DOI: 10.46924/jihk.v8i1.495

Reconstructing Taxpayer Data Protection Through a Cyber-Restorative State Accountability Framework

Imam Cahyo Pornomo[1]*, Ismiyanto Ismiyanto[2], & Hafid Zakariya[3]

[1,2,3]Universitas Islam Batik Surakarta, Indonesia

Correspondence

Imam Cahyo Pornomo, Universitas Islam Batik Surakarta, Indonesia, Jl. Agus Salim No.10, Sondakan, Kec. Laweyan, Kota Surakarta, Jawa Tengah 57147, *e-*mail: imamcp@gmail.com

How to cite

Pornomo, Imam Cahyo., Ismiyanto, Ismiyanto., & Zakariya, Hafid. 2026. Reconstructing Taxpayer Data Protection Through a Cyber-Restorative State Accountability Framework. *Jurnal Ilmu Hukum Kyadiren* 8(1), 723-745. https://doi.org/10.46924/jihk.v8i1.495

Original Article

Abstract

The digital transformation of tax administration has significantly improved the efficiency of public services; however, it has also heightened the risk of taxpayer data breaches involving highly sensitive personal and financial information. This study aims to examine the legal status of taxpayer data, identify the fragmentation of the regulatory framework governing taxpayer data protection, analyze state responsibility from a cyber law perspective, and develop a cyber-restorative state accountability framework. The research employs a normative legal methodology using statutory, conceptual, and comparative approaches. Data are analyzed prescriptively through systematic legal interpretation. The findings indicate that taxpayer data simultaneously constitute specific personal data, confidential tax information, and electronic information, each protected under multiple legal regimes. Nevertheless, the existing regulatory framework remains fragmented, resulting in inconsistencies in legal protection and state accountability. To address these shortcomings, this study proposes a cyber-restorative state accountability framework that integrates preventive measures, cybersecurity governance, breach notification, incident investigation, data recovery, and compensation mechanisms. The study concludes that reconstructing the legal framework based on this model is essential for strengthening legal certainty, enhancing state accountability, and fostering public trust in digital tax administration.

Keywords: *Taxpayer Data, Personal Data Protection, Cyber Law*

Abstrak

Perkembangan digital administrasi perpajakan meningkatkan efisiensi pelayanan, namun juga memperbesar risiko kebocoran data wajib pajak yang mengandung informasi pribadi dan keuangan bernilai tinggi. Penelitian ini bertujuan menganalisis kedudukan hukum data wajib pajak, mengidentifikasi fragmentasi pengaturan perlindungan data, mengkaji tanggung jawab negara dari perspektif hukum siber, serta merumuskan model *cyber-restorative state accountability*. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan perbandingan, dianalisis secara preskriptif melalui interpretasi sistematis. data wajib pajak merupakan data pribadi spesifik, rahasia perpajakan, dan informasi elektronik yang dilindungi secara kumulatif, namun regulasinya masih terfragmentasi. Penelitian ini menawarkan model *cyber-restorative state accountability* yang mengintegrasikan pencegahan, keamanan siber, notifikasi, investigasi, pemulihan, dan kompensasi. Disimpulkan bahwa rekonstruksi tersebut diperlukan untuk memperkuat kepastian hukum, akuntabilitas negara, dan kepercayaan publik terhadap administrasi perpajakan digital.

Kata kunci: *Data Wajib Pajak, Perlindungan Data Pribadi, Hukum Siber*

1. INTRODUCTION

The digital transformation of public administration has become a cornerstone of governance reform in Indonesia, particularly in the taxation sector. To modernize tax administration, the Directorate General of Taxes (DGT) has introduced a range of technology-driven services, including e-Filing, e-Billing, e-Invoicing, the integration of the National Identification Number (NIK) with the Taxpayer Identification Number (NPWP), and the development of the Core Tax Administration System (CTAS). These initiatives have improved administrative efficiency, accelerated service delivery, expanded the national tax database, and strengthened taxpayer compliance monitoring.

Despite these significant advancements, digitalization has also introduced new challenges, particularly the heightened risk of cybersecurity incidents associated with the processing and storage of large volumes of taxpayers' personal data. Consequently, taxpayer data protection has emerged as a strategic legal issue that extends beyond administrative confidentiality to encompass the protection of citizens' constitutional rights to privacy, personal data protection, and information security.

Taxpayer data constitute a category of highly sensitive personal data because they contain information relating to an individual's identity, financial status, economic activities, asset ownership, and tax compliance history.[1] Accordingly, the legal protection of taxpayer data should not be limited to the confidentiality provisions established under the General Provisions and Tax Procedures Law (Law on General Provisions and Tax Procedures, UU KUP). It must also comply with the principles established under Law No. 27 of 2022 on Personal Data Protection (UU PDP). Furthermore, the governance of taxpayer data must adhere to the principles of accountability, electronic system security, transparency, and respect for the rights of data subjects. This multidimensional regulatory framework requires effective coordination among tax law, personal data protection law, administrative law, and cyber law.

The need to strengthen taxpayer data protection has become increasingly evident in light of several cybersecurity incidents in Indonesia, including the alleged breach involving millions of Taxpayer Identification Numbers (NPWP) reported in 2024, which generated widespread public concern.[2] These incidents demonstrate that cyber threats to digital tax administration are no longer merely theoretical but constitute tangible risks capable of undermining public confidence in the tax system. The traditional paradigm of taxpayer data protection, which primarily relies on the official secrecy provisions contained in Article 34 of the General Provisions and Tax

---

1 Siti Kurnia Rahayu, *Keamanan Digital Dalam Audit Pajak: Integrasi Cyber Security Dengan CRM, BDA, Dan BI Untuk Revolusi Compliance* (Unikom Press, 2024).

2 Hanin Marwah, "6 Juta Data NPWP Bocor: Diduga Milik Jokowi, Sri Mulyani, Dan Zulhas, Diperjualbelikan Seharga Rp 152 Juta," *Tempo*, 2024, https://www.tempo.co/ekonomi/6-juta-data-npwp-bocor-diduga-milik-jokowi-sri-mulyani-dan-zulhas-diperjualbelikan-seharga-rp-152-juta-8164.

Procedures Law, is no longer sufficient to address contemporary cybersecurity challenges. Current threats arise from vulnerabilities in electronic information systems, cyberattacks, inadequate information security governance, and limited institutional capacity for incident prevention and response. Consequently, a shift toward a cyber-accountability paradigm is required. Such a paradigm conceptualizes the state as bearing comprehensive responsibility throughout the entire data governance lifecycle, encompassing preventive measures, cybersecurity management, threat detection, incident response, data recovery, and the restoration of the legal rights of affected individuals.

Previous studies have examined taxpayer data protection from various perspectives. Widayanti et al. argue that Indonesia's cyber legal framework remains fragmented across sectors, resulting in overlapping institutional authority and weak interagency coordination. They advocate the development of an integrated national cyber legal framework informed by international best practices, including the European Union's General Data Protection Regulation (GDPR) and Australia's Critical Infrastructure Bill.[3] Similarly, Judijanto emphasizes that taxpayer data constitute highly sensitive personal information because they reveal taxpayers' identities, financial conditions, and economic transactions.[4] Accordingly, effective protection requires robust information security measures, transparent data governance, and stronger public trust in government institutions. Although these studies make valuable contributions to the discourse on personal data protection and cybersecurity governance, neither specifically examines the legal basis and scope of state accountability for taxpayer data breaches within Indonesia's digital tax administration system. This gap underscores the need for a comprehensive legal framework capable of integrating personal data protection, cyber law, and state responsibility into a coherent model of cyber-restorative accountability.

