Jurnal Kajian Pembaruan Hukum (2025) 5:2 199-236
DOI: https://doi.org/10.19184/jkph.v5i2.53686
Published by the University of Jember, Indonesia
Available online 30 November 2025

Conceptualising Big Data within the Indonesian Trade Secrets Legal Framework

Moch. Marsa Taufiqurrohman
Padjadjaran University, Bandung, Indonesia

Tarsisius Murwadji
Padjadjaran University, Bandung, Indonesia

Helza Nova Lita
Padjadjaran University, Bandung, Indonesia

ABSTRACT: The big data phenomenon has transformed the global digital economy landscape, yet an unclear legal status in Indonesia creates protection gaps that disadvantage technology innovators and business actors. This legal uncertainty has become increasingly urgent as Indonesia's digital economy accelerates post-pandemic, with data-driven startups and established businesses facing immediate risks from inadequate intellectual property protection in competitive global markets. An insufficient legal framework to protect big data as intellectual property potentially hinders technology investment and knowledge transfer in the digital transformation era. This article, employing a combination of normative juridical research and comparative analysis, aims to establish big data conceptualisation as a trade secret within Indonesia's intellectual property legal framework. This article argues that the characteristics of big data, encompassing information secrecy, substantial economic value, and adequate protection efforts, fulfil the trade secret requirements set out in Article 3 of Law Number 30 Year 2000 concerning Trade Secrets. Analysis of big data protection practices in the European Union through the Trade Secrets Directive and a comparative study with United States and China jurisprudence demonstrates legal convergence, enabling adaptation within the Indonesian legal system. This ultimately meets the business information protection requirements under Article 2 of Law Number 30 Year 2000 concerning Trade Secrets, rendering big data protection practices legally justifiable as trade secrets. The article concludes by suggesting that policymakers should establish adequate frameworks and regulations to accommodate big data protection as trade secrets in digital markets. This would promote sustainable technological innovation and protect the interests of Indonesian digital business actors in global competition.

KEYWORDS: Big Data; Digital Technology; Intellectual Property Law; Trade Secrets; Personal Data Protection.

HOW TO CITE:
Taufiqurrohman, Moch. Marsa, et.al., "*Conceptualising Big Data within the Indonesian Trade Secrets Legal Framework*" (2025) 5:2 Jurnal Kajian Pembaruan Hukum 199-236. DOI: <https://doi.org/10.19184/jkph.v5i2.53686>.

* Corresponding author's e-mail: moch23009@mail.unpad.ac.id

Submitted: 10/05/2025 Reviewed: 18/09/2025 Revised: 07/10/2025 Accepted: 25/11/2025

I. INTRODUCTION

The digital revolution has fundamentally transformed the global economic landscape, positioning data as the most valuable commodity of the 21st century.[1] This transformation is particularly evident in the emergence of big data as a critical business asset, with companies investing billions of dollars in data collection, processing, and analysis infrastructure to gain a competitive advantage in increasingly saturated markets.[2]Indonesia's current intellectual property regime lacks specific provisions for protecting big data as a form of intellectual property.[3] The existing trade secrets law, Law Number 30 Year 2000 concerning Trade Secrets, was enacted when big data technologies were nascent, creating a regulatory gap that could undermine Indonesia's competitiveness in the global digital economy.[4] This legal uncertainty is compounded by the recent enactment of Law Number 27 Year 2022 concerning Personal Data Protection, which primarily focuses on privacy rights rather than the commercial value and protection of data assets, leaving businesses uncertain about their rights to protect and monetise data investments.[5]

The intersection between digital markets and data exploitation has become a critical concern for competition law enforcement globally. Taufiqurrohman et al. highlight how digital markets create unique challenges for traditional competition law frameworks, particularly in addressing abuse of dominance by tech giants who leverage their control over vast datasets to maintain market power.[6] The concentration of data in the hands of a few dominant players raises significant concerns about

[1] Meglena Kuneva, "Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling" (European Commission, Brussels, 31 March 2009), online: European Commission.

[2] Kelly D Martin et al, "Data Privacy in Retail" (2020) 96:4 *Journal of Retailing* 474.

