raises issues regarding accountability, transparency, protection of citizens' rights, and an adequate governance framework . This phenomenon raises fundamental questions about legitimacy, accountability, and protection of citizens' rights in the context of digital governance.

According to Farouq Ahmad Faleh Alazzam et al,[11] " *E-commerce trading law is now inescapably converged with digital governance, data*

[5] Rebecca Williams., "Rethinking Administrative Law for Algorithmic Decision Making," *Oxford Journal of Legal Studies* 42, no. 2 (2022): 468–494

[6] Madalina Busuioc., "Accountable Artificial Intelligence: Holding Algorithms to Account," *Public Administration Review* 81, no. 5 (2021): 825–836,

[7] Elfian Fauzy and Nabila Alif Radika Shandy., "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2022)

[8] Febrian Hilmi Firdaus., "Perlindungan dan Kepastian Hukum bagi Pengendali Data Pribadi di Masa Depan," *Masalah-Masalah Hukum* 53, no. 2 (2024): 135–144, https://doi.org/10.14710/mmh.53.2.2024.135-144.

[9] Predderics Hockop Simanjuntak., "Perlindungan Hukum terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)," *Esensi Hukum* 6, no. 2 (2024), https://doi.org/10.35586/esensihukum.v6i2.412.

[10] N. A. Smuha., "The Use of Algorithmic Systems by Public Administrations: Practices, Challenges and Governance Frameworks," in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).

[11] F. A. F. Alazzam, H. J. M. Shakhatreh, K. K. A. R. Aldroub, M. A. M. Assaf, N. M. Albalawee, and A. A. A. Almahasneh, "Mapping IS Governance and Cyber Risk in E-Commerce: A

protection, platform accountability, and risk management.", the statement shows that modern cyber law and digital law no longer only regulate electronic transactions, but also digital governance, data protection, platform accountability, and risk management. This is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions, then experienced the first amendment through Law Number 19 of 2016 concerning the first amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, and the last is the second amendment, namely in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. All of these regulations are then abbreviated as the ITE Law. The regulation of the ITE Law starts from the traffic of information and electronic transactions, electronic signatures, prohibited acts in the digital world, threats of punishment to child protection in cyberspace. Furthermore, more comprehensive regulations are regulated in Law Number 27 of 2022 concerning Personal Data Protection, abbreviated as the PDP Law.

In the context of taxation, these risks take on a more sensitive dimension. Tax administrations manage highly personal and valuable data and make decisions that directly impact taxpayers' economic well-being. Studies on data protection and information security indicate that data leaks or misuse in digital tax systems not only cause financial losses but can also undermine the legitimacy of tax institutions and public trust in the state. Furthermore, the use of automated systems in administrative decision-making also raises legal accountability issues. In classical administrative law, administrative decisions (beschikking) are understood as public legal actions taken by government officials or bodies based on statutory authority. Consequently, legal responsibility for these decisions rests principally with the state as the governing body. However, when these decisions are generated or significantly influenced by algorithm-based electronic systems, a new question arises: does this responsibility remain solely with the state, or can it be shifted to system developers, technology providers, or even simply dismissed as "technical errors."

Wu and Lin identify a regulatory gap created when the rapid introduction of AI outpaces the law. The implication for Coretax is not that every digital function is legally equivalent to an autonomous algorithm. Rather, where a computerized process affects taxpayer records, legal supervision must require comprehensible procedures, the ability to examine the grounds of a system-generated result, the capacity to correct defective processing, and responsibility attributable to the competent public institution. These linked requirements make transparency, auditability, adaptability, and ethical accountability practical safeguards against the loss of procedural protection. [12]

Bibliometric Analysis of Technical Infrastructure, Trading Law, and Risk Management," *Journal of Electronic Commerce in Organizations* (2026),

[12] Y. Wu and C. Lin., "Navigating the Labyrinth: Essential Conditions for Generative Artificial Intelligence Governance," *IT Professional*, 28, no. 2 (2026): 18–24

From the perspective of administrative law and cyber law, this opinion shows that: Formal regulations do not only contain regulations on how to use technology, but also regulations on transparency, auditability of algorithmic systems, and clear accountability mechanisms when technology causes harm to society.

Legal assessments of algorithmic transparency in Indonesian public services distinguish the government's authority to use a technical system from its obligation to give intelligible reasons for administrative acts.[13] Comparative discussion of automated administrative discretion also treats technological due process as a legal safeguard, not simply a software feature.[14] The constitutionality of AI-assisted public decision-making is therefore assessed in terms of legal authorization, due process, and officials' accountability.[15]

In the context of taxation, this principle is crucial due to the imbalance between tax authorities and taxpayers. Without adequate procedural guarantees, the use of automated systems has the potential to strengthen power asymmetries and weaken legal protection for taxpayers. In the Indonesian context, the development of Coretax as the core tax administration system places these issues in a highly strategic position. On the one hand, Coretax symbolizes modernization and the state's efforts to improve tax administration capacity. On the other hand, Coretax also carries complex legal consequences, particularly regarding the status of administrative decisions made through electronic systems, state accountability standards, and legal protection mechanisms for taxpayers. Indonesia's positive legal framework, such as the State Administration Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, and the General Provisions and Procedures Law, does provide a general basis for the administration of government and electronic systems. However, various studies indicate that these regulations still assume human decision-making and do not specifically address the complexity of *algorithmic decision-making* in the public sector.

Previous studies clarify different aspects of the problem, but each leaves a distinct question open. Septia and Supriyo examine confidentiality of regional taxpayers' data, providing a sectoral personal-data analysis rather than an assessment of Coretax as an integrated national platform.[16] Studies of automated administrative decision-making investigate officials' legal duties and the internal values of good administration, yet do not

[13] Wahab and Muhammad Suhardi., "Algorithmic Transparency in Digital Public Services: An Administrative Law Perspective," *Jurnal Kecerdasan Buatan dan Teknologi Informasi* 5, no. 1 (2026)

[14] Rommy Igirisa, Ferdinand Boba Panaha, and Yovan Iristian., "Algorithmic Transparency and Due Process in Automated Administrative Discretion: A Comparative Regulatory Analysis," *Lex Journal: Kajian Hukum dan Keadilan* 8, no. 2 (2025).