A more recent study by Nurmala and Wiraguna examined the 2024 breach involving approximately 6.6 million Taxpayer Identification Numbers (NPWP) in light of Law No. 27 of 2022 on Personal Data Protection. The authors concluded that the Directorate General of Taxes (DGT), acting as the data controller, had failed to comply with the principle of accountability and could therefore be subject to administrative sanctions.[5] Similarly, Alfajri and Najicha identified significant weaknesses in the governance of Indonesia's Electronic-Based Government System (Sistem

---

[3] Tri Fenny Widayanti et al., "Enhancing Cybersecurity and Legal Integration: Reforming Indonesia's Cyber Law to Foster Sustainable Growth in the Digital Economy," *Diponegoro Law Review* 10, no. 1 (2025): 105–19, https://doi.org/10.14710/dilrev.10.1.2025.105-119.

[4] Loso Judijanto, "Protection of Taxpayer Personal Data in Tax Administration: A Review," *Digital Business: Tren Bisnis Masa Depan* 15, no. 3 (2024): 185–94.

[5] Salma Ayu Nurmala and Sidi Ahyar Wiraguna, "Analisis Yuridis Tanggung Jawab Direktorat Jenderal Pajak (DJP) Terhadap Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Kajian Ilmiah* 26, no. 1 (2026): 85–94, https://doi.org/10.31599/207r0b59.

Pemerintahan Berbasis Elektronik or SPBE), particularly with respect to its legal framework, the effectiveness of supervisory mechanisms, and the institutional authority of the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara or BSSN).[6] Satoto and Santiago further argued for the enactment of a comprehensive National Cyber Law to address the growing complexity of contemporary cyber threats. Although these studies make valuable contributions to the development of cyber law and personal data protection, they do not examine how cybersecurity failures should shape the legal framework of state accountability in the administration of electronic taxation systems.[7]

Likewise, Huda et al. found that personal data breaches in Indonesia are primarily attributable to inadequate information security infrastructure, limited human resource capacity, and insufficient interinstitutional coordination.[8] Dirgantara et al. emphasized the importance of regulatory harmonization and strengthening supervisory mechanisms governing organizations that process personal data.[9] At the international level, Zhang demonstrated that mandatory data breach notification requirements can promote organizational improvements in cybersecurity risk management. Nevertheless, these studies primarily focus on the responsibilities of corporations, data controllers, or broader cyber law reform, without developing a comprehensive framework of state accountability specifically applicable to the protection of taxpayer data within digital tax administration.[10]

The existing body of literature generally addresses personal data protection, cyber law reform, SPBE governance, or the legal responsibilities of the Directorate General of Taxes as the data controller. However, no previous study has comprehensively integrated tax law, administrative law, personal data protection law, and cyber law to reconstruct a coherent framework of state accountability for taxpayer data breaches. Accordingly, the principal novelty of this study lies in the development of a cyber-restorative state accountability framework, which emphasizes preventive measures, institutional accountability, post-breach recovery, and the protection of taxpayers' constitutional rights throughout the entire lifecycle of digital tax data governance.

---

6 Farhan Zaidan Alfajri and Fatma Ulfatun Najicha, "Legal Reconstruction of Accountability for the Security of Electronic-Based Government Systems Based on the Principles of Good Governance," in *Proceedings of the International Conference on Democracy and National Resilience 2025 (ICDNR 2025)*, vol. 981, ed. Sunny Ummul Firdaus et al., Advances in Social Science, Education and Humanities Research (Atlantis Press SARL, 2025), https://doi.org/10.2991/978-2-38476-529-4_12.

7 Endro Satoto and Faisal Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption," *Greenation International Journal of Law and Social Sciences* 3, no. 2 (2025): 309–17, https://doi.org/10.38035/gijlss.v3i2.425.

8 Uu Nurul Huda et al., "Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights Within The Framework of The Indonesian Legal State," *Jambura Law Review* 1, no. 1 (2026): 144–59, https://doi.org/10.33756/jlr.v1i1.32666.

9 Febrian Dirgantara et al., "Legal Responsibility of Companies in Cases of Personal Data Breaches," *Innovative: Journal of Social Science Research* 5, no. 1 (2025): 5053–65, https://doi.org/10.31004/innovative.v5i1.18046.

10 Yanlei Zhang, "Data Breach Disclosure Laws and Corporate Tax Planning Activities," *Journal of International Accounting, Auditing and Taxation* 60 (2026): 100749, https://doi.org/10.1016/j.intaccaudtax.2026.100749.

This study therefore seeks to (1) analyze the legal status of taxpayer data as a category of sensitive personal data; (2) identify regulatory fragmentation and weaknesses in the legal framework governing taxpayer data protection across multiple legal regimes; (3) examine the scope of state responsibility for taxpayer data breaches from a cyber law perspective; and (4) formulate a cyber-restorative state accountability framework that integrates prevention, cybersecurity governance, breach notification, incident investigation, data recovery, and compensation as the legal foundation for safeguarding taxpayers' constitutional rights in Indonesia's digital tax administration system.

2. RESEARCH METHODOLOGY

This study employs a normative legal research (doctrinal legal research) design with a prescriptive orientation to analyze, reconstruct, and formulate a legal framework for state accountability in response to taxpayer data breaches from a cyber law perspective. As a doctrinal inquiry, the research conceptualizes law as a normative system (law in the books), focusing on the analysis of statutory provisions, legal principles, doctrines, and theoretical concepts governing personal data protection, tax law, administrative law, and cyber law.

The study adopts four complementary research approaches. First, the statutory approach examines the legal framework established under the Law on General Provisions and Tax Procedures (UU KUP), Law No. 27 of 2022 on Personal Data Protection (UU PDP), the Electronic Information and Transactions Law (UU ITE), Government Regulation on the Implementation of Electronic Systems and Transactions (PP PSTE), and regulations governing the Electronic-Based Government System (SPBE). Second, the conceptual approach analyzes the doctrines and theories of state accountability, good governance, cyber accountability, and legal protection. Third, the case approach evaluates the alleged 2024 breach involving Taxpayer Identification Number (NPWP) data and the cybersecurity incident affecting Indonesia's National Temporary Data Center (Pusat Data Nasional Sementara or PDNS). Finally, the comparative approach examines the principles embodied in the European Union's General Data Protection Regulation (GDPR) together with internationally recognized cybersecurity standards to identify best practices relevant to Indonesia's legal framework.

The analysis is based on primary, secondary, and tertiary legal materials collected through an extensive literature review. Primary legal materials include statutes and regulations, while secondary materials consist of scholarly books, peer-reviewed journal articles, legal commentaries, and relevant judicial and policy documents. Tertiary materials comprise legal dictionaries, encyclopedias, and other reference sources that support legal interpretation. All legal materials were analyzed qualitatively using

descriptive-analytical and prescriptive methods. Legal interpretation was conducted through grammatical, systematic, teleological, and prospective (futuristic) interpretative techniques to ensure a comprehensive understanding of the applicable legal norms. The findings provide the basis for reconstructing a cyber-restorative state accountability framework, designed as a comprehensive model of state responsibility for safeguarding taxpayer data within Indonesia's digital tax administration system.

