Journal of International Islamic Law, Human Rights, and Public Policy
(JISHUP Journal) | ISSN(e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volume 4 No. 3 (2026)

REFORMULATION OF TAX AND CYBER LAW: TOWARDS INTELLECTUAL PROPERTY-FRIENDLY DIGITAL TRANSACTION OVERSIGHT

Irwansyah Tanjung[1], Misnan Al-Jawi[2]
[1]Universitas Al-Azhar, Medan, Indonesia. [2]Uninversitas Alwasliyah, Medan, Indonesia.
Email: [1]irwansya.tg@gmail.com, [2]misnanaljawi32@gmail.com

Received: 05/06/2026 | **Revised:** 11/06/2026 | **Accepted:** 25/06/2026 | **Published:** 05/07/2026

Abstract

This study analyzes the legal tension between data extraction authority within digital tax oversight in Indonesia and taxpayers' rights to trade secret protection. The implementation of the Core Tax Administration System (Coretax) and the Artificial Intelligence Compliance System (AICEco) proses risks of disclosing technological data and internal corporate financial information due to the absence of comprehensive technical regulations. Employing a normative legal research method coupled with a comparative approach, this study examines the tax and cyber legal frameworks in the United States, Germany, and Australia. The findings indicate that regulations in Indonesia lack integration regarding digital evidence management compared to the United States, which implements protective orders, and Germany, which aligns fiscal audits with the boundaries of the General Data Protection Regulation (GDPR). This study recommends the reformulation of national tax policy, encompassing the institutionalization of the Tax Control Framework (TCF), the adoption of protective order provisions within tax court procedural law, encryption standardization in third-party partnership system sandboxing, and the optimization of the *dominus litis* principle by the Public Prosecution Service to guarantee legal certainty and the protection of taxpayers' intellectual property rights.

Keywords: Taxation; Cyber; Secrecy; Comparative.

INTRODUCTION

The global economic and trade order is undergoing structural transformation as a result of the penetration of digitalization. Conventional business models that historically relied on a physical presence (brick-and-mortar) are being gradually replaced by cross-jurisdictional digital business models operating through e-commerce platforms, cloud computing services, and artificial intelligence algorithms. This transitional phenomenon, as defined by multilateral institutions such as the Asian Development Bank and the International Monetary Fund, shifts the parameters of value creation from labor-intensive and capital-intensive sectors toward knowledge-intensive sectors driven by intangible assets (Mullins, 2022). These economic dynamics in turn present a dual challenge to the legal and fiscal sovereignty of nations, including the Republic of Indonesia.

On one hand, state instruments are required to prevent base erosion and profit shifting (BEPS). This cross-border tax avoidance practice is facilitated by the highly mobile nature of intangible assets, enabling multinational enterprises (MNEs) to shift their profit base to low-tax jurisdictions (tax havens) without relocating their real economic activities (EY, 2015). The fundamental difficulty experienced by tax authorities worldwide stems from the absence of traditional parameters, such as a permanent establishment as required under classical double taxation treaties (EY, 2015). On the other hand, the national legal regime is also faced with the need to continuously adapt to attract and protect investments in the information technology sector. A conducive investment climate in the era of a knowledge-based economy requires certainty in the protection of intellectual property rights (IPR), particularly trade secrets, which are recognized as fundamental assets driving innovation in technology companies (Hudson, 2024).

The Government of the Republic of Indonesia has responded to these digital economic dynamics through a series of regulatory reforms. Specifically, the enactment of Presidential Regulation No. 68 of 2025 on the Tax Collection System for Foreign Digital Transactions (PR 68/2025) marks a strategic state intervention to accelerate and secure Value Added Tax (VAT) revenue from foreign digital service providers (Assegaf Hamzah & Partners,

n.d.). This regulation mandates the establishment of a centralized technological instrument designated as the Foreign Digital Transaction Tax Collection System (SPP-TDLN). The operation of this system is delegated to PT Jalin Pembayaran Nusantara, an assigned entity tasked with automating the monitoring, data collection, and tax collection processes for every cross-border transaction in real time (Pajakku, n.d.-a). Additionally, tax administration within the Directorate General of Taxes (DGT) is undergoing comprehensive modernization through the implementation of the Core Tax Administration System (Coretax) and the launch of the Artificial Intelligence Compliance Ecosystem (AICEco) (Aguspajak, n.d.). This transformation promotes a data-driven audit approach to precisely trace taxpayers' digital footprints.

Although these tax base broadening initiatives are crucial for the sustainability of the State Revenue and Expenditure Budget (APBN), the penetration of technology within tax oversight and audit processes simultaneously generates fundamental legal friction. An intersection occurs when the extractive authority of tax officials conflicts with data protection and intellectual property laws. Effective digital tax oversight, particularly in detecting the arm's length nature of affiliated transactions or transfer pricing, necessitates the authority's access to high-resolution transaction data, consumer behavior footprints, price formulation structures, database architectures, and an in-depth review of source code levels and pricing algorithms owned by taxpayers (Fiskusmagnews, n.d.). The arising legal issue is that pursuant to Law No. 30 of 2000 on Trade Secrets (Trade Secret Law), such a collection of information is legally classified and exclusively protected as intellectual property because it possesses high economic value and is consistently maintained in secrecy by its owner through appropriate measures (Tomo, 2020). Tax audit processes that employ administrative coercion to compel the submission of such sensitive data, if not accompanied by multi-layered cybersecurity protocols and legal guarantees of confidentiality equivalent to a court-issued protective order, risk triggering large-scale trade secret leaks (Kilpatrick, 2026).