[15] Luh Putu Vera Astri Pujayanti., "Constitutionality of the Use of Artificial Intelligence in Government Administrative Decision-Making: An Analysis of the Principle of Due Process of Law in Indonesia," *International Journal of Scientific Research* (2025),

[16] Vima Septia and Agus Supriyo., "Legal Protection of Confidentiality of Personal Data for Regional Taxpayers," *Mendapo: Journal of Administrative Law* 4, no. 2 (2023): 176–195

determine the particular relationship between national tax administration and the Indonesian personal data controller.[17] The digital-justice literature assesses efficiency, transparency, and security risks in e-Court, an institutional comparison rather than research on the tax authority's data-processing responsibilities.[18] Research on judicial consistency and the principle of legality provides a related rule-of-law perspective, although its findings on criminal adjudication cannot be directly transferred to tax information processing.[19]

Empirical syntheses of e-government adoption establish links between security, perceived risk, and trust, while legal studies of digital public services examine transparency and accountability at the institutional level.[20] The latter work identifies the limits of merely making services accessible when citizens cannot understand or challenge opaque outcomes.[21] A study of Indonesian e-government trust also confirms that privacy and security are factors affecting confidence in public digital services. These contributions inform the analysis but do not replace the normative question at its center: how the DGT's obligations under tax administration, electronic-systems law, and personal-data law operate together in Coretax.

However, studies specifically linking these issues to the context of tax administrative decisions and legal accountability to the Directorate General of Taxes (DGT), particularly within the framework of systems such as Coretax in Indonesia, are still relatively limited. Therefore, research on the DGT's accountability for electronic system-based tax administrative decisions (Coretax) from a cyber law perspective is highly relevant and offers significant novelty. This research not only contributes to the development of administrative law and cyber law theory in the digital era but also has practical implications for policy formulation, regulatory refinement, and strengthening legal protection for taxpayers. By positioning the government, in this case the DGT, as the party that continues to bear primary responsibility for the use of electronic systems in tax administration, this study is expected to emphasize that digital transformation must go hand in hand with strengthening accountability, transparency, and fairness within the framework of a modern rule of law. In particular, the research gap concerns the legal allocation of responsibility when errors arise from an integrated tax system: privacy scholarship addresses data-controller duties,

[17] Ulrik B. U. Roehl., "Automated Decision-Making and Good Administration: Views from Inside the Government Machinery," *Government Information Quarterly* 40, no. 4 (2023): 101864

[18] Indriana Masru'iyati Salma Izzah., "Digital Acceleration in the Justice System: Weighing Effectiveness and Challenges E-Court in Indonesia," *Journal Critical Legal System* 1, no. 1 (2026): 38–55

[19] Andhika Yuli Rimbawan., "Harmonization of Judicial Decisions: Analysis of Compliance with Jurisprudence and Application of the Principle of Legality in Special Criminal Cases," *Journal Critical Legal System* 1, no. 1 (2026): 19–37

[20] Parul Gupta et al., "Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis," *Information Systems Frontiers* 27, (2025): 1089–1105

[21] Douglas Morgan Fullin Saldanha, Cleidson Nogueira Dias, and Siegrid Guillaumon., "Transparency and Accountability in Digital Public Services: Learning from the Brazilian Cases," *Government Information Quarterly* 39, No. 2 (2022): 101680

while digital-service scholarship focuses largely on adoption and operational outcomes; neither approach by itself explains how the DGT should account for taxpayer harm caused by data handling and administrative outputs within Coretax. The present study addresses that narrower intersection without assuming that all Coretax operations constitute fully automated administrative decisions.

This study has two objectives: (1) to determine the legal position of Coretax under cyber law and digital public administration; and (2) to analyze the DGT's accountability as personal data controller for system failures, misuse, or breaches affecting taxpayers.

B. RESEARCH METHOD

This study uses normative legal research to examine the DGT's position as a personal data controller and its responsibility for Coretax-related risks. A statutory approach analyzes Law No. 27 of 2022 on Personal Data Protection, the ITE Law, the KUP Law as amended, Government Regulation No. 71 of 2019, and relevant rules on electronic tax administration. A conceptual approach examines controller accountability, electronic-system security, administrative legality, and the protection of taxpayer rights; an analytical approach relates those concepts to possible system errors and data breaches. Primary legal materials comprise legislation and relevant official instruments, supported by scholarly legal literature and government publications. Materials are collected through library research and assessed qualitatively through systematic interpretation of legal duties, institutional authority, and remedies. The analysis is prescriptive: it identifies the extent of the DGT's legal responsibility and the safeguards required under the legal framework, without treating unverified media reports as proof of a Coretax data breach.

C. RESULTS AND DISCUSSION

1. Coretax's Position in the Perspective of Cyber Law and Digital Government Administration

The digital transformation of tax administration through Coretax must be understood as part of a paradigm shift in government governance toward *digital* and *algorithmic governance* . The Coretax system represents a modernization of the national tax system. The comprehensive Coretax regulations also regulate technical and operational aspects that ensure the system's effectiveness and security. The primary foundation for CoreTax's implementation is based on the General Provisions and Tax Procedures Law (UU KUP), which has undergone several amendments to accommodate developments in information technology in tax administration. This significant change in the KUP Law provides a strong legal foundation for the digitization of tax services, including the implementation of the CoreTax system as the backbone of modern tax administration. In this context, Coretax is no longer merely a technical tool, but rather a legal-administrative infrastructure that significantly impacts how state authority is exercised

in the taxation sector.

Coretax combines reporting, identification, administrative processing, and data management within a state-operated environment; the legal inquiry must therefore distinguish the authority authorizing taxation from the rules governing digital means of exercising it. An analysis of public value from emerging digital technologies supports examining government services in terms of legally relevant benefits for users, not merely automation.[22]

The classification of Coretax as a state electronic administrative system does not automatically mean it makes final decisions without human intervention. Where software detects inconsistencies, flags risk, or generates a draft assessment, its role may nevertheless shape administrative conduct, making the source of information and the authority to approve a final act legally material. The resulting legal obligation remains with the authorized institution even when tasks are distributed among technical components or external contractors.

The implementation of the CoreTax system brings a new dimension to tax compliance in Indonesia. This digital transformation not only changes the way tax administration is conducted but also fundamentally impacts the paradigm of tax compliance. This system builds a more structured and measurable compliance framework through the integration of technology with tax law principles. CoreTax provides a real-time compliance monitoring mechanism that enables early detection of tax non-compliance. This system integrates various legal compliance parameters, including timeliness of reporting, calculation accuracy, and consistency of tax data [23]. Although the CoreTax system is considered from a cyber law perspective, systems like CoreTax must be positioned as *critical public digital infrastructure* subject to stricter legal standards regarding legality, security, accountability, and protection of citizens' rights. Cyber law not only regulates aspects of electronic transactions or cybercrime but also regulates the governance of electronic systems used by the state in carrying out government functions. Therefore, the legality of CoreTax is not only assessed from the existence of a legal basis for its formation, but also from its compliance with fundamental principles of the rule of law, such as legality, proportionality, accountability, and *due process of law* in the digital context. Algorithmic governance experts argue that the use of algorithms in the public sector has shifted the paradigm of administrative decision-making from being entirely based on human discretion to a hybrid model involving interaction between

[22] D. Valle-Cruz., "Public Value of e-Government Services through Emerging Technologies," *International Journal of Public Sector Management* 32, no. 5 (2019): 530–545, https://doi.org/10.1108/IJPSM-03-2018-0072.