3. RESEARCH RESULT AND DISCUSSION

3.1. Legal Status of Taxpayer Data as Personal Data and Confidential Tax Information

Indonesia's legal framework protects taxpayer data through two distinct but interrelated legal regimes: the tax confidentiality regime and the personal data protection regime. Despite pursuing the common objective of safeguarding taxpayer information, these regimes continue to operate independently, resulting in a fragmented legal framework that has yet to provide comprehensive protection against cybersecurity threats arising from the digitalization of tax administration.

Taxpayer data possess a dual legal status. First, they constitute administrative data collected and processed by the state to perform fiscal functions, administer tax collection, monitor taxpayer compliance, and formulate revenue policies.[11] The government's authority to process such data derives from its public law mandate to administer taxation as an essential function of the state. Accordingly, the collection and use of taxpayer information represent an exercise of governmental authority rather than a purely administrative activity.

Second, taxpayer data also qualify as personal data because they relate to an identified or identifiable natural person.[12] Such data include the National Identification Number (Nomor Induk Kependudukan or NIK), the Taxpayer Identification Number (Nomor Pokok Wajib Pajak or NPWP), names, residential addresses, income, asset ownership, tax liabilities, financial transactions, and taxpayer compliance records. Pursuant to Article 1 of Law No. 27 of 2022 on Personal Data Protection, these categories of information satisfy the statutory definition of personal data because they enable the direct or indirect identification of an individual through one or more identifiable data elements.

Moreover, taxpayer data extend beyond the category of ordinary personal data and encompass sensitive personal data, particularly because they disclose an individual's financial condition and economic activities. Article 4 of the Personal Data Protection Law classifies financial information as sensitive personal data requiring a higher standard

---

[11] Naura Atania Putri Aghna, "Kepastian Hukum Keamanan Data Pribadi Wajib Pajak Dalam Pembayaran Pajak Secara Digital," *Jurnal Hukum Indonesia* 5, no. 2 (2026): 165–73, https://doi.org/10.58344/jhi.v5i2.2530.

[12] Aghna, "Kepastian Hukum Keamanan Data Pribadi Wajib Pajak Dalam Pembayaran Pajak Secara Digital."

of legal protection than ordinary personal data. This classification has significant legal implications, as it places the state, acting through the Directorate General of Taxes, in the position of a data controller that is legally obligated to process taxpayer data in accordance with the principles of lawfulness, transparency, proportionality, security, and accountability. Consequently, taxpayer data should no longer be regarded merely as administrative records maintained for taxation purposes; rather, they constitute an object of fundamental rights protection, directly linked to the constitutional rights to privacy and personal data protection.

The confidentiality of taxpayer information has long been recognized under Indonesian tax law through the doctrine of official tax secrecy. Article 34 of the Law on General Provisions and Tax Procedures prohibits tax officials and experts who obtain taxpayer information in the course of performing their official duties from disclosing such information to unauthorized parties. This provision reflects the legislature's longstanding recognition that preserving taxpayer confidentiality is essential to maintaining public trust in the tax administration system and ensuring the integrity of the relationship between taxpayers and the state.

Nevertheless, the protection afforded under the General Provisions and Tax Procedures Law remains centered on official confidentiality, focusing primarily on preventing unauthorized disclosures by individual public officials. This personnel-based model of protection was developed during an era in which tax administration relied predominantly on manual recordkeeping and paper-based procedures. Consequently, the principal risk to taxpayer confidentiality was perceived to arise from the misuse of authority or misconduct by government officials.

The digital transformation of tax administration has fundamentally altered the nature of these risks. In contemporary electronic tax administration systems, taxpayer data breaches are no longer attributable solely to the conduct of individual officials. Instead, they may result from deficiencies in cybersecurity architecture, malware and ransomware attacks, phishing schemes, identity theft, the exploitation of software vulnerabilities, unauthorized access to electronic databases, or failures in access control mechanisms. These evolving threats demonstrate that a legal framework based exclusively on official confidentiality is no longer adequate to protect taxpayer data in the digital environment. Accordingly, the legal paradigm governing taxpayer data protection must evolve from one centered on official secrecy to one grounded in institutional accountability. Under this approach, the state bears comprehensive responsibility for the entire lifecycle of taxpayer data governance, including data collection, storage, processing, use, disclosure, interagency data exchange, cybersecurity management, incident response, and post-breach recovery.[13] Such a paradigm reflects

[13] David Acev et al., "Systematic Analysis of Data Governance Frameworks and Their Relevance to Data Trusts," *Management Review Quarterly*, ahead of print, July 31, 2025, https://doi.org/10.1007/s11301-025-00545-1.

the broader principles of modern cyber law, which emphasize institutional responsibility, risk management, and the protection of fundamental rights throughout the digital governance process.

This study both reinforces and extends the findings of Judijanto, who argues that taxpayer information constitutes highly sensitive personal data and therefore requires enhanced legal protection to safeguard taxpayers' privacy rights.[14] It also supports the analysis of Nurmala and Wiraguna, which identifies the Directorate General of Taxes (DGT) as the data controller under Law No. 27 of 2022 on Personal Data Protection.[15] However, this study advances the existing literature by arguing that, beyond the DGT's operational responsibilities, the state itself constitutes the primary legal entity accountable for ensuring the security, integrity, and resilience of the electronic tax administration system. Furthermore, this study complements the work of Satoto and Santiago and Widayanti et al. concerning the need to reconstruct Indonesia's cyber law framework by demonstrating that such reform should begin with recognizing the dual legal status of taxpayer data as an object of legal protection situated at the intersection of tax law and personal data protection law.[16]

The coexistence of two legal regimes governing taxpayer data should not be interpreted as regulatory duplication. Rather, it establishes a complementary framework of dual legal protection that affords multiple layers of safeguards for taxpayers' rights. Under tax law, the state is obligated to preserve the confidentiality of information obtained from taxpayers and to prevent its unauthorized disclosure or misuse by public officials or third parties. At the same time, under the Personal Data Protection Law and the legal framework governing electronic systems, the state's obligations are considerably broader. They encompass ensuring that all processing of taxpayer data is conducted lawfully, securely, proportionately, transparently, and accountably in accordance with the principles of good governance and cybersecurity governance. These responsibilities extend beyond maintaining the confidentiality of taxpayer information to include establishing robust information security systems, implementing comprehensive cybersecurity risk management, conducting periodic security audits, ensuring continuous monitoring of electronic systems, and providing effective legal remedies whenever the rights of data subjects are violated.

Accordingly, the legal status of taxpayer data within the Indonesian legal system is characterized by dual legal protection: as confidential tax information under the Law on General Provisions and Tax Procedures (UU KUP) and as sensitive personal data under Law No. 27 of 2022 on Personal Data Protection (UU PDP). This dual legal status gives

---

[14] Judijanto, "Protection of Taxpayer Personal Data in Tax Administration: A Review."

[15] Nurmala and Wiraguna, "Analisis Yuridis Tanggung Jawab Direktorat Jenderal Pajak (DJP) Terhadap Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) Berdasarkan Undang-Undang Nomor 27 Tahun 2022."