Failure to reconcile and manage this asymmetry of legal interests not only potentially leads to prolonged administrative disputes and judicial litigation, but essentially risks creating a global perception that Indonesia's investment climate is hostile to technological innovation. A phenomenon wherein the state forcefully extracts intellectual property information without adequate protection can be construed as a form of regulatory expropriation or indirect seizure of intellectual assets (Fiskusmagnews, n.d.). Therefore, a thorough analysis of this legal intersection is essential. This study comprehensively delineates the crucial dimensions concerning the urgency of reformulating tax and cyber law in Indonesia. The primary focus of this analysis is to design a legal construct for digital transaction oversight mechanisms that not only operate effectively to secure state revenue for fiscal justice, but simultaneously provide protection and legal certainty for taxpayers' intellectual property rights and trade secrets amidst the era of cloud computing and artificial intelligence.

METHOD

This study employs a normative legal research method to analyze regulatory lacunae and legal disparities within digital transaction oversight and the protection of taxpayers' trade secrets. The approaches utilized include a statutory approach and a comparative approach. The statutory approach reviews tax regulations, cyber law, and trade secret legislation in Indonesia, while the comparative approach evaluates the legal frameworks and judicial practices of the United States, Germany, and Australia to identify a legal governance model applicable nationally.

The legal materials utilized in this study consist of primary and secondary legal materials. Primary legal materials encompass Law No. 30 of 2000 on Trade Secrets, the Electronic Information and Transactions Law, the Personal Data Protection Law, and related tax regulations. Secondary legal materials are sourced from scholarly literature, accredited national and international law journals, and global tax policy reports. These legal materials were gathered through library research and subsequently analyzed using a qualitative-normative method combined with deductive reasoning to formulate prescriptive conclusions regarding the reformulation of digital fiscal policy in Indonesia.

RESULTS AND DISCUSSION

A. Legal Framework of Digital Tax Oversight, Cybersecurity, and Trade Secret Protection in Indonesia

The legal regulation of the digital economy in Indonesia is based on various regulations governing the validity of transactions and the balance of rights and obligations between parties. Law No. 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law (EIT Law) provides legal certainty for obligations within cyberspace, including the validity of electronic contracts (e-contracts), the obligation to maintain personal data confidentiality, and the admissibility of electronic evidence in judicial proceedings (Kusuma & Partners Law

Firm, 2025). Additionally, trading activities through electronic systems are specifically regulated under Government Regulation No. 80 of 2019 on Trading Through Electronic Systems (GR PMSE). Implementing provisions of this regulation require all electronic commerce (e-commerce) entities, whether domestic or foreign operating within Indonesian jurisdiction, to register their business licenses through the Business License for Trading Through Electronic Systems (SIUPMSE) mechanism (Kusuma & Partners Law Firm, 2025).

Apart from business licensing and consumer protection aspects, these regulations encompass legal liability burdens concerning intellectual property rights infringements. Pursuant to Article 10 of Law No. 28 of 2014 on Copyright, e-marketplace platform providers bear attributable legal liability to prevent, block, and prohibit the sale or reproduction of copyright-infringing goods within their managed platforms (Putri Aldina, 2023). These regulations serve to foster digital economic growth through facilitative legal instruments, while simultaneously providing preventive and repressive intellectual property rights protection against cybercrimes, such as data theft or trademark counterfeiting (Kusuma & Partners Law Firm, 2025).

Within the development of cyber tax law, Presidential Regulation No. 68 of 2025 regulates the Value Added Tax (VAT) collection system for Foreign Digital Transactions (TDLN) entities (Hakim et al., 2025). In accordance with international consensus guidelines, this regulation categorizes TDLN as the utilization or exchange of intangible goods, services, or algorithmic information transacted cross-jurisdictionally using computer networks or other electronic media (Assegaf Hamzah & Partners, n.d.). Under this policy, tax jurisdiction is no longer grounded in the physical presence doctrine, but has shifted to the destination doctrine, namely the location of final consumption of the digital goods or services (Baker McKenzie, 2025).

The Tax Collection System for Foreign Digital Transactions (SPP-TDLN) is operated by a specially assigned business entity, namely PT Jalin Pembayaran Nusantara (PT PSI, 2025). The appointment of a third party outside the institutional structure of the tax authority as an aggregator aims to integrate real-time collection into the national payment system infrastructure and avoid duplicative hardware investment (Assegaf Hamzah & Partners, n.d.). Delegating the management authority of large-scale commercial transaction data to such a third party necessitates applying the principle of strict liability within its governance system.

To guarantee this accountability, the technology partner is required to pass a sandboxing process encompassing testing for functionality, workload scalability capabilities, network architecture performance, cybersecurity compliance, Governance, Risk, and Compliance (GRC), conformity with the Personal Data Protection Law (PDP Law), system evaluation within a simulated isolated computing environment, and the standardization of operational procedures for logging, anomaly monitoring, and data analytics reporting (PT PSI, 2025). Administratively, the partner must be free from any record of sanctions or inclusion on blacklists within global jurisdictions, such as the Office of Foreign Assets Control (OFAC) or the Securities and Exchange Commission (SEC), and must have no conflict of interest with ministry officials (PT PSI, 2025). This entire appointment process is periodically evaluated by an inter-ministerial coordination team established pursuant to a Presidential Decree (Pajakku, n.d.).

Concurrent with the management of the SPP-TDLN focusing on VAT, the Directorate General of Taxes (DGT) integrates the Coretax system and the Artificial Intelligence Compliance Ecosystem (AICEco) to support compliance with Income Tax (PPh) and other tax categories (Aguspajak, n.d.). The Coretax system serves as a single source of truth that consolidates financial transaction data from institutions, agencies, associations, and third parties—such as banking, customs, insurance, and digital platforms—to construct centralized taxpayer compliance profiles (Aguspajak, n.d.). Meanwhile, AICEco functions as an analytical system to detect behavioral anomalies through the application of artificial intelligence algorithms, including identifying indications of the abuse of transfer pricing within cross-border affiliated transaction flows (Fiskusmagnews, n.d.).