[23] Gevan Naufal Wala and Retha Tesalonika., "Transforming Tax Administration Through Coretax: A Legal and Accounting Analysis," *JKIS: Journal of Communication and Social Sciences*, https://dinastires.org/JKIS.

humans and machines.[24]

A distinction must also be made between Coretax availability, data accuracy, and the validity of a tax administrative decision. An outage may primarily affect access and timeliness; an erroneous data match may impair the factual basis of a notice; a data breach raises confidentiality and incident-response obligations. Research into information-system success and cybersecurity demonstrates that confidence in public systems depends on both service performance and security arrangements.[25] The legal assessment must therefore attach the applicable duty and remedy to the actual type of failure rather than apply one undifferentiated category of technological error.

For taxpayers, legal safeguards must remain accessible even when electronic systems are the principal channel for compliance. A study of e-inclusion explains why a digital-by-default public service can create barriers for some users.[26] These findings do not by themselves establish a breach of Indonesian law; they indicate why access to correction and alternative administrative assistance should be considered within procedural protection.

In this context, Coretax can be understood as a system that has the potential to *pre-process* , *filter* , and even *decision-shape* the administrative authority of tax officials. This means that although formal decisions are still made by authorized officials, the system's structure and output can significantly influence the content and direction of those decisions. From an administrative law perspective, this situation has important implications. Administrative tax decisions must still be viewed as public legal acts originating from state authority. However, when the process of their formation is heavily influenced by electronic systems, these systems must be treated as an integral part of the decision-making process subject to public law standards. In other words, Coretax should not be positioned as a technical "black box" beyond the reach of the law, but rather as an instrument of administrative power that must be subject to legality and accountability. The legal importance of intermediary trust, as studied in developing e-government systems, also supports clear institutional points of contact for taxpayers.

The legal novelty lies in treating algorithm-assisted tax administration as an interconnected sequence of legally relevant stages: collection, verification, processing, generation of administrative outputs, and review. At each stage the question is who authorizes processing, which safeguards apply, and how a taxpayer can contest a harmful or

[24] S. Grimmelikhuijsen and A. Meijer., "Legitimacy of Algorithmic Decision-Making: Six Threats and the Need for a Calibrated Institutional Response," *Perspectives on Public Management and Governance* 5, no. 3 (2022): 232–242

[25] M. S. Al-Zahrani, "Integrating IS Success Model with Cybersecurity Factors for e-Government Implementation in the Kingdom of Saudi Arabia," *International Journal of Electrical and Computer Engineering* 10, no. 5 (2020): 4937–4955.

[26] A. Al-Muwil, V. Weerakkody, R. El-Haddadeh, and Y. Dwivedi, "Balancing Digital-by-Default with Inclusion: A Study of the Factors Influencing e-Inclusion in the UK," *Information Systems Frontiers* 21 (2019): 635–659.

inaccurate result. The applicable legal test, however, follows from the functions of public authority and the duties assigned to the controller, rather than from user acceptance alone.

2. Legal accountability to the DGT for Coretax System Errors

The issue of accountability is at the heart of the discourse on the use of electronic systems in public administration. This has led researchers to question the Coretax system's data control and guarantee of taxpayers' personal data protection. The official *Instagram* page @ditjenpajakri has repeatedly posted warnings about fraudulent Coretax activations or taxpayer data synchronization with Coretax via email, *WhatsApp* , telephone, social media, and fake websites, targeting taxpayers under the guise of Directorate General of Taxes (DGT) employees. Earlier research on technology failure in the public sector cautions against mistaking service availability for organizational effectiveness.[27]

Warnings about phishing and false Coretax activation links illustrate the possibility of social-engineering attacks, but such warnings alone do not establish that Coretax's own database has been penetrated. The legal assessment must first establish whether personal data were improperly disclosed, whether the incident involved a system controlled by the DGT, and which security and notification obligations were triggered. Studies of public-sector cybersecurity and users' trust show that perceived risk may affect confidence before any particular institutional breach is proved.[28] Research on privacy, security, risk, and optimism bias likewise supports separating perceptions from demonstrable incidents.[29] This evidentiary distinction is necessary when attributing responsibility for financial or informational harm.

These fraudulent approaches demonstrate the need for public warnings and careful verification of taxpayer communications, but they do not, without technical investigation, prove a vulnerability or data leak inside Coretax. In the context of an integrated tax platform, the complexity of processing and the volume of records make documented risk assessment, access control, and incident investigation important. A confirmed breach or improper disclosure can harm individuals and may erode institutional trust. The DGT's accountability must be assessed from the source of the event, the controller's legal duties, and the proven consequences, rather than inferred solely from the existence of

[27] S. Goldfinch., "Pessimism, Computer Failure, and Information Systems Development in the Public Sector," *Public Administration Review* 67, no. 5 (2007):917–929.

[28] J. Ejdys, R. Ginevicius, Z. Rozsa, and K. Janoskova., "The Role of Perceived Risk and Security Level in Building Trust in e-Government Solutions," *E+M Ekonomie a Management* 22, no. 3 (2019):220–235

[29] W. Munyoka and M. S. Maharaj., "Privacy, Security, Trust, Risk and Optimism Bias in e-Government Use: The Case of Two Southern African Development Community Countries," *SA Journal of Information Management* 21, no. 1 (2019) :1–9

impersonation attempts.[30]

A useful legal distinction is between obligations owed before an incident and remedies due after a violation. Preventive obligations concern lawful processing, adequate security, access restrictions, accuracy, and documented oversight; responsive obligations may concern notice, correction, investigation, and access to remedies. Studies of tax-specific personal-data confidentiality show why a fiscal purpose does not negate the taxpayer's privacy interest.[31] Legal research on data controllers' legal certainty further reinforces the need to identify who bears obligations even when technical operations are delegated.[32] The existence and legal effect of a security failure should nevertheless be established in each case.

Even in the reporting of Annual Tax Returns, coretax obstacles such as Error 502, OTP problems, login failures, NIK-NPWP data desynchronization, *downtime* and server *overload* still occur, which impact the quality of service, including reliability, responsiveness, accessibility, information accuracy, satisfaction, and taxpayer compliance.[33] This risk becomes significant when system *output* is used as the basis for administrative decisions that have legal and financial consequences for citizens.[34] This condition causes anxiety and chaos for taxpayers in carrying out their tax obligations, as well as the emergence of economic losses for taxpayers due to delays in tax documents used in their business operations.