[16] Satoto and Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption"; Widayanti et al., "Enhancing Cybersecurity and Legal Integration."

rise to a corresponding dual obligation on the part of the state. On the one hand, the state must maintain the confidentiality of taxpayer information; on the other, it must ensure the security, integrity, confidentiality, availability, and accountability of taxpayer data throughout the entire lifecycle of digital tax administration.

These findings provide an important conceptual foundation for the development of a cyber-restorative state accountability framework. In the era of digital transformation, taxpayer data protection can no longer rely solely on the traditional doctrine of official secrecy or passive confidentiality. Instead, it requires an active and preventive model of state accountability that integrates cybersecurity governance with mechanisms for restoring the legal rights of affected individuals following a data breach. Within this framework, the state's responsibility extends beyond preventing unauthorized disclosures to encompassing comprehensive risk management, timely incident response, effective data recovery, and appropriate compensation where legal rights have been infringed. Consequently, recognizing the dual legal status of taxpayer data serves as the normative basis for harmonizing tax law, personal data protection law, and cyber law, thereby supporting the development of a secure, accountable, and legally certain system of digital tax administration.

3.2. Fragmentation of the Legal Framework Governing Taxpayer Data Protection in Digital Tax Administration

Indonesia has established a relatively comprehensive legal foundation for the protection of taxpayer data. Nevertheless, the relevant legal instruments remain sector-specific and have yet to be integrated into a coherent regulatory framework. This fragmentation creates normative inconsistencies and legal uncertainty regarding the scope and basis of state accountability when taxpayer data breaches occur within the electronic tax administration system.

The legal protection of taxpayer data is founded upon four complementary layers of regulation. The first layer consists of constitutional protection derived from the 1945 Constitution of the Republic of Indonesia. Article 28G(1) guarantees every individual's right to personal security and to the protection of their person, family, honor, dignity, and property. Article 28D(1) guarantees the right to legal certainty and equal protection under the law, while Article 28H(4) protects the right to property against arbitrary deprivation. Collectively, these constitutional provisions establish that personal data—including taxpayer information containing financial and economic details—constitute an aspect of citizens' constitutional rights that must be respected, protected, and fulfilled by the state.

The second layer comprises the personal data protection regime established under Law No. 27 of 2022 on Personal Data Protection. This statute provides a comprehensive legal framework governing the rights of data subjects, the principles of

lawful data processing, the obligations of data controllers, mandatory notification of personal data breaches, and mechanisms for administrative sanctions. Within this framework, the Directorate General of Taxes (DGT), as the data controller, is required to ensure that taxpayer data are processed lawfully, transparently, proportionately, securely, and accountably. However, the Personal Data Protection Law functions as lex generalis and therefore does not specifically regulate the unique legal characteristics of taxpayer data as public fiscal information that directly affects state revenue and fiscal administration.

The third layer consists of the tax confidentiality regime established under Article 34 of the Law on General Provisions and Tax Procedures (UU KUP). This provision requires tax officials and other authorized persons who obtain taxpayer information in the course of performing their official duties to maintain its confidentiality. Unlike the Personal Data Protection Law, which emphasizes the protection of data subjects' rights and the accountability of data controllers, the UU KUP focuses primarily on preventing unauthorized disclosure of confidential tax information by public officials. Consequently, its regulatory scope is confined to official conduct rather than the broader governance of taxpayer data throughout its lifecycle. This traditional confidentiality model is therefore ill-equipped to address contemporary cybersecurity risks associated with digital tax administration, including ransomware attacks, exploitation of software vulnerabilities, unauthorized access to electronic databases, and other forms of cyber intrusion.

The fourth layer comprises the electronic systems governance regime, principally governed by the Electronic Information and Transactions Law (UU ITE) and Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions. These instruments require electronic system operators to maintain reliable, secure, and accountable information systems in accordance with recognized information security principles. They also establish the legal basis for cybersecurity governance within both public and private electronic systems. However, these regulations remain broadly applicable and do not prescribe sector-specific cybersecurity requirements for digital tax administration. In particular, they do not establish mandatory standards for periodic cybersecurity audits, Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), or specialized procedures for responding to taxpayer data breaches.

These four legal regimes have evolved with distinct normative objectives. Constitutional law is primarily concerned with safeguarding fundamental constitutional rights. The Personal Data Protection Law focuses on protecting data subjects and ensuring the accountability of data controllers. The UU KUP emphasizes the confidentiality of taxpayer information, whereas the Electronic Information and Transactions Law and Government Regulation No. 71 of 2019 are principally directed

toward ensuring the reliability and security of electronic systems. Because these regulatory frameworks were developed independently, they operate in parallel rather than as an integrated legal system. As a result, none explicitly establishes a comprehensive mechanism for allocating state accountability in the event of taxpayer data breaches.

Accordingly, although Indonesia possesses multiple legal instruments capable of protecting taxpayer data, the existing framework remains fragmented and lacks normative integration. The absence of harmonized provisions connecting constitutional guarantees, tax confidentiality obligations, personal data protection principles, and cybersecurity governance has created a regulatory gap in defining the state's legal responsibilities following taxpayer data breaches. This fragmentation underscores the need for an integrated framework of cyber-restorative state accountability capable of harmonizing these legal regimes and providing coherent standards for prevention, incident response, recovery, and the protection of taxpayers' constitutional rights within the digital tax administration system.

The fragmentation of these regulatory frameworks creates significant legal uncertainty in practice. When taxpayer data breaches occur, there is no clear legal basis for determining which regulatory regime should govern the resolution of the incident. It remains uncertain whether such cases should be addressed under the tax confidentiality provisions of the Law on General Provisions and Tax Procedures (UU KUP), the personal data protection mechanisms established by Law No. 27 of 2022 on Personal Data Protection (UU PDP), the electronic system security framework under the Electronic Information and Transactions Law (UU ITE) and Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions, or the principles of governmental accountability derived from administrative law. This normative ambiguity weakens the legal position of taxpayers as data subjects because their rights to receive timely breach notifications, obtain information regarding the nature and scope of compromised data, access risk mitigation measures, submit complaints, and seek restitution or compensation are not regulated within a unified legal framework.

The findings of this study reinforce those of Widayanti et al., who argue that Indonesia's cyber law framework remains fragmented and is characterized by overlapping institutional authority and inadequate interagency coordination.[17] They also support the conclusions of Alfajri and Najicha, who identified structural deficiencies in the governance of the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik or SPBE), particularly the weak legal foundation of the system and the limited supervisory authority of the National Cyber and Crypto Agency (Badan Siber

[17] Widayanti et al., "Enhancing Cybersecurity and Legal Integration."

dan Sandi Negara or BSSN).[18] Furthermore, the present study corroborates the findings of Satoto and Santiago, who emphasize the need to harmonize Indonesia's cyber law framework to address increasingly sophisticated digital threats.[19] Unlike previous studies, however, this research specifically maps the normative fragmentation governing taxpayer data protection and demonstrates that the principal challenge lies not in the absence of legislation, but in the lack of integration among the existing legal regimes.