The use of predictive algorithms and data mining in tax audits, termed the AI-Driven Tax Audit Model (ATAM), can reduce the subjectivity of tax auditors and improve the efficiency of state revenue collection (Valderrama, 2021). However, within the framework of a constitutional state (*rechtsstaat*), public law must establish legal boundaries regarding the extent to which the algorithmic authority of tax organs is permitted to access a taxpayer's internal systems. Cybersecurity law and the EIT Law No. 1 of 2024 fundamentally focus on the admissibility of digital evidence and the limits of legal liability within computer networks (Kusuma & Partners Law Firm, 2025). If tax audit algorithmic processes are executed without clear regulatory limitations, the potential over-collection of data—which may penetrate servers containing confidential corporate information—risks raising issues within cyber law and constitutional law (Awaisheh et al., 2025).

In principle, the Personal Data Protection Law (PDP Law) focuses on protecting the fundamental rights of individual data subjects (Pajakku, n.d.). However, in the context of large-scale digital businesses, collections of information regarding consumer preferences, search history, demographic tracks, and transaction behavior databases are frequently aggregated and compiled by corporations, thereby satisfying the legal classification of a trade secret. International and national legal instruments uniformly recognize that compilations of business information possessing economic value constitute an integral part of corporate intellectual property rights (Oroh et al., 2024). Alongside the increasing trend of automatic exchange of tax information across nations, such as through the Automatic Exchange of Information (AEOI) agreement, the implementation of the Common Reporting Standard (CRS), and mandatory Country-by-Country Reporting (CbCR), the operational financial information of multinational corporations has become more exposed (Nurbekova et al., 2026). This condition creates a digital vulnerability where legal tax compliance obligations intersect with the legal right to corporate asset protection. Large-scale transaction data (big data) risks hacking, leakage, or exfiltration when accessed by institutions with inadequate encryption systems, as well as within data management partnership schemes with external service providers (Fontanela et al., 2026).

This escalation of digital tax oversight generates a direct conflict of interest with the aspect of trade secret protection. Pursuant to Article 1 Paragraph 1 of Law No. 30 of 2000 on Trade Secrets, the normative definition of a trade secret is information unknown to the public in the fields of technology and/or business, possessing economic value because it is useful in business activities, and maintained in secrecy by its owner (Tomo, 2020). The statutory scope of protection covers production methods, processing methods, sales methods, database architectures, artificial intelligence algorithm designs (machine learning models), and the source code of commercial software (Law of the Republic of Indonesia No. 30 of 2000, 2000). The distinguishing characteristic of trade secrets compared to other intellectual property rights (IPR) regimes, such as copyright or patents, is the absence of a public registration element. While a patent requires an inventor to disclose the invention to the public to obtain a time-limited monopoly, the economic value of a trade secret relies on the principle of confidentiality (Fau & Verawaty, 2024). Article 3 of the Trade Secret Law emphasizes that information is deemed maintained in secrecy if the owner has taken appropriate and reasonable administrative and technical measures, such as implementing mandatory Non-Disclosure Agreements (NDAs) for employees, and adopting encryption protocols to restrict technological access by external parties (Iskandar, 2009).

Based on a Property Theory perspective on IPR, forced disclosure of confidential elements by state organs can result in the loss of competitive advantage. This situation risks causing irreparable harm, as information once exposed to the public cannot have its confidential status restored (Fontanela et al., 2026). The Trade Secret Law classifies the infringement of this exclusive right as a criminal offense. Pursuant to Article 17 of Law No. 30 of 2000, any person who intentionally and unlawfully uses or discloses the trade secret of another party for commercial purposes is subject to a criminal penalty of imprisonment for a maximum of two years and/or a maximum fine of Rp300,000,000.00 (Tomo, 2020).

Within cross-border tax administrative law, an enforcement focus is directed at addressing transfer pricing manipulation. Transfer pricing is a pricing mechanism for transactions involving the transfer of intangible goods, services, or financial instruments between multinational enterprise entities that share a special relationship. The abuse of this mechanism aims to achieve operational profit shifting toward low-tax jurisdictions (tax havens) (Irawan & Ulinnuha, 2022). Instruments utilized in these aggressive transfer pricing schemes include manipulating the value transfer of intangible assets, such as trademark licenses, copyright utilization, and trade secrets through royalty payment instruments (Irawan & Ulinnuha, 2022). To ensure that pricing schemes comply with the Arm's Length Principle (ALP), the DGT regulates documentation obligations through Minister of Finance Regulation No. 172 of 2023 (PMK 172/2023). This transfer pricing documentation reporting obligation requires taxpayers with gross turnover exceeding a specific threshold to prepare a Master File, a Local File, and a Country-by-Country Report (CbCR) (Fiskusmagnews, n.d.).

To conduct substantive reviews, the DGT adopts the global standard of the DEMPE (Development, Enhancement, Maintenance, Protection, and Exploitation) framework based on OECD guidelines (Fiskusmagnews, n.d.). This analytical framework is utilized by the tax authority to analyze the operational economic substance underlying the formal ownership of an IPR asset. In verifying claims regarding which affiliated entity funds and executes the development or enhancement process of software service algorithms (Software as a Service/SaaS) or digital business models, tax auditors may issue an administrative document request. This instrument requires taxpayers to grant access to algorithmic metrics and database management procedures, or to submit source code

blueprints for evaluation (Fiskusmagnews, n.d.). The relationship between the dimensions of the DEMPE framework and the risk impacts on trade secret assets is contained in Table 1.

Table 1: Correlation of DEMPE Framework Dimensions and Vulnerability Impacts on Trade Secret Assets.