[3] Shevierra Danmadiyah et al, "A Party's Recall Right in the Concept of Democratic Country" (2019) 19:2 *Syariah: Jurnal Hukum dan Pemikiran* 151-158.

[4] Undang-Undang Republik Indonesia Nomor 30 Tahun 2000 tentang Rahasia Dagang, LN Tahun 2000 Nomor 242 [Indonesian Trade Secrets Law].

[5] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, LN Tahun 2022 Nomor 220 [Indonesian Personal Data Protection Law].

[6] Moch Marsa Taufiqurrohman, Helza Nova Lita & Gress Gustia Adrian Pah, "Digital Markets and Data Exploitation: Addressing Abuse of Dominance Under Indonesian Competition Law" (2024) 25:1 *Jurnal Penelitian Hukum De Jure* 1.

market competition and innovation, as these companies can use their data advantages to exclude competitors and create barriers to entry.[7] This phenomenon is particularly relevant in Indonesia, where global tech giants compete with domestic players for market dominance in various digital sectors.

The theoretical foundation for protecting data as intellectual property has been extensively debated in academic literature. Zech argues that the nature of information is less important than how it is treated, distinguishing between semantic, syntactic, and structural information, with both personal data and trade secrets falling into the semantic category. This classification provides a conceptual framework for understanding how big data, as semantic information with certain meaning and knowledge about objects, can be protected under intellectual property regimes.[8] Furthermore, the intersection between data protection and intellectual property law has gained increasing attention, particularly in the context of the European Union's Trade Secrets Directive, which explicitly acknowledges that trade secrets may include information containing personal data.[9]

The relationship between personal data protection and competition law has become increasingly complex in the digital age. Taufiqurrohman et al. argue that the interrelation between these two legal regimes creates both opportunities and challenges for market regulation in Indonesia.[10] While data protection laws aim to safeguard individual privacy rights, competition law seeks to ensure fair market competition and prevent abuse of market power. The tension between these objectives becomes apparent when companies use privacy compliance as a justification for practices that may have anticompetitive effects, such as limiting data portability or restricting data sharing with competitors.[11]

[7] *Ibid* at 5.

[8] Herbert Zech, "A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data" (2016) 11:6 *Journal of Intellectual Property Law and Practice* 460.

[9] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[10] Moch Marsa Taufiqurrohman, Helza Nova Lita & Gress Gustia Adrian Pah, "The Interrelation Between Personal Data Protection and Competition Legal Regime in the Indonesian Digital Market" (2024) 8:3 *Syiah Kuala Law Journal* 275.

[11] *Ibid* at 280.

The role of automation and artificial intelligence in legal professions also impacts how big data is conceptualised and protected. Taufiqurrohman's analysis of automation in legal practice demonstrates how AI technologies are transforming traditional legal frameworks and creating new challenges for intellectual property protection.[12] As AI systems become more sophisticated in processing and analysing big data, the distinction between human-generated insights and machine-generated outputs becomes increasingly blurred, raising questions about the appropriate legal frameworks for protecting AI-enhanced data analytics.

Previous research on data protection and intellectual property has primarily focused on traditional forms of intellectual property rights, such as patents and copyrights, with limited attention to trade secrets as a mechanism for protecting big data. Disemadi's seminal work on data ownership in Indonesia provides valuable insights into the intersection of big data and intellectual property law, arguing that integrating intellectual property elements into big data regulation could threaten the antitrust climate and requires more concrete evidence from actual big data utilisation.[13] His analysis reveals that the normative space for big data regulations through an intellectual property rights perspective remains too small to be comprehensively described, necessitating further research on the potentials and risks of regulating big data under intellectual property law frameworks.

Similarly, Radoń's comprehensive analysis of trade secrets protection for big data in the European Union demonstrates that personal data can fulfil trade secret requirements under the EU Trade Secrets Directive, particularly regarding secrecy, commercial value, and reasonable protection measures. Her research provides guidelines on how personal data fulfils the definition of trade secrets and analyses the provisions of reverse engineering along with its relevance for anonymised data.[14] The study concludes that personal data can be conceptualised as trade secrets in the EU, provided

[12] Moch Marsa Taufiqurrohman, "Otomatisasi Dan Kecerdasan Buatan Pada Profesi Hukum: Kerangka Teoritis Dan Narasi Ideal Di Masa Depan" (2024) 13:2 *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 195.