Addressing this fragmentation requires a systematic approach to legal interpretation consistent with the theory advanced by Mertokusumo, which views legal norms as components of a unified legal system that should be interpreted harmoniously rather than in isolation.[20] Under this approach, the four relevant legal regimes should not be applied as alternative or mutually exclusive sources of law; instead, they should operate cumulatively and complement one another. Constitutional law provides the normative foundation by guaranteeing the fundamental rights of citizens. The Personal Data Protection Law establishes the rights of data subjects and the obligations of data controllers. The Law on General Provisions and Tax Procedures safeguards the confidentiality of taxpayer information. Meanwhile, the Electronic Information and Transactions Law and Government Regulation No. 71 of 2019 regulate the security, reliability, and governance of electronic systems. Applying these legal frameworks cumulatively creates a more comprehensive system of legal protection because each addresses a distinct dimension of taxpayer data governance while collectively supporting a coherent accountability framework.

Accordingly, the principal weakness of Indonesia's legal framework is not the lack of legal instruments governing taxpayer data protection, but rather the fragmentation of those instruments and the absence of an integrated mechanism for state accountability in the event of taxpayer data breaches. This study therefore argues that taxpayer data protection should be reconstructed through the harmonization of the 1945 Constitution of the Republic of Indonesia, the Personal Data Protection Law, the Law on General Provisions and Tax Procedures, the Electronic Information and Transactions Law, and Government Regulation No. 71 of 2019. Such harmonization would establish a multilayered legal protection framework in which these legal regimes operate cumulatively rather than independently. This integrated approach provides the conceptual foundation for the proposed cyber-restorative state accountability framework, under which the state assumes comprehensive responsibility for preventing data breaches, ensuring cybersecurity, responding effectively to incidents, restoring affected individuals' rights, and strengthening public trust in digital tax administration.

---

[18] Alfajri and Najicha, "Legal Reconstruction of Accountability for the Security of Electronic-Based Government Systems Based on the Principles of Good Governance."

[19] Satoto and Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption."

[20] Sudikno Mertokusumo, *Penemuan Hukum: Sebuah Pengantar*, 6th ed. (Liberty, 2009).

Only through the integration of these legal regimes can Indonesia achieve greater legal certainty, reinforce state accountability, and ensure effective protection of taxpayers' rights within the digital tax administration system.

3.3. State Accountability for Taxpayer Data Breaches from a Cyber Law Perspective

Law No. 27 of 2022 on Personal Data Protection (Personal Data Protection Law), Law No. 1 of 2024 amending the Electronic Information and Transactions Law (Electronic Information and Transactions Law), Government Regulation No. 71 of 2019 concerning the Operation of Electronic Systems and Transactions, and the principles of administrative law collectively demonstrate that the state's role in the governance of taxpayer data is multifaceted. First, the state acts as the fiscal authority constitutionally empowered to collect and process taxpayer data in order to perform its public revenue function. Second, through the Directorate General of Taxes (DGT), the state serves as the data controller because it determines the purposes and means of processing taxpayer information. Third, the state also functions as the operator of a public electronic system and is therefore legally obligated to ensure that the digital tax administration system is reliable, secure, and accountable. These overlapping institutional roles give rise to a corresponding framework of multilayered state accountability, under which the state's legal responsibilities are cumulative and cannot be separated from one another.

Traditionally, taxpayer data breaches have been viewed primarily as the consequence of malicious acts committed by hackers or other external actors. From a cyber law perspective, however, a data breach constitutes a legal event that reflects not only the conduct of third parties but also the effectiveness of the cybersecurity governance framework established by the state. Accordingly, an assessment of state accountability should not be limited to identifying the perpetrators of cyberattacks. It must also evaluate whether the state fulfilled its legal obligations to implement appropriate organizational, technical, and administrative safeguards capable of preventing, detecting, mitigating, and responding to cybersecurity incidents.

This analysis is consistent with Lessig's theory that "code is law," which posits that the architecture of digital systems shapes user behavior, determines the level of cybersecurity risk, and influences the effectiveness of legal protection in cyberspace.[21] Viewed through this theoretical lens, the protection of taxpayer data cannot be achieved solely through legal norms prohibiting tax officials from disclosing confidential information. Rather, those legal obligations must be translated into secure system architecture incorporating appropriate cybersecurity controls, including strong access controls, multi-factor authentication, comprehensive audit logs, continuous monitoring,

[21] Lawrence Lessig, *Code: And Other Laws of Cyberspace* (Basic Books, 1999).

anomaly detection, periodic security assessments, and effective incident response mechanisms. Consequently, state accountability under cyber law is expressed not only through statutory regulation but also through the design, implementation, and continuous maintenance of a secure digital infrastructure capable of protecting taxpayer data throughout its lifecycle.

The Personal Data Protection Law reinforces this obligation by requiring data controllers to implement adequate technical and organizational measures to ensure the security of personal data. Article 35 requires personal data controllers to safeguard personal data through appropriate technical and operational protections. Article 46 establishes the obligation to notify affected data subjects in the event of a personal data breach, while Article 47 requires data controllers to demonstrate compliance with the principles governing personal data protection. Complementing these provisions, the Electronic Information and Transactions Law and Government Regulation No. 71 of 2019 require electronic system operators to maintain information systems that are reliable, secure, and accountable, thereby establishing the legal foundation for cybersecurity governance within Indonesia's digital public administration.

Accordingly, the standard of state accountability in digital tax administration should not be determined solely by whether a cyberattack was perpetrated by external actors. Rather, it should be assessed based on whether the state exercised the level of digital due diligence required by law. This standard encompasses the implementation of appropriate cybersecurity governance, effective risk management, continuous monitoring, and adequate technical safeguards to protect taxpayer data. A failure to implement these mandatory security measures may give rise to state accountability even where the immediate cause of a data breach is a third-party cyberattack.

These findings extend the analysis presented by Nurmala and Wiraguna, who characterize the Directorate General of Taxes as the data controller under the Personal Data Protection Law and therefore administratively accountable for taxpayer data breaches resulting from violations of the principle of accountability.[22] While that characterization is legally sound, the present study advances a broader conceptual framework by identifying the state itself—rather than the Directorate General of Taxes alone—as the primary subject of legal accountability. Within this framework, state accountability extends beyond compliance with the Personal Data Protection Law to encompass the constitutional obligation to safeguard the rights to privacy and personal data protection, the administrative duty to ensure the secure operation of public electronic systems, and the broader responsibility to maintain public trust in the integrity, reliability, and security of Indonesia's digital tax administration system.

[22] Nurmala and Wiraguna, "Analisis Yuridis Tanggung Jawab Direktorat Jenderal Pajak (DJP) Terhadap Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) Berdasarkan Undang-Undang Nomor 27 Tahun 2022."

This analysis further reinforces the findings of Satoto and Santiago and Widayanti et al., both of whom emphasize the need to reform Indonesia's national cyber law framework through stronger cybersecurity governance and enhanced institutional coordination.[23] However, the present study argues that cyber law reform must be accompanied by a fundamental reconstruction of the concept of state accountability. The state cannot avoid legal responsibility merely by asserting that a taxpayer data breach resulted from an external cyberattack. Rather, it must be able to demonstrate that all reasonable and appropriate organizational, technical, and administrative safeguards were effectively implemented. This approach reflects the principle of digital due diligence, which imposes a legal obligation on the state to proactively prevent, identify, assess, and mitigate cybersecurity risks before they result in harm.[24]

The concept of state accountability proposed in this study does not impose a regime of strict or absolute liability. Instead, the state retains the opportunity to demonstrate that it exercised due diligence by implementing preventive measures, maintaining adequate cybersecurity safeguards, and adopting appropriate incident mitigation strategies consistent with applicable legal and technical standards. Nevertheless, because the state collects, controls, and processes taxpayer data pursuant to its public authority, the standard of care expected of public institutions must be higher than that imposed on private-sector data controllers. Accordingly, the state cannot simply attribute a taxpayer data breach to the actions of third parties where deficiencies in system architecture, cybersecurity governance, security oversight, or risk management materially contributed to the incident. From a cyber law perspective, the focus of legal accountability therefore shifts from identifying the immediate perpetrator of the attack to evaluating whether the state established and maintained an adequate framework for electronic system security and cybersecurity governance.