DEMPE Analytical Approach Dimension	Relevance to Tax Audit Requirements (Audit Objective)	Risks to Intellectual Property Rights (Trade Secret Specific)
Development	Investigating the factual location and technical capabilities of the research team designing the algorithm.	Disclosure of source code development methodology, beta-version architecture, and early-stage proprietary know-how.
Enhancement	Analyzing update cost logs and efficiency optimization of computing programs or artificial intelligence.	Exposing the update logic and machine learning architectural framework.
Maintenance	Auditing the arm's length nature of transfer pricing for server maintenance and system patching allocations.	Exposure of internal network topology data and server vulnerabilities that could affect cybersecurity posture.
Protection	Verifying patent payments, NDA contracts, and IPR litigation costs proportionally.	Submission of unredacted client lists or exclusive third-party licensing contracts that include pricing confidentiality.
Exploitation	Assessing the entity deriving dominant economic benefits and the arm's length nature of pricing methods.	Disclosure of internal documents regarding profit margin projections and dynamic pricing algorithmic models.

Source: Compiled by the author (2026) based on the OECD Transfer Pricing Guidelines and Fiskusmagnews (n.d.).

This administrative document request is based under positive law on Article 29 of the Law on General Provisions and Tax Procedures (KUP Law), which authorizes tax auditors to inspect or borrow books, records, and documents during an audit (Aguspajak, 2022). However, tax auditors are not parties bound by commercial confidentiality contracts. These audit instruments can escalate to the authority of a Tax Criminal Investigation provided there is sufficient preliminary evidence. Pursuant to Minister of Finance Regulation No. 17 of 2025 (PMK 17/2025), investigators are authorized to seize hardware and access a taxpayer's server systems to gather evidence (Organisation for Economic Co-operation and Development, 2011). These seized digital assets carry security risks in the form of potential external cyber breaches during their retention in evidence storage, or risks of management negligence that could expose information to competitors (Fontanela et al., 2026).

Within the constitutional legal framework of taxation in Indonesia, the protection of taxpayers' sensitive information is governed by the instrument of Official Secrecy (*Rahasia Jabatan*) enshrined in Article 34 of the KUP Law (Maier, 2026). This provision requires every tax official, appointed external expert, or supporting agency to maintain the confidentiality of all matters known or disclosed by the taxpayer in the performance of their official duties (Maier, 2026). Nonetheless, the effectiveness of Article 34 of the KUP Law as an instrument to protect trade secrets for technology companies and multinational entities faces several structural weaknesses in the digital era.

The first weakness pertains to the lack of specificity in handling high-technology digital assets. The confidentiality provisions in Article 34 of the KUP Law were historically designed to anticipate physical documents, such as conventional financial statements or client identity lists. This regulation has not specifically governed the protection of encrypted server log data or the governance of handling autonomous computing algorithms (agentic AI algorithms) (Awaisheh et al., 2025). The absence of tax standard operating procedures (SOPs) restricting database copying, prohibiting reverse engineering, or banning algorithmic analysis outside corporate facilities generates risks to the protection of intellectual property rights (Law of the Republic of Indonesia No. 30 of 2000, 2000).

The second weakness is the expansion of inter-agency data transmission without being balanced by adequate data redaction mechanisms. Fulfilling tax administration currently expands the Exchange of Information, both on a domestic scale with other ministries or agencies—such as within the Coretax system integration and the delegation of authority in the SPP-TDLN sandboxing—and at the global level (Assegaf Hamzah & Partners, n.d.). Increasing data interconnection without strict trade secret redaction protocols expands digital vulnerabilities involving unauthorized access or duplication of data (Fontanela et al., 2026).

The third weakness is the absence of regulations concerning certified destruction obligations. Within national tax audit execution guidelines, a clause mandating the certified destruction of a taxpayer's electronic documents after the audit finishes or the legal case closes has not been regulated. Conversely, several foreign jurisdictions mandate the permanent deletion of post-audit database copies to prevent the future misuse of residual data (Royka & Zuziak,

2025).

B. Comparative Study of Trade Secret Disclosure Dispute Resolution in the United States, Germany, and Australia

As a foundation of comparative law for formulating national legal reform, comparative data indicate that Indonesia and Germany face challenges characterized by fragmented legal frameworks, whereas the United States and Australia feature more integrated legal safeguards against the potential misuse of trade secrets (Disemadi et al., 2025). In the United States, legal instruments such as the Uniform Trade Secrets Act (UTSA) and the Defend Trade Secrets Act (DTSA) provide robust legal certainty against trade secret misappropriation within cyberspace (Risch, 2012). When disputes arise concerning the disclosure of commercial data, as observed in cases such as *United States v. BMC Software, Inc.* and *United States v. Caltex Petroleum Corp.*, the United States federal judicial system applies due process principles by imposing jurisdictional restrictions on trial documents (United States v. Cox, 1999).

To balance the need for tax evidence extraction with taxpayers' privacy rights, the US Tax Court issues protective orders pursuant to Rule 103 of the Tax Court Rules, which align with Rule 26 of the Federal Rules of Civil Procedure (FRCP) (Internal Revenue Service, 2026). This mechanism grants discretion to tax judges to seal pre-trial records, restrict third-party access, and order the destruction or return of technical documents post-trial (Internal Revenue Service, 2026). Additionally, within the developing digital era, the United States federal judiciary implements prohibitions on using public generative artificial intelligence platforms to process confidential taxpayer data, thereby mitigating the risk of data ingestion into external databases (Kilpatrick, 2026).

Conversely, Germany adopts an enforcement approach focused on tax criminal law under the Trade Secret Protection Act (*Geschäftsgeheimnisgesetz*/*GeschGehG*) and the European Union Trade Secrets Directive (Schröder & Widera, 2021). Unlike the United States, which prioritizes aggressive litigation instruments such as *ex parte* seizures, Germany emphasizes a consensus-based approach, out-of-court mediation, and horizontal monitoring bounded by strict compliance with the General Data Protection Regulation (GDPR) (Chwalek et al., 2025). German fiscal courts (*Finanzgerichte*) integrate public interest protection with risk-based confidentiality safeguards to ensure that electronic evidence collection in transfer pricing disputes is executed proportionally without compromising corporate operational confidentiality (Oestreicher, 2014).