For an interruption affecting tax reporting, the legally relevant evidence includes the period of unavailability, affected transactions, published guidance, proof of attempted compliance, and available means of correction. The personal data inquiry is separate: it requires a finding about confidentiality, integrity, or inappropriate processing of taxpayer information. Research on e-tax filing in Thailand supports evaluating digital compliance through both user experience and service characteristics.[35]

Coretax, as a system that manages taxpayer data digitally, relies on technology to improve tax administration efficiency. However, as data management becomes increasingly large and complex, the potential risk

[30] R. P. Maramis., "Use of Personal Data and Customer Identity in Banking Crimes," *Lex Privatum* VII, no. 7 (2019).

[31] Vima Septia and Agus Supriyo., "Legal Protection of Confidentiality of Personal Data for Regional Taxpayers," *Mendapo: Journal of Administrative Law* 4, no. 2 (2023): 176–195

[32] Febrian Hilmi Firdaus., "Perlindungan dan Kepastian Hukum bagi Pengendali Data Pribadi di Masa Depan," *Masalah-Masalah Hukum* 53, no. 2 (2024): 135–144

[33] Yulfa Widiastuti et al., "The Impact of Coretax System Errors on the Quality of Taxpayers' Annual Tax Return Services," *Journal of Accounting, Taxation and Auditing* 6, no. 3 (2025): 597–605.

[34] Agung Tejopremono Kurnianto, "Coretax, Data Reliability, and Legal Consequences of Tax Administrative Decisions," *Journal of Artificial Intelligence and Digital Business* 5, no. 1 (2026): 3572–3579.

[35] W. Bhuasiri, H. Zo, H. Lee, and A. P. Ciganek., "User Acceptance of e-Government Services: Examining an e-Tax Filing and Payment System in Thailand," *Information Technology for Development* 22, no. 4 (2016): 672–695

of data leaks increases.[36] As the amount of personal data managed in this system increases, protecting taxpayers' personal data becomes a crucial issue. Taxpayer personal data, such as Taxpayer Identification Numbers (NPWP), financial status, addresses, and other tax-related information, are highly vulnerable to leaks or misuse if not managed properly.[37] If this data is not properly protected, it can potentially be misused by irresponsible parties.

Taxpayer information may include identification data, fiscal records, and financial information provided under a statutory obligation. The duties of the controller should consequently be examined by reference to purpose limitation, proportionality of access, data accuracy, confidentiality, and retention, while distinguishing the lawful basis for processing from consent in situations involving a legal obligation. Evidence on public institutions' handling of citizens' personal information explains how expectations concerning such uses influence institutional trust.[38] [39]These empirical findings support the relevance of protection duties, not a claim that confidence alone determines their legal content.

Cybersecurity issues in tax administration are also closely related to the concept of *cybersecurity governance* , namely governance that comprehensively integrates legal, institutional, policy, and technical aspects. [40], emphasizes that the success of data protection in the public sector is largely determined by clear legal responsibilities, internal oversight mechanisms, and inter-agency coordination. In the Indonesian context, cybersecurity governance still faces challenges of fragmented authority and overlapping regulations, which have the potential to weaken the effectiveness of taxpayer data protection.

Security governance is not exhausted by installing protective software. It includes an intelligible allocation of duties, internal monitoring, access reviews, record-keeping, and procedures for response to suspected incidents. Research on governmental digital-service adoption connects citizens' confidence with perceived service security.[41]

---

[36] N. N. Fajriyah., "The Influence of the Core Tax Administration System (CTAS) on Tax System Reform in the Digital Era," *Ekonomipedia: Journal of Economics, Management, and Business* 3, no. 1 (2025): 136–150.

[37] L. Y. Purnama and D. T. Della N., "The Effect of Taxpayer Data Leaks on Individual Taxpayers' Tax Trust and Compliance," *Global Education Scientific Journal* 6, no. 2: 436–446.

[38] A. Beldad, T. van der Geest, M. de Jong, and M. Steehouder., "A Cue or Two and I'll Trust You: Determinants of Trust in Government Organizations in Terms of Their Processing and Usage of Citizens' Personal Information Disclosed Online," *Government Information Quarterly* 29, no. 1 (2012): 41–49.

[39] A. Hooda, P. Gupta, A. Jeyaraj, and Y. K. Dwivedi., "Clarifying the Role of e-Government Trust in e-Government Success Models: A Meta-Analytic Structural Equation Modeling Approach," *Australasian Journal of Information Systems* 27 (2023)

[40] Gevan Naufal Wala and Retha Tesalonika., "Transforming Tax Administration Through Coretax: A Legal and Accounting Analysis," *JKIS: Journal of Communication and Social Sciences*, https://dinastires.org/JKIS.

[41] N. Alharbi, M. Papadaki, and P. Dowland, "The Impact of Security and Its Antecedents in Behaviour Intention of Using e-Government Services," *Behaviour & Information Technology* 36, no. 6 (2017): 620–636.

Normatively, Indonesia already has several regulations governing personal data protection and electronic system security, including the Electronic Information and Transactions Law (UU ITE), the Government Regulation on the Implementation of Electronic Systems and Transactions (PP PSTE), and Law Number 27 of 2022 concerning Personal Data Protection. Furthermore, the National Cyber and Crypto Agency (BSSN) has established information security management system standards for electronic system providers. However, various studies have shown that these regulations have not been fully followed by the implementation of effective cybersecurity governance in the public sector [42].

The distribution of legal rules across taxation, general electronic systems, and personal-data legislation requires an issue-specific determination of the applicable provisions. The KUP framework establishes the tax authority's access to information for statutory purposes; the PDP Law governs the obligations of personal data controllers; and electronic-system provisions address operational duties. Comparative research on the availability of privacy and security safeguards in digital government confirms that sectoral rules must be read together rather than treated as interchangeable. [43] [44] The legal assessment must still identify the specific statutory duty allegedly violated.

Purnama and Della's study shows that perceived data insecurity negatively impacts individual taxpayer compliance. This reinforces the argument that cybersecurity is not merely a technical issue but also a determining factor in the success of tax policies. Without strong data protection guarantees, digital tax reform risks losing social legitimacy. In this regard, state accountability is crucial, particularly in cases of data breaches. Aji [45]stated that the primary role of the state, specifically the Directorate General of Taxes (DGT), as the controller of taxpayer data, is to develop regulations on cyber data protection and cybersecurity. The DGT also acts as a personal data processor in coretax. Guaranteeing personal data protection is a citizen's right that requires citizen capacity and capability. A *state-centered approach* is often used in cybersecurity development. However, without a *people-centered approach* , it will be difficult to achieve protection for citizens regarding their highly valuable personal data. The dominance of a state-centered approach in

[42] Desi Rahma Aryanti., "Cybersecurity Governance in Public Institutions: Managing Digital Risks and Resilience," *Visioner: Jurnal Pemerintahan Daerah di Indonesia* 17, no. 3 (2025): 24–35.