Within this framework, state accountability for taxpayer data breaches encompasses three interrelated dimensions. First, preventive accountability requires the state to establish an effective protection system before a breach occurs. This obligation includes implementing recognized information security standards, conducting periodic security audits, adopting comprehensive cybersecurity risk management practices, providing continuous cybersecurity training for personnel, and strengthening institutional cybersecurity governance. Second, procedural accountability requires the state to respond appropriately once a suspected data breach has occurred by conducting timely verification and investigation, notifying affected taxpayers without undue delay, providing transparent and accurate information regarding the incident, and coordinating

---

[23] Satoto and Santiago, "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption"; Widayanti et al., "Enhancing Cybersecurity and Legal Integration."

[24] Luke Chircop, "A Due Diligence Standard of Attribution in Cyberspace," *International and Comparative Law Quarterly* 67, no. 3 (2018): 643–68, https://doi.org/10.1017/S0020589318000015.

with relevant supervisory and law enforcement authorities. Third, restorative accountability requires the state to remedy the consequences of a data breach by providing risk mitigation assistance, ensuring accessible and effective complaint mechanisms, restoring compromised systems, rehabilitating the rights of affected data subjects, and providing compensation where losses are attributable to failures in the operation or governance of electronic systems.

This multidimensional framework reflects a model of active state accountability, which extends beyond the traditional passive obligation to preserve the confidentiality of taxpayer information.[25] Under this approach, the state's responsibility encompasses the entire lifecycle of taxpayer data governance, including prevention, preparedness, incident response, recovery, and the restoration of affected individuals' legal rights. This paradigm shift provides the normative foundation for the proposed cyber-restorative state accountability framework, under which the state, as the operator of the digital tax administration system, bears legal responsibility not only before and during a cybersecurity incident but also after the incident through effective remedial and recovery mechanisms.

Accordingly, taxpayer data protection in the era of digital transformation can no longer depend solely on statutory provisions prohibiting the disclosure of confidential tax information. Effective protection requires the state to establish a comprehensive cybersecurity governance framework grounded in the principles of legal certainty, accountability, transparency, digital due diligence, and the constitutional protection of fundamental rights. These findings further demonstrate that the success of digital tax administration should not be evaluated solely in terms of administrative efficiency or technological innovation. Rather, it must also be measured by the state's capacity to ensure the security, integrity, and resilience of taxpayer data while maintaining public confidence in the digital tax administration system.

3.4. Cyber-Restorative State Accountability Framework: Reconstructing State Responsibility for Taxpayer Data Breaches

The 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, the Law on General Provisions and Tax Procedures, the Electronic Information and Transactions Law, and Government Regulation No. 71 of 2019 collectively establish a substantial legal foundation for the protection of taxpayer data. However, these legal instruments have evolved within distinct regulatory regimes, each pursuing different normative objectives. The Law on General Provisions and Tax Procedures primarily emphasizes the confidentiality obligations of tax officials; the Personal Data Protection Law focuses on protecting the rights of data subjects and

[25] "The State's Positive Obligation to Ensure Personal Data Protection," *GRUR International* 74, no. 5 (2025): 501–4, https://doi.org/10.1093/grurint/ikaf018.

ensuring the accountability of data controllers; whereas the Electronic Information and Transactions Law and Government Regulation No. 71 of 2019 are principally concerned with the security, reliability, and governance of electronic systems.

As a consequence, when taxpayer data breaches occur, no single legal framework comprehensively integrates these overlapping obligations into a coherent system of state accountability. This regulatory gap cannot be remedied merely by introducing additional provisions into individual statutes. Instead, it requires a fundamental reconstruction of the paradigm of state accountability capable of harmonizing these legal regimes within a unified and comprehensive framework.

This study therefore proposes a cyber-restorative state accountability framework based on the premise that taxpayer data constitute sensitive personal data processed under the authority of the state in the exercise of its public functions. Because taxpayer information is collected and processed pursuant to public authority, the state is subject to a higher standard of care than private-sector data controllers. Consequently, the state's responsibilities extend beyond preserving the confidentiality of taxpayer information under Article 34 of the Law on General Provisions and Tax Procedures. They also encompass safeguarding the entire lifecycle of taxpayer data through the application of the principles of lawfulness, accountability, security, transparency, proportionality, and digital due diligence. Accordingly, the proposed framework rejects the traditional separation between tax law, personal data protection law, and cyber law. Instead, it conceptualizes these legal regimes as complementary components of an integrated system of legal protection. The proposed cyber-restorative state accountability framework is structured around five interrelated pillars.

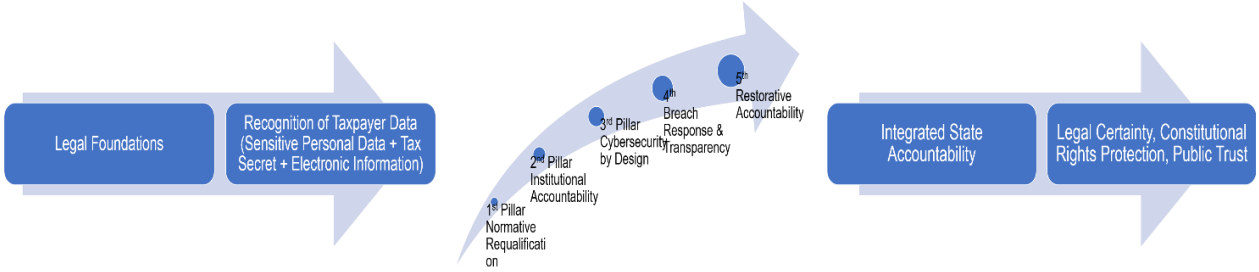

Figure 1. Cyber-Restorative State Accountability Framework for Taxpayer Data Protection in Digital Tax Administration

The first pillar is normative requalification, which recognizes taxpayer data as simultaneously constituting personal data, confidential tax information, and electronic information. This reconceptualization is essential because it eliminates the artificial distinction between the protection of taxpayer information under tax law and the protection of personal data under privacy law (Navarro-Schiappacasse et al., 2023). Under this approach, all processing of taxpayer data must comply cumulatively with the requirements of the Law on General Provisions and Tax Procedures, the Personal Data

Protection Law, and the legal framework governing electronic systems. Consequently, taxpayer data protection is no longer grounded exclusively in the doctrine of official confidentiality but is instead recognized as an integral component of the constitutional protection of privacy, personal data security, and legal certainty.