[13] Hari Sutra Disemadi, "Data Ownership in Regulating Big Data in Indonesia Through the Perspective of Intellectual Property" (2022) 13:2 *Jurisdictie: Jurnal Hukum dan Syariah* 188.

[14] *Ibid* 46-47.

adequate protection measures are implemented and balanced with data protection rights.

Martin et al.'s global study on data privacy in retail contexts reveals that big data serves as a driver of customer relationship performance, with companies across four countries demonstrating significant behavioural rewards from data-enabled customer value.[15] Their research identifies three emergent themes: big data as a driver of customer relationship performance, profound impacts of regulation, and privacy protection as a proactive retail strategy.[16] The study's findings indicate that across all four countries surveyed, the value resulting from personalised, improved customer experiences, supported by big data, leads to critical behavioural rewards such as increased share of wallet, loyalty, and opt-in willingness.

The challenge posed by tech giants' non-negotiable privacy policies adds another dimension to the data protection debate. Taufiqurrohman et al. examine how major technology companies use standardised privacy policies that users must accept without modification, effectively creating a "take it or leave it" scenario that may violate competition law principles.[17] This practice is particularly problematic in digital markets where consumers have limited alternatives and where network effects create strong incentives to accept unfavourable terms. The Indonesian competition law framework must evolve to address these challenges while balancing the need for data protection with fair competition principles.

However, these studies primarily focus on developed economies with established intellectual property frameworks, leaving a significant gap in understanding how emerging economies like Indonesia can adapt these concepts to their unique legal and economic contexts. The main limitation of previous research lies in the absence of a comprehensive analysis specifically addressing how big data can be conceptualised within Indonesia's existing trade secrets legal framework. While international studies provide valuable comparative insights, they do not address the

[15] Martin et al, *Supra* note 2 476.

[16] *Ibid* 475.

[17] Moch Marsa Taufiqurrohman, Helza Nova Lita & Gress Gustia Adrian Pah, "Tech Giants' Non-Negotiable Privacy Policies Strategy Versus Indonesian Competition Law" (2024) 9:1 Jurnal Bina Mulia Hukum 159.

specific challenges and opportunities presented by Indonesia's legal system, cultural context, and developmental priorities.

This article aims to address these limitations by providing a comprehensive analysis of how big data can be conceptualised as trade secrets within Indonesia's legal framework, specifically examining the applicability of Law Number 30 Year 2000 concerning Trade Secrets to the protection of big data. The research seeks to establish a theoretical foundation for protecting big data as intellectual property while providing practical guidance for businesses and policymakers. The scientific merit and novelty of this paper lie in its systematic application of trade secrets principles to big data protection in an emerging economy context, offering a unique perspective that bridges theoretical legal analysis with practical implementation considerations.

II. METHODS

This research employs a normative juridical research methodology with a comparative law approach to analyse the conceptualisation of big data within Indonesia's trade secrets legal framework. The normative juridical method focuses on examining legal norms, principles, and doctrines through systematic analysis of legislation, legal literature, and jurisprudence.[18] This approach is particularly suitable for investigating how existing legal frameworks can be interpreted and applied to emerging technological phenomena such as big data protection.

The research utilises secondary data sources consisting of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include Law Number 30 Year 2000 concerning Trade Secrets, Law Number 27 Year 2022 concerning Personal Data Protection, and relevant international legal instruments such as the TRIPS Agreement and the European Union Trade Secrets Directive.[19] Secondary legal materials comprise academic literature and journal articles. Comparative analysis focuses on three key jurisdictions, the European Union, the United

[18] Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana Prenada Media Group, 2019).

[19] Soerjono Soekanto & Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat (Jakarta: Rajawali Pers, 2020) 13.

States, and China, selected for their digital market influence and comprehensive big data protection frameworks.