[43] J. Sarabdeen, G. Rodrigues, and S. Balasubramanian., "e-Government Users' Privacy and Security Concerns and Availability of Laws in Dubai," *International Review of Law, Computers & Technology* 28, no. 3 (2014): 261–276.

[44] V. Venkatesh, J. Y. L. Thong, F. K. Chan, and P. J.-H. Hu., "Managing Citizens' Uncertainty in e-Government Services: The Mediating and Moderating Roles of Transparency and Trust," *Information Systems Research* 27, no. 1 (2016): 87–111.

[45] Hizkia Roland Prawyra Sitorus, Dewi Pika Lumbanbatu, Daniel David Sidebang, Dules Ery Pratama, and Risky Sakti Lumban Gaol., "Legal Review and Prevention Efforts for NPWP Data Leak Cases," *Aspirasi: Publikasi Hasil Pengabdian dan Kegiatan Masyarakat* 3, no. 4 (2025): 14–18

cybersecurity development has not yet achieved national data sovereignty, nor has it protected the personal data of each citizen. Building citizen capacity and capability is essential to safeguarding personal data in cyberspace.

The discussion of public trust is relevant to legal accountability but should not displace a rights-based analysis. Empirical studies distinguish the role of trust in access to public technology from direct evidence that an institution has complied with legal obligations. A meta-analytic account of risk, privacy, and security explains how trust can mediate citizens' use of government services. [46] Accountability in Coretax, however, must be based on the DGT's obligations and the demonstrated effect of its acts or omissions on taxpayer rights.

Personal data protection in electronic systems is governed by the PDP Law, the ITE Law, Government Regulation No. 71 of 2019, and relevant sector-specific provisions, while Government Regulation No. 80 of 2019 and ministerial rules govern matters within their respective scope. The enactment of the PDP Law supplies a general statutory basis for personal data protection, although the interaction among this law, tax secrecy requirements, and electronic-system obligations still requires close interpretation. The existence of multiple instruments is not itself proof of regulatory conflict; the question is whether any distinct obligations or remedies fail to operate coherently when applied to Coretax.[47]

This distinction matters because tax data may be processed for statutory compliance without eliminating controls on unauthorized access or secondary uses. Research on personal-data protection in Indonesia places the right to privacy within the legal protection provided by the PDP framework.[48] A more recent comparative account of data-protection rules similarly identifies the importance of oversight and legal enforcement, beyond enactment of the statute itself.[49] The duties of the DGT must therefore be determined from the text of the applicable provisions and its actual role in each processing activity.

In the context of taxation, the implications of the PDP Law are significant, given that the Directorate General of Taxes (DGT) has extensive access to taxpayer financial data. Therefore, implementing the PDP Law in the digital tax system requires policy adjustments and enhanced information technology security to ensure optimal data protection principles are implemented. Comparative scholarship

[46] Parul Gupta et al., "Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis," *Information Systems Frontiers* 27 (2025): 1089–1105

[47] Danny Kobrata and Rahma Atika., "The Privacy, Data Protection and Cybersecurity Law Review: Indonesia," *The Law Reviews* (5 November 2021), https://thelawreviews.co.uk/

[48] Elfian Fauzy and Nabila Alif Radika Shandy., "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2022)

[49] Predderics Hockop Simanjuntak., "Perlindungan Hukum terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)," *Esensi Hukum* 6, no. 2 (2024),

regarding the legal regulation of electronic government underscores the significance of public-law responsibility.

The regulation on personal data protection in the ITE Law is covered in Article 26 paragraph (1) where the use of information via electronic media must obtain the consent of the person concerned and Article 26 paragraph (3) regarding the deletion of information and/or electronic documents that are no longer relevant. In PP 80/2019 itself, the regulation on personal data protection is covered in CHAPTER XI Articles 58-59. In general, the regulation on personal data protection in PP 80/2019 talks about storing personal data according to applicable protection standards; the rules for personal data protection, including obtaining data honestly and legally, keeping personal data accurate and up-to-date, processing according to purpose, prohibition on sending personal data outside Indonesia unless it provides the same level of protection, and deletion of personal data. Neither the ITE Law nor PP 80/2019 has explicitly regulated, among other things, the rights of data subjects, the concept of data processors.

In PP 71/2019, there are more comprehensive regulations regarding personal data protection. The regulations are covered in Articles 14-18, 29, 37. In principle, the regulations in PP 71/2019 talk about the obligation to implement the principles of personal data protection in processing activities; the obligation to obtain consent from data owners; notification of failures in personal data protection; the obligation to delete and the deletion mechanism; and privacy guarantees. The most comprehensive regulation of personal data protection under positive law in Indonesia is currently regulated in Permenkominfo 20/2016. In general, Permenkominfo 20/2016 regulates the acquisition and collection of personal data according to the purpose (*purpose limitation*); respect for personal data owners (*confidentiality*); the obligation to obtain consent; storage of personal data for a certain period (*storage limitation*); transfer of data outside Indonesia; destruction of personal data; the rights of personal data owners; PSE obligations; dispute resolution; and administrative sanctions. The provisions regarding sanctions in Ministerial Regulation 20/2016 are limited to administrative sanctions only, and there are no provisions regarding the imposition of fines or the amount of fines that may be imposed in the event of violations. The role of data controller and data processor remains mixed, suggesting that PSEs are always both data controllers and data processors.

Regulations on personal data protection in the context of taxation in Indonesia are covered by "Law of the Republic of Indonesia Number 6 of 1983 concerning General Provisions and Procedures for Taxation," which was most recently amended by Law of the Republic of Indonesia Number 7 of 2021 (the KUP Law). Several articles relevant to personal data protection are Article 34, Article 35, and Article 35A. For example, Article 35 of the KUP Law stipulates that "in implementing tax laws and regulations, if information or evidence is required from banks, public

accountants, notaries, tax consultants, administrative offices, and/or other third parties related to the Taxpayer, then these parties are required to provide the requested information or evidence." However, such requests must be based on a written request from the Director General of Taxes. Naturally, this article has implications for taxpayers' personal data. In this case, taxpayer data privacy must be balanced with the state's interest in collecting taxes. This implication opens up discussion about how the state can protect its citizens' personal data while still fulfilling its tax collection duties.[50]

Overlapping regulations can be seen in the Law on General Provisions and Tax Procedures (UU KUP), which was updated in Law Number 7 of 2021 concerning the Harmonization of Tax Regulations (UU HPP), which authorizes the Directorate General of Taxes (DGT) to access and use taxpayer data extensively for tax collection purposes.[51] This may conflict with the data minimization principle in the PDP Law, which states that data controllers may only collect and process data to the extent strictly necessary.