The second pillar is the reconstruction of the subject of accountability. The Directorate General of Taxes simultaneously performs three distinct legal functions: it acts as the national tax authority, serves as the controller of taxpayer personal data, and operates a public electronic information system. These overlapping institutional roles require a corresponding reconstruction of legal accountability. Responsibility for taxpayer data governance should not be imposed solely upon individual officials or technical system operators. Rather, because all taxpayer data are processed pursuant to public authority, accountability must ultimately rest with the state itself. This reconstruction expands the traditional concept of official confidentiality into a broader framework of institutional accountability, encompassing organizational governance, cybersecurity risk management, internal oversight, regulatory compliance, and the implementation of effective technical and organizational security controls. Such an approach reflects contemporary principles of cyber law, under which accountability is assessed not only by the conduct of individual actors but also by the effectiveness of institutional governance and the resilience of the digital infrastructure responsible for protecting sensitive personal information.

The third pillar is cybersecurity by design, which reflects the state's obligation to incorporate security measures into the digital tax administration system from the earliest stages of its development. Under this principle, cybersecurity is embedded into the system architecture rather than implemented as a reactive measure after deployment. As Lessig argues, the effectiveness of legal protection in cyberspace is fundamentally influenced by the architecture of digital systems.[26] Consequently, the protection of taxpayer data cannot rely solely on administrative policies or post hoc security measures but must be integrated into the design and operation of the digital tax administration system itself. The implementation of this principle includes the adoption of multi-factor authentication, data encryption, risk-based access controls, comprehensive audit trails, automated anomaly detection, periodic penetration testing, risk-based classification of taxpayer data, and independent cybersecurity audits conducted on a regular basis. Compared with regulatory models that depend primarily on statutory prohibitions against unauthorized disclosure, a security-by-design approach provides a more effective and sustainable mechanism for protecting taxpayer data against evolving cyber threats.

The fourth pillar is breach response and transparency, which requires the state to establish effective mechanisms for incident notification, investigation, risk

[26] Lessig, *Code: And Other Laws of Cyberspace*.

communication, and public transparency whenever a taxpayer data breach occurs.[27] One of the principal shortcomings of Indonesia's current legal framework is the absence of detailed procedures governing the notification of affected taxpayers regarding the categories of compromised data, the potential risks arising from the breach, recommended mitigation measures, and the progress of official investigations. Although the Personal Data Protection Law requires data controllers to notify data subjects following a personal data protection failure, the proposed cyber-restorative state accountability framework extends this obligation by requiring a transparent, timely, and measurable breach notification system. Such a framework enhances public accountability, enables affected individuals to take appropriate protective measures, and strengthens public confidence in the integrity of digital tax administration.

The fifth pillar is restorative accountability, which recognizes the state's obligation to provide effective remedies to taxpayers whose rights have been adversely affected by data breaches. Under the existing Indonesian legal framework, post-breach enforcement primarily focuses on imposing administrative sanctions upon data controllers, while the legal rights and remedies available to affected taxpayers remain inadequately regulated. The proposed framework therefore positions restorative accountability as an essential component of state responsibility rather than a supplementary or discretionary measure.

Within this framework, restorative measures include the provision of identity theft prevention and mitigation services, accessible and effective complaint mechanisms, continuous monitoring to prevent the misuse of compromised taxpayer data, the restoration of data subjects' legal rights, and compensation where material or non-material harm can be demonstrated to have resulted from failures in the operation or governance of electronic systems. Consequently, the proposed model shifts the orientation of state accountability from a predominantly punitive or regulatory approach toward a restorative model that prioritizes the protection of citizens' rights, the remediation of harm, and the restoration of public trust.

Comparative experience further supports the proposed framework. The European Union's General Data Protection Regulation (GDPR) integrates data processing principles, cybersecurity requirements, mandatory breach notification, and the right to compensation within a single, coherent legal framework. Similarly, Singapore's Personal Data Protection Act 2012 establishes an integrated system that connects organizational accountability, mandatory breach notification, and regulatory oversight into a unified data protection regime. Estonia likewise demonstrates that the successful digitalization of public services depends not only on comprehensive legislation but also on the development of secure, interoperable, transparent, and auditable digital infrastructure. The experience of these jurisdictions illustrates that effective data protection is achieved

[27] Hamzah Haikal Riziq Alwi Alatas and Gunawan Djajaputra, "Examining Indonesian Government Accountability And Mitigation Measures In The 2024 Taxpayer Identification Number Data Breach," *Jurnal Ilmu Hukum Kyadiren* 7, no. 2 (2025): 1234–48, https://doi.org/10.46924/jihk.v7i2.385.

through the integration of legal norms, institutional governance, and technological architecture rather than through isolated regulatory measures. These comparative models therefore provide valuable guidance for reconstructing Indonesia's legal framework governing taxpayer data protection and for developing a comprehensive cyber-restorative state accountability framework capable of addressing the legal and technological challenges of digital tax administration.

This study further extends the work of Widayanti et al., who emphasize the need for comprehensive reform of Indonesia's national cyber law framework,[28] Alfajri and Najicha, who advocate strengthening the governance of the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik or SPBE),[29] and Nurmala and Wiraguna, who identify the Directorate General of Taxes (DGT) as the data controller under the Personal Data Protection Law. Unlike these earlier studies,[30] the present research not only identifies the regulatory deficiencies underlying taxpayer data protection but also develops a novel conceptual framework that integrates tax law, administrative law, personal data protection law, and cyber law into a unified and operational model of state accountability.

Within this framework, taxpayer data breaches should no longer be understood merely as violations of official confidentiality. Rather, they should be recognized as failures of state cybersecurity governance. Accordingly, the assessment of state accountability should no longer depend solely on evidence that public officials unlawfully disclosed confidential taxpayer information. Instead, accountability should be evaluated according to whether the state has satisfied the requirements of digital due diligence, namely the legal standard requiring measurable and effective implementation of preventive safeguards, cybersecurity controls, institutional oversight, incident response, and post-incident recovery. This approach represents a fundamental shift in legal doctrine by relocating the focus of accountability from the conduct of individual officials to the quality, effectiveness, and resilience of the electronic systems and cybersecurity governance established by the state.

The proposed framework therefore positions the state as the steward of taxpayer data and imposes upon it a comprehensive legal obligation to prevent cybersecurity incidents, strengthen digital security, provide timely breach notification, conduct transparent investigations, restore compromised electronic systems, rehabilitate the rights of affected taxpayers, and provide compensation where legally cognizable losses have been established. Consequently, state accountability should no longer be measured solely by whether public officials disclose confidential taxpayer information, but by

---

[28] Widayanti et al., "Enhancing Cybersecurity and Legal Integration."

[29] Alfajri and Najicha, "Legal Reconstruction of Accountability for the Security of Electronic-Based Government Systems Based on the Principles of Good Governance."

[30] Nurmala and Wiraguna, "Analisis Yuridis Tanggung Jawab Direktorat Jenderal Pajak (DJP) Terhadap Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) Berdasarkan Undang-Undang Nomor 27 Tahun 2022."

whether the state has exercised the level of digital due diligence required in the governance and operation of the digital tax administration system.

The findings of this study have both theoretical and practical implications. From a theoretical perspective, they establish a conceptual bridge among tax law, administrative law, personal data protection law, and cyber law by integrating these previously fragmented legal regimes into a single and coherent framework of state accountability. From a practical perspective, the proposed framework underscores the need for implementing regulations that establish clear cybersecurity standards for taxpayer data, risk-based classifications of taxpayer information, mandatory periodic cybersecurity audits, standardized data breach notification procedures, accessible taxpayer complaint mechanisms, procedures for restoring the rights of affected individuals, and transparent rules governing compensation for material and non-material harm. Accordingly, the proposed cyber-restorative state accountability framework contributes not only to the advancement of cyber law scholarship in Indonesia but also provides a normative blueprint for legal reform aimed at strengthening legal certainty, enhancing state accountability, and restoring public confidence in the country's digital tax administration system.