Data collection was conducted through a comprehensive literature review and legal document analysis. The literature review encompasses scholarly articles published in peer-reviewed journals, focusing on recent publications from 2018 to 2024 to ensure the currency and relevance of the analysis.[20] Legal document analysis involves a systematic examination of statutory provisions and regulatory frameworks related to trade secrets protection.[21] The data analysis process follows a qualitative approach using legal interpretation techniques, including grammatical interpretation, systematic interpretation, and teleological interpretation.[22]

III. THEORETICAL FRAMEWORK OF BIG DATA AS TRADE SECRETS

The conceptualisation of big data as trade secrets requires a comprehensive understanding of both the nature of big data and the legal requirements for trade secret protection. Big data, characterised by the "5V" framework of volume, velocity, variety, value, and veracity, represents a fundamental shift in how information is collected, processed, and utilised for commercial purposes. The volume dimension refers to the massive scale of data generation, with global data creation reaching unprecedented levels in the digital economy.[23] Velocity encompasses the speed at which data is generated, collected, and analysed, often in real-time applications that drive immediate business decisions. Variety refers to the diverse types and sources of data, including structured databases, unstructured social media content, sensor data from Internet of Things devices, and behavioural analytics from digital platforms. These characteristics of big data create unique considerations for determining how such information can qualify for trade secret protection under Indonesian law.

[20] Sudikno Mertokusumo, Mengenal Hukum: Suatu Pengantar (Yogyakarta: Cahaya Atma Pustaka, 2019) 158.

[21] Konrad Zweigert & Hein Kötz, An Introduction to Comparative Law, 3rd ed (Oxford: Oxford University Press, 1998) 34.

[22] *Ibid.*

[23] Martin et al, *Supra* note 2.

The theoretical foundation for protecting data as intellectual property has evolved significantly in recent years. Zech's categorisation of information into semantic, syntactic, and structural types provides a crucial framework for understanding how big data can be conceptualised within intellectual property regimes.[24] Semantic information, which includes both personal data and trade secrets, has a certain meaning and refers to actual or potential knowledge about objects or processes.[25] This classification is particularly relevant for big data, as most commercially valuable datasets contain semantic information that provides insights into consumer behaviour, market trends, or operational efficiencies.

Recent scholarship has emphasised the growing importance of data as an economic asset. Drexl et al. argue that data-driven innovations are becoming core resources of growth, with acknowledged positive results including new, improved products and services, business opportunities, and cost reductions. This economic significance of data supports arguments for trade secret protection mechanisms that can incentivize continued innovation and investment in data-driven technologies.. Furthermore, the intersection between data protection and intellectual property law has gained increasing attention, particularly in determining how big data compilations and analytical methodologies can be protected as trade secrets while complying with data protection requirements.

Artificial intelligence and machine learning algorithms applied to big data processing create additional dimensions for trade secret protection. When companies develop proprietary algorithms, analytical models, or data processing methodologies to extract insights from big data, these technological components constitute potential trade secrets alongside the underlying datasets. The combination of raw data with sophisticated AI-driven analytical frameworks creates multi-layered intellectual property assets where both the data compilation and the processing methodologies can qualify for trade secret protection, provided they satisfy the fundamental requirements of secrecy, economic value, and reasonable protection measures

[24] Zech, *Supra* note 13.

[25] *Ibid.*

IV. LEGAL FRAMEWORK FOR TRADE SECRETS PROTECTION IN INDONESIA

Indonesia's trade secrets protection regime is primarily governed by Law Number 30 Year 2000 concerning Trade Secrets, which was enacted to fulfill Indonesia's obligations under the TRIPS Agreement and to provide domestic protection for confidential business information. The law defines trade secrets as "information that is not known to the public in the field of technology and/or business, has economic value because it is useful in business activities, and is maintained in secrecy by the owner of the trade secret." [26]

Article 3 of the Trade Secrets Law establishes three fundamental requirements for trade secret protection: secrecy, economic value, and reasonable protection measures. The secrecy requirement stipulates that information is considered secret if it is only known by certain parties or not generally known by the public. This criterion is particularly relevant for big data, as most valuable datasets are maintained with restricted access and sophisticated security measures to prevent unauthorized disclosure or use.[27]

Law Number 27 Year 2022 concerning Personal Data Protection establishes a comprehensive framework for protecting individual privacy rights while creating important intersections with trade secret protection. Article 1(1) defines personal data as "any data about a person either identified and/or identifiable individually or in combination with other information either directly or indirectly through electronic and/or non-electronic systems." This definition creates potential overlap with big data that may contain personal information while simultaneously qualifying as trade secrets.