Meanwhile, Australia exhibits distinct law enforcement characteristics due to the absence of a specific statutory regime that comprehensively integrates trade secret law with cybersecurity law (Mordaunt, 2026). The protection of commercial confidentiality in Australia remains reliant on conventional contract law and the breach of confidence doctrine (Nashkova, 2024). Although Australian e-courts have implemented digital evidence management protocols and electronic proceedings, reliance on the common law leaves significant legal gaps (May & Burdon, 2006). Australian criminal law criminalizes foreign state-sponsored economic espionage, but has yet to establish comprehensive criminal liability for trade secret misappropriation by individuals, such as independent hackers or corporate insiders (Nashkova, 2024). This vulnerability is evident in several national cyber incidents that disrupted critical infrastructure and exposed valuable corporate commercial log data due to fragmented technological oversight (Gill et al., 2025).

To provide a more structured overview of the differing regulatory and law enforcement approaches among these four jurisdictions, Table 1 presents a comparative matrix of trade secret dispute resolution characteristics.

Table 2: Comparative Matrix of Characteristics and Cross-Jurisdictional Trade Secret Dispute Resolution Frameworks.

Jurisdiction	Primary Regulatory Framework	Evidence and Cybersecurity Characteristics	Dispute Resolution Mechanism	Enforcement Effectiveness
Indonesia	Law No. 30 of 2000 (Fragmented and lacking specific cyber safeguards).	Digital evidence management is weak, fragmented, and limited to conventional instruments.	Tax court litigation and arbitration (Incurring legal uncertainty and high costs).	Low (Hindered by institutional gaps and the substance of legal norms).
United States	Robust regulation through specific statutory codification (UTSA and DTSA).	High-level cyber integration (Accommodating *ex parte* seizures, digital evidence, and encryption standards).	Litigation with protective order safeguards, mediation, and well-developed arbitration.	High (Highly effective in addressing cyber trade secret misappropriation cases).
Germany	Trade Secret Protection Act (*Geschäftsgeheimnisgesetz/GeschGehG)* and European Union Directive.	Moderate technical safeguards strictly aligned with GDPR privacy rules.	Emphasizing a consensus-based approach, out-of-court mediation, and limited litigation.	Moderate to robust (Supported by structured law enforcement investigative capabilities).
Australia	Relying on general contract law and the breach of confidence doctrine.	Electronic court protocols are operational, but integrated cyber safeguards remain limited.	Common law-based litigation and emerging orientation toward Online Dispute Resolution (ODR).	Moderate (Possessing legal gaps in criminalizing individual trade secret misappropriation).

Source: Disemadi et al. (2025), Risch (2012), Schröder & Widera (2021), and Nashkova (2024), adapted by the author (2026).

Electronic evidence governance practices that respect intangible assets and implement data isolation standards, as applied in the United States and Germany, have yet to be institutionalized within either the procedural law of the Tax Court in Indonesia or the audit execution guidelines of the Directorate General of Taxes (DGT). This procedural gap potentially positions Indonesia at a high level of cyber vulnerability when confronting cross-border digital corporate taxpayers.

C. Policy Reformulation for Digital Transaction Oversight Based on Justice and Intellectual Property Rights Protection

Addressing institutional gaps and weak cyber integration within the national tax law system, the reformulation of cyber and tax law in Indonesia is imperative to establish legal certainty for business actors (Widayanti et al., 2025). This national policy reformulation must rest upon four operational pillars.

The first pillar is the implementation of cooperative compliance schemes through the integration of a Tax Control Framework (TCF) into the core tax administration system (Ortax, n.d.). Based on a comparison with Australian and United States jurisdictions, the TCF drives a paradigm shift from invasive, repressive audits to preventive compliance grounded in mutual good faith (Pajakku, n.d.-a). Through this mechanism, large-scale digital corporate taxpayers are authorized to self-map their compliance risks and demonstrate them by presenting system log reports and restricted application programming interface (API) access. This approach leverages the success of horizontal monitoring in several OECD pioneering countries to shield taxpayers from investigative audits that threaten the confidentiality of internal corporate information (Valderrama, 2021). The second pillar involves overhauling tax procedural law by establishing technical regulations on protective orders within tax administrative dispute resolutions (Kilpatrick, 2026). Modeled after US Tax Court jurisprudence and alignment with the EU Trade Secrets Directive, this regulation must be enacted as a binding Regulation of the Director General of Taxes or a

Supreme Court Regulation (Fontanela et al., 2026). The regulation must comprise three core operational components:

1. Sealing the record for technological evidence so that the taxpayer's algorithmic formulas are excluded from public rulings (Internal Revenue Service, 2026);
2. Utilizing clean room review facilities equipped with air-gapped systems during digital forensic audits to prevent unauthorized data duplication (Royka & Zuziak, 2025); and
3. Recognizing the functional equivalence principle, which permits the submission of secondary documents containing the validity conclusions of independent experts as a substitute for primary source code if the risk of data exposure is deemed excessive (Royka & Zuziak, 2025).

To summarize the analytical framework regarding tax regulatory gaps, risks to taxpayers' intellectual property rights, and the direction of reform recommendations prior to addressing technical infrastructural aspects, Table 3 presents a comprehensive mapping of legal provision gaps.