Furthermore, in practice and reality, tax regulations, including coretax, are regulated by the Minister of Finance Regulation and the Directorate General of Taxes Circular Letter, which do not have the same legal force as a law. Hierarchically, a law has a higher hierarchy than a Ministerial Regulation. This has the potential to be one of the causes of suboptimal enforcement of data breach cases in Indonesia. This is also what actually encourages the creation of a law specifically regulating personal data protection, because without a law, personal data breach cases will never be optimally and appropriately prosecuted.[52] Evaluations of the digital trust relationship underline why clarity about government processing is relevant to the taxpayer's willingness to engage with administrative services.[53]

Beyond regulatory aspects, the issue of government responsibility is also crucial. The government has a constitutional obligation to protect citizens' rights, including the right to privacy. If taxpayer data is leaked through Coretax, the government must be held accountable, either through administrative, civil, or criminal mechanisms. [54]This question is relevant considering that tax data is managed by state institutions, so data leaks can be considered a form of negligence or a violation of the

[50] Nafis Dwi Kartiko, Samuel Putra Soegiono, Carissa Amanda Siswanto, and Rizky Pratama Putra Karo-Karo., "Legal Consequences of Personal Data Protection Regulations on Taxpayer Data from a Taxation Perspective," *Proceedings of the 5th National Conference on Law Studies*:355–365.

[51] Law Number 7 of 2021 concerning Harmonization of Tax Regulations.

[52] Wenderlin Koswara., "Implementation of Personal Data Protection Rules by Electronic System Organizers Linked to the Theory of Justice and Legal Certainty," *Journal of Development Law Paradigm* 7, no. 2 (2022).

[53] Onora O'Neill., "Linking Trust to Trustworthiness," *International Journal of Philosophical Studies* 26, no. 2 (2018):293–300.

[54] Wenderlin Koswara., "Implementation of Personal Data Protection Rules by Electronic System Organizers Linked to the Theory of Justice and Legal Certainty," *Journal of Development Law Paradigm* 7, no. 2 (2022).

state's obligation to protect citizens' rights. In international literature, data protection in tax administration is viewed as part of the right to privacy and *good governance*. *The World Bank* (2021) emphasizes the importance of integrating data protection and cybersecurity principles from the design stage of a digital tax system (*privacy and security by design*). However, most studies in Indonesia remain sectoral, separating data protection law, cybersecurity, and digital tax policy. This has led to a lack of comprehensive analysis that links these three aspects in an integrated manner within the context of Coretax.

For alleged harm, an effective accountability mechanism must permit the relevant facts to be reconstructed: what data were processed, what purpose authorized the action, what system operation occurred, which official or organizational unit supervised it, and how the taxpayer was affected. Normative analysis of good administration in automated decision-making supports the requirement for identifiable institutional responsibility.[55] Research on the transparency of public digital services demonstrates the importance of explaining decisions and preserving reviewability.[56] In a state-run tax platform, vendor participation may create contractual responsibility, but it does not by itself transfer the DGT's public-law duties toward the taxpayer.

Institutional remedies should correspond to the failure identified rather than presume that every defect requires the same response. If taxpayer information is inaccurate, rectification and review of the resulting administrative consequences are central. If a service is unavailable, recorded attempts to comply and a lawful administrative solution may be more relevant. If data are disclosed without authorization, breach-related investigation and legally available claims must be considered. Research on government digitalization in Indonesia identifies public trust as a concern across institutional service settings.[57]

The Personal Data Protection Law (PDP) provides a legal basis for personal data protection, but challenges remain in its implementation. One of the main challenges facing the implementation of the PDP Law in Coretax is low awareness of the importance of data protection among system administrators and data users, namely taxpayers. Although the PDP Law provides clear guidelines for personal data management, many parties, both data administrators and taxpayers, do not fully understand the legal implications of data breaches. Furthermore, limited infrastructure and skilled human resources in cybersecurity are major obstacles to implementing effective data protection policies in the

[55] Ulrik B. U. Roehl., "Automated Decision-Making and Good Administration: Views from Inside the Government Machinery," *Government Information Quarterly* 40, no. 4 (2023): 101864

[56] Douglas Morgan Fullin Saldanha, Cleidson Nogueira Dias, and Siegrid Guillaumon., "Transparency and Accountability in Digital Public Services: Learning from the Brazilian Cases," *Government Information Quarterly* 39, no. 2 (2022): 101680

[57] Sose Raeinaldo Virnandes, Jun Shen, and Elena Vlahu-Gjorgievska., "Building Public Trust through Digital Government Transformation: A Qualitative Study of Indonesian Civil Service Agency," *Procedia Computer Science* 234, (2024):1183–1191

Coretax system.[5859] Survey-based findings from Indonesia on perceived security and data privacy offer related support for the service-trust dimension.[60]

The central contribution of the article is thus a combined test for DGT accountability: first, establish its role and legal authority in the processing activity; second, identify the duty attaching to the relevant data or administrative output; third, determine the proven failure and causal connection to the taxpayer's harm; and fourth, identify the lawful avenue for correction, review, or redress.

In this regard, government accountability is crucial, particularly in cases of data breaches. The government, through authorized agencies such as the Directorate General of Taxes, must be responsible for ensuring that data breaches are prevented and, if they occur, that affected individuals are provided with adequate redress. In this regard, the provisions regarding government accountability in the PDP Law need to be further evaluated, including the redress mechanisms available to taxpayers whose data is breached.[61]

D. CONCLUSION

The first objective of this study establishes that Coretax is not merely a technical application but an electronic instrument through which the DGT performs public tax-administration functions. Its operation must therefore comply with the legal requirements for electronic systems, the exercise of statutory tax authority, and the protection of personal data. The existence of electronic assistance or automated data processing does not displace the authority and accountability attached to the competent public institution. The second objective establishes that the DGT's accountability as a personal data controller depends on the particular processing activity and legal obligation involved. A service outage, inaccurate taxpayer data, an improper administrative output, and a verified personal-data breach entail different facts, possible legal violations, and avenues of review or redress. Suspicious messages and phishing attempts cannot, without further evidence, be treated as proof that the Coretax database has been compromised. Where an error or violation is established, the DGT remains responsible for discharging its public-law duties even if the system involves external technical providers. The novelty of this research is the combined accountability assessment linking the DGT's data-controller obligations to the stages of Coretax-based tax administration: lawful data collection and verification, secure processing, accountable administrative outputs, and available correction or review. It clarifies that the legal analysis must identify

[58] Wenderlin Koswara., "Implementation of Personal Data Protection Rules by Electronic System Organizers Linked to the Theory of Justice and Legal Certainty," *Journal of Development Law Paradigm* 7, no. 2 (2022).