Distinction between commercial data protection under trade secrets law and personal data protection under data protection law becomes crucial for businesses processing big data. While trade secrets law focuses on protecting confidential business information from unauthorized disclosure

[26] Indonesian Trade Secrets Law, *Supra* note 9, Preliminary Considerations.

[27] *Ibid* art 3.

or use by competitors, personal data protection law emphasizes individual rights including consent, access, rectification, and erasure. Article 20 of Personal Data Protection Law grants data subjects rights to access, correct, and delete their personal data, which may conflict with trade secret holders' interests in maintaining data secrecy and integrity.

Relationship between these two legal regimes requires careful navigation to ensure compliance with both frameworks. Trade secrets protection under Article 3 of Law 30/2000 requires information to be "not known to public," while personal data protection under Law 27/2022 may require transparency about data processing activities to data subjects. This apparent tension can be resolved through understanding that trade secret protection applies to compilation, analysis methods, and derived insights from data, while personal data protection applies to underlying individual information.

Article 65 of Personal Data Protection Law provides important guidance by stating that personal data processing for legitimate business interests must balance individual rights with business needs. This provision creates space for protecting big data analytics and insights as trade secrets while respecting individual privacy rights. Companies can maintain trade secret protection over their analytical methodologies, algorithmic processes, and aggregated insights while ensuring transparency about personal data collection and processing activities as required by data protection law.

Economic value requirement is satisfied when the secrecy of the information can be used to conduct commercial activities or increase economic profits. This requirement aligns well with the commercial nature of big data, which has become increasingly valuable for businesses seeking to understand consumer preferences, optimize operations, or develop new products and services.[28] The monetization of data through advertising, personalization, and predictive analytics demonstrates clear economic value that satisfies this requirement.

Reasonable protection measures requirement mandates that owners or controlling parties have taken appropriate and proper steps to maintain secrecy.[29] The explanatory notes to the Trade Secrets Law clarify that these

[28] Martin et al, *Supra* note 2.

[29] Indonesian Trade Secrets Law, *Supra* note 9 art 3(4).

measures should include all steps that contain standards of reasonableness, appropriateness, and propriety that must be undertaken.[30] For example, companies must establish standard procedures based on common practices and internal company regulations that specify how trade secrets are protected and who is responsible for maintaining secrecy.

Article 2 of the Trade Secrets Law defines the scope of protection to include "production methods, processing methods, sales methods, or other information in the field of technology and/or business that has economic value and is not known by the general public."[31] This broad definition potentially encompasses various forms of big data, including customer databases, behavioral analytics, predictive algorithms, and market intelligence systems. The inclusion of "other information in the field of technology and/or business" provides flexibility to accommodate emerging forms of valuable business information, including big data applications.

Practical implementation of both legal frameworks requires companies to distinguish between different types of information within their big data systems. Raw personal data collected from individuals remains subject to personal data protection requirements including consent, purpose limitation, and data minimization principles under Articles 20-28 of Law 27/2022. However, aggregated datasets, analytical insights, and proprietary algorithms developed from this data can qualify for trade secret protection provided they meet secrecy, economic value, and reasonable protection requirements.

Article 40 of Personal Data Protection Law regarding data security measures aligns with trade secret protection requirements for reasonable protection measures. Companies implementing comprehensive data security frameworks to comply with personal data protection obligations often simultaneously satisfy trade secret protection requirements, creating synergies between both legal regimes rather than conflicts.