Table 3: Legal Gap Matrix of Digital Tax Oversight and Proposed Reforms for IPR Protection

Legal Analysis Domain	Regulatory Gap / Empirical Practice Weakness	Proposed Normative Structure Reform and National Policy
Tax Law and Collection Procedures (KUP Law & PR 68/2025)	Tax data extraction authority is broad, lacking binding regulations on certified post-audit destruction protocols for taxpayers' sensitive information.	Widespread implementation of cooperative compliance technical guidelines based on the TCF framework, alongside establishing regulations empowering the Panel of Judges to grant protective orders.
Intellectual Property Law (Law No. 30 of 2000)	Statutory provisions have not anticipated threats of automated data extraction by external cyber actors (automated scraping agents) or through machine learning analytical processing.	Revising the law to expand the definition of unauthorized disclosure of trade secrets, including the act of inputting confidential data files into public generative AI platforms without authorization.
Integrated Cyber Privacy Law (EIT Law & PDP Law)	Implementing regulations have yet to govern encryption layer security standards specifically within cross-jurisdictional SPP-TDLN collection network operations by third parties.	Mandating high-level cybersecurity standards (military-grade encryption) in overseeing partnership sandboxing processes, and prohibiting unauthorized secondary analytical data processing.

Source: Compiled by the author (2026) based on the provisions of Law No. 30 of 2000, and data from Royka & Zuziak (2025), TaxPrime (2023), Fontanela et al. (2026), Elyani et al. (2025), and PT PSI (2025).

The third pillar is the tightening of system sandboxing requirements for third parties managing cyber tax infrastructure. Pursuant to Article 5 of Presidential Regulation No. 68 of 2025, delegating SPP-TDLN collection authority to private aggregators or assigned business entities such as PT Jalin Pembayaran Nusantara necessitates rigid international cybersecurity standardization, such as ISO/IEC 27001 and ISO/IEC 20000-1 certifications (PT PSI, 2025). Given that foreign digital transaction data flows are heavily populated with consumer preference data and e-commerce platform algorithmic tracks that qualify as trade secrets, the sandboxing process must include the validity of penetration testing (Muh Sidratul et al., 2019). The state must enforce strict data sovereignty rules by strictly prohibiting all collecting partners from data segregation or unauthorized data profiling for training third-party external artificial intelligence (Pajakku, n.d.-b).

The fourth pillar is directed at strengthening the authority of the Public Prosecution Service of the Republic of Indonesia in protecting the public interest and enforcing the law by optimizing the *dominus litis* principle within digital trade secret disputes (Rismanto et al., 2021). Within the current tax-related civil legal system, public prosecutors have limited scope to initiate legal interventions in cybercrime cases targeting corporate trade secrets, particularly those with a broad impact on national economic stability (Allo et al., 2025). Adopting reform models from Germany and Finland, the revision of the Trade Secret Law needs to be synchronized with the new Criminal Procedure Code to expand the definition of the offense of unauthorized information disclosure, including the act of uploading confidential tax dispute documents into public generative artificial intelligence models without authorization (Ackermann-Blome & Rindell, 2018). Public prosecutors must be granted robust coordination authority based on the *dominus litis* principle to control cyber tax investigation processes, align the actions of law enforcement agencies, and ensure that the DGT's Coretax database and AICEco modules operate using centralized on-premise servers to guarantee national data confidentiality parameters (Nelson & Aini, 2025).

CONCLUSION

Based on the analysis conducted, it can be concluded that the implementation of digital tax oversight in Indonesia through the Coretax and AICEco systems requires clear legal boundaries to prevent the leakage of taxpayers' trade secrets. Comparative findings indicate that the legal framework in Indonesia lacks comprehensive integration regarding digital evidence management compared to the jurisdictions of the United States, which implements protective orders, and Germany, which binds fiscal oversight to data privacy protection rules. The absence of standard procedures concerning source code access restrictions and post-audit data destruction procedures potentially diminishes legal certainty for business entities within the information technology sector. To ensure a balance between state revenue interests and the protection of intellectual property rights, it is recommended that the government systematically reformulate national tax policy. This reform is directed toward the institutionalization of cooperative compliance schemes through a Tax Control Framework, the adoption of protective orders in the form of sealing evidence and utilizing clean room review facilities within tax court procedural law, alongside the application of high-level encryption standards to third-party partnership system sandboxing. Additionally, strengthening coordination by the Public Prosecution Service of the Republic of Indonesia based on the *dominus litis* principle is necessary to control cyber tax investigation processes, ensuring the enforcement of equitable legal certainty.

REFERENCES

Ackermann-Blome, N., & Rindell, J. (2018). Should trade secrets be protected by private and/or criminal law? A comparison between Finnish and German laws. *Journal of Intellectual Property Law and Practice*, 13(9), 743-752.

Aguspajak. (2022, 7 Oktober). *Pemeriksaan pajak*. Konsultan Pajak di Botax Consulting Indonesia. https://aguspajak.com/2022/10/07/pemeriksaan-pajak/

Aguspajak. (n.d.). *Konsultan pajak di Botax Consulting Indonesia: Praktisi dengan pengalaman lebih dari 30 tahun*. Diakses pada 18 Juni 2026, dari https://aguspajak.com/

Alfreda, I. J., Permata, R. R., & Ramli, T. S. (2021). Pelindungan dan tanggung jawab kebocoran informasi pada penyedia platform digital berdasarkan perspektif rahasia dagang. *Jurnal Sains Sosio Humaniora*, 5(1), 1-16.

Allo, Z. T., Akub, M. S., Aswanto, ..., & Anas, A. M. A. (2025). Strengthening Dominus Litis Principle for Effective Corruption Case Management in Indonesia: Harmonizing Positive Law and Islamic Legal Principles. *Jurnal Ilmiah Mizani*, 12(1), 45-58.

Assegaf Hamzah & Partners. (n.d.). *New presidential regulation sets up VAT collection system for cross-border digital transactions*. Diakses pada 18 Juni 2026, dari https://www.ahp.id/new-presidential-regulation-sets-up-vat-collection-system-for-cross-border-digital-transactions/

Awaisheh, S. M. A., Odeibat, M. A., Althunibat, A. O., Hmaidan, R., Al_Zboon, M. S. M., Alamawi, M. A. M., & Alsalamat, M. A. M. (2025). Protecting Trade Secrets Arises from Artificial Intelligence in UAE and Jordanian Legislation. *Journal of Human Security*, 21(1), 50-53.