4. CONCLUSION

Taxpayer data possess a dual legal status as sensitive personal data, confidential tax information, and electronic information, thereby receiving cumulative legal protection under the 1945 Constitution of the Republic of Indonesia, Law No. 27 of 2022 on Personal Data Protection, the Law on General Provisions and Tax Procedures, and the legal framework governing the operation of electronic systems. Despite this multilayered protection, the existing regulatory framework remains fragmented, resulting in legal uncertainty concerning the scope and implementation of state accountability in the event of taxpayer data breaches.

This study argues that the existing paradigm of state responsibility should be reconstructed from one centered on official confidentiality to a cyber-restorative state accountability framework that integrates preventive obligations, cybersecurity governance, breach notification, incident investigation, system recovery, restoration of taxpayers' rights, and compensation for demonstrable losses. The study contributes to legal scholarship by integrating tax law, administrative law, personal data protection law, and cyber law into a unified framework of state accountability for digital tax administration. From a practical perspective, the proposed framework provides a normative foundation for developing cybersecurity standards applicable to digital tax administration.

This research is limited by its reliance on a normative legal methodology and therefore does not empirically evaluate the effectiveness of the Directorate General of Taxes' cybersecurity governance or the practical implementation of the proposed

framework. Accordingly, the Indonesian government should develop implementing regulations establishing technical standards for taxpayer data security, mandatory cybersecurity audits, standardized breach notification procedures, post-incident recovery mechanisms, and compensation schemes for individuals affected by taxpayer data breaches. Future research should adopt empirical and comparative methodologies to assess the effectiveness of implementing the proposed cyber-restorative state accountability framework within Indonesia's digital tax administration system.

REFERENCES

Journals

Acev, David, Sankalp Biyani, Florian Rieder, et al. "Systematic Analysis of Data Governance Frameworks and Their Relevance to Data Trusts." *Management Review Quarterly*, ahead of print, July 31, 2025. https://doi.org/10.1007/s11301-025-00545-1.

Aghna, Naura Atania Putri. "Kepastian Hukum Keamanan Data Pribadi Wajib Pajak Dalam Pembayaran Pajak Secara Digital." *Jurnal Hukum Indonesia* 5, no. 2 (2026): 165–73. https://doi.org/10.58344/jhi.v5i2.2530.

Alatas, Hamzah Haikal Riziq Alwi, and Gunawan Djajaputra. "Examining Indonesian Government Accountability And Mitigation Measures In The 2024 Taxpayer Identification Number Data Breach." *Jurnal Ilmu Hukum Kyadiren* 7, no. 2 (2025): 1234–48. https://doi.org/10.46924/jihk.v7i2.385.

Chircop, Luke. "A Due Diligence Standard of Attribution in Cyberspace." *International and Comparative Law Quarterly* 67, no. 3 (2018): 643–68. https://doi.org/10.1017/S0020589318000015.

Dirgantara, Febrian, Dharma Setiawan Negara, Didit Darmawan, Endra Andie Aryanto, and Alwi Mohamad Shahab. "Legal Responsibility of Companies in Cases of Personal Data Breaches." *Innovative: Journal of Social Science Research* 5, no. 1 (2025): 5053–65. https://doi.org/10.31004/innovative.v5i1.18046.

Huda, Uu Nurul, Tatang Astarudin, Muhammad Irsan Nasution, Ahmad Abdul Khozin, and Muhammad Irsan. "Legal Protection for Personal Data Leaks and Its Implications for Citizens' Privacy Rights Within The Framework of The Indonesian Legal State." *Jambura Law Review* 1, no. 1 (2026): 144–59. https://doi.org/10.33756/jlr.v1i1.32666.

Judijanto, Loso. "Protection of Taxpayer Personal Data in Tax Administration: A Review." *Digital Business: Tren Bisnis Masa Depan* 15, no. 3 (2024): 185–94.

Nurmala, Salma Ayu, and Sidi Ahyar Wiraguna. "Analisis Yuridis Tanggung Jawab Direktorat Jenderal Pajak (DJP) Terhadap Kebocoran Data Nomor Pokok Wajib Pajak (NPWP) Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Kajian Ilmiah* 26, no. 1 (2026): 85–94. https://doi.org/10.31599/207r0b59.

Satoto, Endro, and Faisal Santiago. "Reconstruction of Indonesia's Cyber Law System for Adaptive and Integrated Digital Crime Prevention in the Era of Technological Disruption." *Greenation International Journal of Law and Social Sciences* 3, no. 2 (2025): 309–17. https://doi.org/10.38035/gijlss.v3i2.425.

"The State's Positive Obligation to Ensure Personal Data Protection." *GRUR International* 74, no. 5 (2025): 501–4. https://doi.org/10.1093/grurint/ikaf018.

Widayanti, Tri Fenny, Aditya Dwi Rohman, A. Nuril Zamharir Haris, Eka Merdekawati Djafar, and Muhammad Zulfan Hakim. "Enhancing Cybersecurity and Legal Integration: Reforming Indonesia's Cyber Law to Foster Sustainable Growth in the Digital Economy." *Diponegoro Law Review* 10, no. 1 (2025): 105–19. https://doi.org/10.14710/dilrev.10.1.2025.105-119.

Zhang, Yanlei. "Data Breach Disclosure Laws and Corporate Tax Planning Activities." *Journal of International Accounting, Auditing and Taxation* 60 (2026): 100749. https://doi.org/10.1016/j.intaccaudtax.2026.100749.

Proceedings

Alfajri, Farhan Zaidan, and Fatma Ulfatun Najicha. "Legal Reconstruction of Accountability for the Security of Electronic-Based Government Systems Based on the Principles of Good Governance." In *Proceedings of the International Conference on Democracy and National Resilience 2025 (ICDNR 2025)*, vol. 981, edited by Sunny Ummul Firdaus, Gayatri Dyah Suprobowati, R. Prihandjojo Andri Putranto, et al. Advances in Social Science, Education and Humanities Research. Atlantis Press SARL, 2025. https://doi.org/10.2991/978-2-38476-529-4_12.

Books

Lessig, Lawrence. *Code: And Other Laws of Cyberspace*. Basic Books, 1999.

Mertokusumo, Sudikno. *Penemuan Hukum: Sebuah Pengantar*. 6th ed. Liberty, 2009.

Rahayu, Siti Kurnia. *Keamanan Digital Dalam Audit Pajak: Integrasi Cyber Security Dengan CRM, BDA, Dan BI Untuk Revolusi Compliance*. Unikom Press, 2024.

Webpages

Marwah, Hanin. "6 Juta Data NPWP Bocor: Diduga Milik Jokowi, Sri Mulyani, Dan Zulhas, Diperjualbelikan Seharga Rp 152 Juta." *Tempo*, 2024. https://www.tempo.co/ekonomi/6-juta-data-npwp-bocor-diduga-milik-jokowi-sri-mulyani-dan-zulhas-diperjualbelikan-seharga-rp-152-juta-8164.