[59] Yulianto Wibowo, Ida Aryati DPW, and Ismiyanto., "Legal Review of the Protection of Public Personal Data in the Digitalization Era," *Jurnal Serambi Hukum* 18, no. 1 (2025): 1–6.

[60] Ulung Pribadi, Muhammad Iqbal, and Fittia Restiane., "Factors Affecting Trust in e-Government," *Journal of Government and Civil Society* 5, no. 2 (2021)

[61] Yulianto Wibowo, Ida Aryati DPW, and Ismiyanto., "Legal Review of the Protection of Public Personal Data in the Digitalization Era," *Jurnal Serambi Hukum* 18, no. 1 (2025): 1–6.

the competent controller, the applicable duty, the established failure, and the taxpayer's corresponding remedy, rather than treating all digital risks as identical. The study contributes a focused cyber-law and administrative-law interpretation of responsibility in electronic tax administration, while recognizing that separate factual investigation is required to determine liability in an individual incident. Consequently, the modernization of Indonesian tax administration through Coretax depends on both effective electronic services and enforceable protection of taxpayer rights. The study's contribution is to connect security and transparency with the continuing legal responsibility of the DGT, so that technological implementation does not become a reason for weakening administrative accountability.

BIBLIOGRAPHY

Journals:

A. Al-Muwil, V. Weerakkody, R. El-Haddadeh, and Y. Dwivedi., "Balancing Digital-by-Default with Inclusion: A Study of the Factors Influencing e-Inclusion in the UK," *Information Systems Frontiers* 21, (2019).

A. Beldad, T. van der Geest, M. de Jong, and M. Steehouder., "A Cue or Two and I'll Trust You: Determinants of Trust in Government Organizations in Terms of Their Processing and Usage of Citizens' Personal Information Disclosed Online," *Government Information Quarterly* 29, no. 1 (2012).

A. Hooda, P. Gupta, A. Jeyaraj, and Y. K. Dwivedi, "Clarifying the Role of e-Government Trust in e-Government Success Models: A Meta-Analytic Structural Equation Modeling Approach," *Australasian Journal of Information Systems* 27 (2023), https://doi.org/10.3127/ajis.v27i0.4079.

Abdul Wahab and Muhammad Suhardi., "Algorithmic Transparency in Digital Public Services: An Administrative Law Perspective," *Jurnal Kecerdasan Buatan dan Teknologi Informasi* 5, no. 1 (2026), https://doi.org/10.69916/jkbti.v5i1.461.

F. A. F. Alazzam, H. J. M. Shakhatreh, K. K. A. R. Aldroub, M. A. M. Assaf, N. M. Albalawee, and A. A. A. Almahasneh., "Mapping IS Governance and Cyber Risk in E-Commerce: A Bibliometric Analysis of Technical Infrastructure, Trading Law, and Risk Management," *Journal of Electronic Commerce in Organizations* (2026), https://doi.org/10.1080/07366981.2026.2635154.

Andhika Yuli Rimbawan., "Harmonization of Judicial Decisions: Analysis of Compliance with Jurisprudence and Application of the Principle of Legality in Special Criminal Cases," *Journal Critical Legal System* 1, no. 1 (2026), https://doi.org/10.68113/4577ep97.

Desi Rahma Aryanti., "Cybersecurity Governance in Public Institutions: Managing Digital Risks and Resilience," *Visioner: Jurnal Pemerintahan Daerah di Indonesia* 17, no. 3 (2025), https://doi.org/10.54783/jv.v17i3.1424.

D. Valle-Cruz., "Public Value of e-Government Services through Emerging Technologies," *International Journal of Public Sector Management* 32, no. 5 (2019), https://doi.org/10.1108/IJPSM-03-2018-0072.

Danny Kobrata and Rahma Atika., "The Privacy, Data Protection and Cybersecurity Law Review: Indonesia,"*The Law Reviews* (5 November 2021), https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/indonesia.

Douglas Morgan Fullin Saldanha, Cleidson Nogueira Dias, and Siegrid Guillaumon., "Transparency and Accountability in Digital Public Services: Learning from the Brazilian Cases," *Government Information Quarterly* 39, no. 2 (2022), https://doi.org/10.1016/j.giq.2022.101680.

Elfian Fauzy and Nabila Alif Radika Shandy., "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2022), https://doi.org/10.20885/JLR.vol7.iss3.art1.

N. N. Fajriyah., "The Influence of the Core Tax Administration System (CTAS) on Tax System Reform in the Digital Era," *Ekonomipedia: Journal of Economics, Management, and Business* 3, no. 1 (2025).

Febrian Hilmi Firdaus., "Perlindungan dan Kepastian Hukum bagi Pengendali Data Pribadi di Masa Depan," *Masalah-Masalah Hukum* 53, no. 2 (2024), https://doi.org/10.14710/mmh.53.2.2024.135-144.

Gevan Naufal Wala and Retha Tesalonika., "Transforming Tax Administration Through Coretax: A Legal and Accounting Analysis," *JKIS: Journal of Communication and Social Sciences*, https://dinastires.org/JKIS.

S. Grimmelikhuijsen and A. Meijer., "Legitimacy of Algorithmic Decision-Making: Six Threats and the Need for a Calibrated Institutional Response," *Perspectives on Public Management and Governance* 5, no. 3 (2022), https://doi.org/10.1093/ppmgov/gvac008.

H. Deng, K. Karunasena, and W. Xu., Evaluating the Performance of e-Government in Developing Countries: A Public Value Perspective," *Internet Research* 28, no. 1 (2018)

Indriana Masru'iyati Salma Izzah., "Digital Acceleration in the Justice System: Weighing Effectiveness and Challenges E-Court in Indonesia," *Journal Critical Legal System* 1, no. 1 (2026), https://doi.org/10.68113/vjk8d843.

J. Ejdys, R. Ginevicius, Z. Rozsa, and K. Janoskova., "The Role of Perceived Risk and Security Level in Building Trust in e-Government Solutions," *E+M Ekonomie a Management* 22, no. 3 (2019), https://doi.org/10.15240/tul/001/2019-3-014.

J. Sarabdeen, G. Rodrigues, and S. Balasubramanian., "e-Government Users' Privacy and Security Concerns and Availability of Laws in Dubai," *International Review of Law, Computers & Technology* 28, No. 3 (2014)

Nafis Dwi Kartiko, Samuel Putra Soegiono, Carissa Amanda Siswanto, and Rizky Pratama Putra Karo-Karo., "Legal Consequences of Personal Data Protection Regulations on Taxpayer Data from a Taxation Perspective," *Proceedings of the 5th National Conference on Law Studies*.

Wenderlin Koswara., "Implementation of Personal Data Protection Rules by Electronic System Organizers Linked to the Theory of Justice and Legal Certainty," *Journal of Development Law Paradigm* 7, No. 2 (2022).