Baker McKenzie. (2025, Maret). *Navigating the digital tax landscape*. Baker McKenzie Insight. https://www.bakermckenzie.com/en/insight/publications/2025/03/navigating-the-digital-tax-landscape

Chwalek, J., Winter, D., & Biedenbach, M. (2025). Implications of Applying the Act on the Protection of Trade Secrets and GDPR in Data Trustees. *Communications in Computer and Information Science*, 1105, 112-126.

Colvin, J. A. (2016, 21 Juli). Protecting confidential taxpayer information in tax court. *Tax Controversy 360*. https://www.taxcontroversy360.com/2016/07/protecting-confidential-taxpayer-information-in-tax-court/

Disemadi, H. S., Chutia, U., Afdal, W., ..., & Tans, D. (2025). RECONSTRUCTING THE LEGAL FRAMEWORK OF TRADE SECRET PROTECTION VIS-À-VIS CYBER THEFT: A Cross-Jurisdictional Comparative Study. *Jurisdictie: Jurnal Hukum dan Syariah*, 16(1), 88-104.

Elyani, E., Ramlan, R., & Perdana, S. (2025, Juni). Desain Hukum Bisnis Berbasis Teknologi Digital. Dalam *Seminar Nasional Hukum, Sosial dan Ekonomi* (Vol. 4, No. 1, hlm. 139-149).

EY. (2015, November). *Global digital tax developments review*. https://www.ey.com/

Fau, R. T., & Verawaty, S. (2024). Penguatan Perjanjian Lisensi Dan Optimalisasi Perhitungan Royalti Dalam Melindungi Hak Kekayaan Intelektual Berupa Rahasia Dagang Dan Paten. *Technology and Economics Law Journal*, 3(2), Artikel 4. https://scholarhub.ui.ac.id/telj/vol3/iss2/4

Fiskusmagnews. (n.d.). *Analisis strategis korelasi AICEco dan pendeteksian transfer pricing abuse berbasis kerangka kerja DEMPE*. Diakses pada 18 Juni 2026, dari https://fiskusmagnews.com/ekonomi/analisis-strategis-korelasi-aiceco-dan-pendeteksian-transfer-pricing-abuse-berbasis-kerangka-kerja-dempe/

Fontanela, C., Costa, T. A., & Marocco, A. D. A. L. (2026). Harmonising Trade Secret Protection in AI: Innovation, Opacity and Digital Vulnerability. *Laws*, 15(2), 34.

Gill, N. S., Kaur, K., & Sandhu, K. K. (2025). Cybersecurity in Australian Ports: Incidents, Challenges, and Strategic Responses. *International Conference on Electrical, Computer, and Energy Technologies (ICECET 2025)*, 452-461.

Hakim, M. F., Irwanto, D. A. B., & Tjaja, Y. M. (2025). Implikasi Peraturan Presiden Nomor 68 Tahun 2025 terhadap transaksi digital lintas negara oleh pelaku usaha Indonesia. *Jurnal Dunia Ilmu Hukum (JURDIKUM)*, 3(2), 42–50. https://doi.org/10.59435/jurdikum.v3i2.606

Hudson, B. (2024). Trade Secrets as a Cornerstone of Innovation in Knowledge-Based Economies. *Intellectual Property Journal*, 42(1), 75-89.

Internal Revenue Service. (2026, 30 April). *IRM Part 35. Chief Counsel Directives Manual – Tax Court Litigation, Chapter 4, Section 6, Responding to petitioner's information gathering attempts*. U.S. Department of the Treasury. https://www.irs.gov/irm/part35/irm_35-04-06

Irawan, F., & Ulinnuha, I. A. (2022). Transfer pricing aggressiveness in Indonesia: Multinationality, tax haven, and intangible assets. *Jurnal Dinamika Akuntansi Dan Bisnis*, 9(1), 1-18.

Iskandar, A. (2009). Perlindungan Hukum Rahasia Dagang Menurut Undang-Undang Nomor 30 tahun 2000 Tentang Rahasia Dagang. *Pranata Hukum*, 4(2).

Kilpatrick. (2026, 1 Mei). *Protective orders in the age of generative AI: Best practices for safeguarding confidential information*. JD Supra. https://www.jdsupra.com/legalnews/protective-orders-in-the-age-of-1927691/

Kusuma & Partners Law Firm. (2025, 31 Mei). *Aspek hukum e-commerce dan transaksi digital di Indonesia*. https://kusumalawfirm.com/id/article/legal-aspects-of-e-commerce-and-digital-transactions-in-indonesia/

Maier, I. (2026, 17 Juni). *Trade secrets*. RÖDL. https://www.roedl.com/en/legal-advisory/ip-media/trade-secrets/

May, L., & Burdon, M. (2006). Information protection management structures in Australian e-courts. *Journal of Theoretical and Applied Electronic Commerce Research*, 1(2), 15-29.

Mordaunt, D. A. (2026). Balancing rights and governance: comparative analysis of open disclosure frameworks in Australia and New Zealand. *New Zealand Medical Journal*, 139(1630), 44-56.

Muh Sidratul, M. A. M. A., Farani, W., Wahyudin, B. K., ..., & Baskoro Yudhoatmojo, S. (2019). Analyzing the Relevance of Inhibiting Factors in Implementing ISO 27001 Using the DEMATEL Method (Case Study: LPSE Ministry of Finance, Indonesia). *5th International Conference on Computing Engineering and Design (ICCED 2019)*, 88-94.

Mullins, J. (2022). *Digitalization and Value Creation: Policy Challenges for Emerging Economies*. IMF and ADB Joint Working Paper Series, No. 114.

Nashkova, S. (2024). Addressing Criminal Liability for Misuse of Trade Secrets Under Australian Law: Is the Current Legal Framework Adequate to Protect the Interests of Owners of Trade Secrets? *IIC International Review of Intellectual Property and Competition Law*, 55(4), 512-529.

Nelson, F. M., & Aini, A. N. (2025). Bridging the Gap of Ineffective Coordination in Indonesia: A Comparative Study on the Functional Differentiation and Dominus Litis Principle. *Media Iuris*, 8(1), 101-114.

Nurbekova, G. T., Greggi, M., & Tussupova, L. K. (2026). Maintaining Confidentiality in the Exchange of Information on Tax Matters in the Republic of Kazakhstan. *Laws*, 15(3), 41.

Oestreicher, A. (2014). Transfer pricing in Germany. Dalam *Resolving Transfer Pricing Disputes: A Global Analysis*, Cambridge University Press, 204-221.

Organisation de coopération et de développement économiques (Paris). (2011). *Implementing the tax transparency standards: a handbook for assessors and jurisdictions*. OECD.

Oroh, K. B., Amirulloh, M., & Faisal, P. (2024). Penguatan Regulasi Rahasia Dagang Melalui Ketentuan Mengenai Perlindungan Informasi Rahasia dalam Perjanjian Lisensi Rahasia Dagang Berdasarkan Penerapan Asas Kepastian Hukum, Teori Prospek dan Teori Risiko. *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan*, 7(2), 146-159.

Ortax. (n.d.). *Reformasi sistem perpajakan, DJP lakukan transisi ke kepatuhan kooperatif*. Diakses pada 18 Juni 2026, dari https://ortax.org/

PT PSI. (2025, Juli). *Ringkasan Perpres 68 Tahun 2025: Sistem pemungutan pajak atas transaksi digital luar negeri*. https://ptpsi.com/wp-content/uploads/2025/07/Ringkasan-Perpres-68-Tahun-2025-Sistem-Pemungutan-Pajak-atas-Transaksi-Digital-Luar-Negeri.pdf

Pajakku. (n.d.-a). *Dorong kepatuhan kooperatif, Kemenkeu bangun sistem pajak berbasis TCF*. Diakses pada 18 Juni 2026, dari https://pajakku.com/artikel/dorong-kepatuhan-kooperatif-kemenkeu-bangun-sistem-pajak-berbasis-tcf

Pajakku. (n.d.-b). *Mengenal calon mitra SPP-TDLN dalam Perpres 68/2025*. Diakses pada 18 Juni 2026, dari https://pajakku.com/artikel/mengenal-calon-mitra-spp-tdln-dalam-perpres-682025

Pajakku. (n.d.). *Perpres 68/2025: Pungutan PPN digital luar negeri (SPP TDLN)*. Diakses pada 18 Juni 2026, dari https://pajakku.com/

Putri Aldina, D. (2023). *Perlindungan Hukum Terhadap Hak Cipta Penulis Atas Penjualan Buku Bajakan yang Diedarkan Melalui E-Commerce/Shopee* (Skripsi Sarjana, Universitas Islam Indonesia).

Risch, M. (2012). An empirical look at trade secret law's shift from common to statutory law. Dalam *Intellectual Property and the Common Law*, 211-230.

Rismanto, Murwadji, T., Permata, R. R., & Somawijaya. (2021). A new paradigm in trade secret law enforcement by the prosecutor's office of the republic of Indonesia to protect public interests. *Journal of Legal, Ethical and Regulatory Issues*, 24(5), 1-12.

Royka, A. M., & Zuziak, M. M. (2025, 7 Maret). *Managing source code discovery in patent and high-tech intellectual property litigation*. Nixon Peabody. https://www.nixonpeabody.com/insights/alerts/2025/03/07/managing-source-code-discovery-in-patent-and-high-tech-intellectual-property-litigation

Schröder, V., & Widera, P. (2021). Obtaining Evidence in Patent Litigation and Trade Secret Protection-A Tale of Two Poles. *GRUR International*, 70(11), 1045-1056.

TaxPrime. (2023). *TaxPrime Newsletter - Status Quo: Penyidikan Tindak Pidana Perpajakan PMK No. 17 Tahun 2025*. https://www.taxprime.net/wp-content/uploads/2023/03/TaxPrime-Newsletter-Status-Quo-Penyidikan-Tindak-Pidana-Perpajakan-PMK-No-17-Tahun-2025.pdf

Tomo, A. S. N. (2020). *Tinjauan Yuridis Pasal Pemidanaan Bagi Pelanggar Rahasia Dagang Dalam Undang-Undang Nomor 30 Tahun 2000* (Skripsi Sarjana, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta).

Undang-Undang Republik Indonesia Nomor 30 Tahun 2000 tentang Rahasia Dagang. (2000). *Lembaran Negara Republik Indonesia Tahun 2000 Nomor 242*.

United States v. Caltex Petroleum Corp., 12 F. Supp. 2d 545 (N.D. Tex. 1998). https://law.justia.com/cases/federal/district-courts/FSupp2/12/545/2498909/

United States v. Cox, 73 F. Supp. 2d 751 (S.D. Tex. 1999). https://www.justia.com/cases/federal/district-courts/FSupp2/73/751/

Valderrama, I. M. (2021, November). An ASEM Model of Cooperation in Digital Economy Taxation. In *13th Asia-Europe Meeting (ASEM) Summit* (p. 86).

Widayanti, T. F., Rohman, A. D., Haris, A. N. Z., ..., & Hakim, M. Z. (2025). ENHANCING CYBERSECURITY AND LEGAL INTEGRATION: REFORMING INDONESIA'S CYBER LAW TO FOSTER SUSTAINABLE GROWTH IN THE DIGITAL ECONOMY. *Diponegoro Law Review*, 10(1), 14-29.