Agung Tejopremono Kurnianto., "Coretax, Data Reliability, and Legal Consequences of Tax Administrative Decisions," *Journal of Artificial Intelligence and Digital Business* 5, No. 1 (2026)

Luh Putu Vera Astri Pujayanti., "Constitutionality of the Use of Artificial Intelligence in Government Administrative Decision-Making: An Analysis of the Principle of Due Process of Law in Indonesia," *International Journal of Scientific Research* (2025), https://doi.org/10.62894/fqp2nc41.

M. S. Al-Zahrani., "Integrating IS Success Model with Cybersecurity Factors for e-Government Implementation in the Kingdom of Saudi Arabia," *International Journal of Electrical and Computer Engineering* 10, no. 5 (2020)

Madalina Busuioc., "Accountable Artificial Intelligence: Holding Algorithms to Account," *Public Administration Review* 81, no. 5 (2021), https://doi.org/10.1111/puar.13293.

R. P. Maramis., "Use of Personal Data and Customer Identity in Banking Crimes," *Lex Privatum* VII, No. 7 (2019).

N. Alharbi, M. Papadaki, and P. Dowland., "The Impact of Security and Its Antecedents in Behaviour Intention of Using e-Government Services," *Behaviour & Information Technology* 36, No. 6 (2017).

Onora O'Neill., "Linking Trust to Trustworthiness.," *International Journal of Philosophical Studies* 26, no. 2 (2018).

S. R. Paminto et al., "Legal Protection for Victims of Data and Personal Information Theft in the Era of Cybercrime," 2, no. 2 (2024).

Parul Gupta et al., "Trust, Risk, Privacy and Security in e-Government Use: Insights from a MASEM Analysis," *Information Systems Frontiers* 27 (2025). https://doi.org/10.1007/s10796-024-10497-8.

Predderics Hockop Simanjuntak., "Perlindungan Hukum terhadap Data Pribadi pada Era Digital di Indonesia: Studi Undang-Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)," *Esensi Hukum* 6, no. 2 (2024), https://doi.org/10.35586/esensihukum.v6i2.412.

L. Y. Purnama and D. T. Della N., "The Effect of Taxpayer Data Leaks on Individual Taxpayers' Tax Trust and Compliance," *Global Education Scientific Journal* 6, no. 2, pp. 436–446.

Rebecca Williams., "Rethinking Administrative Law for Algorithmic Decision Making," *Oxford Journal of Legal Studies* 42, no. 2 (2022), https://doi.org/10.1093/ojls/gqab032.

Rommy Igirisa, Ferdinand Boba Panaha, and Yovan Iristian., "Algorithmic Transparency and Due Process in Automated Administrative Discretion: A Comparative Regulatory Analysis," *Lex Journal: Kajian Hukum dan Keadilan* 8, no. 2 (2025), https://doi.org/10.25139/lex.v8i2.12746.

S. Goldfinch., "Pessimism, Computer Failure, and Information Systems Development in the Public Sector," *Public Administration Review* 67, no. 5 (2007)

Linda Santioso and Andreas B. Daryatno. "The Effect of Digitalization of Taxation, Tax Morale and Modernization of the Administrative System on Taxpayer Compliance," *International Journal of Application on Economics and Business* 3, no. 2 (2025), pp. 682–695.

Hizkia Roland Prawyra Sitorus, Dewi Pika Lumbanbatu, Daniel David Sidebang, Dules Ery Pratama, and Risky Sakti Lumban Gaol, "Legal Review and Prevention Efforts for NPWP Data Leak Cases," *Aspirasi: Publikasi Hasil Pengabdian dan Kegiatan Masyarakat* 3, no. 4 (2025), https://doi.org/10.61132/aspirasi.v3i4.1851.

N. A. Smuha., "The Use of Algorithmic Systems by Public Administrations: Practices, Challenges and Governance Frameworks," in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).

Sose Raeinaldo Virnandes, Jun Shen, and Elena Vlahu-Gjorgievska, "Building Public Trust through Digital Government Transformation: A Qualitative Study of Indonesian Civil Service Agency," *Procedia Computer Science* 234 (2024), https://doi.org/10.1016/j.procs.2024.03.114.

Ulrik B. U. Roehl, "Automated Decision-Making and Good Administration: Views from Inside the Government Machinery," *Government Information Quarterly* 40, no. 4 (2023), https://doi.org/10.1016/j.giq.2023.101864.

Ulung Pribadi, Muhammad Iqbal, and Fittia Restiane, "Factors Affecting Trust in e-Government," *Journal of Government and Civil Society* 5, no. 2 (2021), https://doi.org/10.31000/jgcs.v5i2.4848.

V. Venkatesh, J. Y. L. Thong, F. K. Chan, and P. J.-H. Hu, "Managing Citizens' Uncertainty in e-Government Services: The Mediating and Moderating Roles of Transparency and Trust," *Information Systems Research* 27, no. 1 (2016)

Vima Septia and Agus Supriyo., "Legal Protection of Confidentiality of Personal Data for Regional Taxpayers," *Mendapo: Journal of Administrative Law* 4, no. 2 (2023), https://doi.org/10.22437/mendapo.v4i2.25206.

W. Bhuasiri, H. Zo, H. Lee, and A. P. Ciganek., "User Acceptance of e-Government Services: Examining an e-Tax Filing and Payment System in

Thailand," *Information Technology for Development* 22, no. 4 (2016), https://doi.org/10.1080/02681102.2016.1173001.

W. Munyoka and M. S. Maharaj., "Privacy, Security, Trust, Risk and Optimism Bias in e-Government Use: The Case of Two Southern African Development Community Countries," *SA Journal of Information Management* 21, no. 1 (2019), https://doi.org/10.4102/sajim.v21i1.983.

Yulianto Wibowo, Ida Aryati DPW, and Ismiyanto., "Legal Review of the Protection of Public Personal Data in the Digitalization Era," *Jurnal Serambi Hukum* 18, no. 1 (2025).

Yulfa Widiastuti et al., "The Impact of Coretax System Errors on the Quality of Taxpayers' Annual Tax Return Services," *Journal of Accounting, Taxation and Auditing* 6, no. 3 (2025).

H. T. Wu., "Regulation of Automated Administration via Technical Due Process in the Context of Algorithmic Black Box," *Advances in Law* 8, no. 2 (2026), https://doi.org/10.35534/al.0802004.

Y. Wu and C. Lin., "Navigating the Labyrinth: Essential Conditions for Generative Artificial Intelligence Governance," *IT Professional* 28, no. 2 (2026), https://doi.org/10.1109/MITP.2026.3663787.

Regulation:

Law Number 7 of 2021 concerning Harmonization of Tax Regulations.