Intersection between trade secrets protection and competition law creates additional complexities in the Indonesian legal framework. The dominance of certain tech companies in data collection and analysis may create

[30] *Ibid*, Explanation of art 3(1).
[31] *Ibid* art 2.

situations where trade secret protection could be used to maintain anticompetitive advantages.[32] Indonesian competition law must therefore balance the legitimate need to protect trade secrets with the requirement to maintain fair competition and prevent abuse of dominant market positions. These also creates a complex regulatory environment that requires careful coordination. While companies have legitimate interests in protecting their data analytics capabilities as trade secrets, they must also ensure compliance with personal data protection requirements and avoid using data advantages to create anticompetitive market conditions. Indonesian regulators must develop integrated approaches that can accommodate all three legal frameworks while promoting innovation and fair competition in digital markets.

V. COMPARATIVE ANALYSIS: INTERNATIONAL APPROACHES TO BIG DATA PROTECTION

The European Union's (EU) approach to protecting big data through trade secrets is governed by Directive (EU) 2016/943 on Trade Secrets Protection, which establishes harmonized standards across member states. Article 2(1) defines trade secrets as information that is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret. This definition closely parallels the Indonesian framework while providing specific guidance for digital applications. [33]

EU Trade Secrets Directive explicitly acknowledges the intersection between trade secrets and data protection through Recital 35, which states that the directive should not affect the application of data protection rules. Article 1(2) clarifies that the directive applies without prejudice to Union and national rules on the protection of personal data. This regulatory approach provides clear framework for protecting big data analytics and insights as trade secrets while maintaining compliance with GDPR requirements.

[32] Taufiqurrohman, Lita & Pah, *Supra* note 11.

[33] Radoń, *Supra* note 20.

Three major jurisdictions demonstrate convergent approaches to core trade secret requirements while diverging in implementation mechanisms. All jurisdictions require secrecy, economic value, and reasonable protection measures, providing consistent foundation for international businesses operating across multiple legal systems. However, enforcement mechanisms and integration with data protection laws vary significantly.

EU approach prioritizes harmonization with data protection regulations, creating comprehensive framework that balances trade secret protection with individual privacy rights. US framework emphasizes robust enforcement through federal criminal provisions while maintaining flexibility in protection standards. China's approach integrates trade secret protection with broader data sovereignty and cybersecurity objectives.

Banterle's analysis of Italian jurisprudence reveals extensive case law supporting the protection of customer data as trade secrets. Italian courts have recognized that business information may include lists of clients, marketing techniques and datasets of profiled clients, price and discount policies, and data relating to promotions and sales. The Italian Court of Venice stated that "customer lists can be protected as trade secrets even though competitors can easily discover the data of one or more customers." This interpretation suggests that the relative secrecy of aggregated data can satisfy trade secret requirements even when individual data points might be discoverable through other means. [34]

Evolution of European case law also demonstrates increasing recognition of the value of digital marketing data. The Florence Court of Appeal noted that "the importance of customer lists depends on peculiar characteristics: where this concerns a vast mass of customers, even a simple email list can become an important asset."[35] This recognition of the aggregative value of customer data aligns with the characteristics of big data, where value often emerges from the combination and analysis of large datasets rather than individual data points.

The United States (US) has also developed extensive jurisprudence regarding trade secret protection for data. The Defend Trade Secrets Act

[34] *Ibid* 9.

[35] *Ibid* 10.

of 2016 provides federal protection for trade secrets, including data and information that derive independent economic value from not being generally known.[36] American courts have increasingly recognized the protection of customer data, marketing strategies, and business intelligence as trade secrets, provided they meet the statutory requirements of secrecy, economic value, and reasonable protection efforts.[37]

US approach emphasizes practical protection measures and economic value demonstration. Courts have consistently recognized customer data, marketing analytics, and business intelligence systems as protectable trade secrets when companies implement adequate security measures. Economic Espionage Act provides criminal penalties for trade secret theft, including cyber-enabled theft of big data and analytical systems.

China's Anti-Unfair Competition Law (revised 2019) and Criminal Law provide comprehensive trade secrets protection framework. Article 9 of Anti-Unfair Competition Law defines trade secrets as technical information and business information that is not known to public, has commercial value, and is subject to confidentiality measures. Recent amendments specifically address digital economy challenges including data protection and algorithmic trade secrets.

China's Cybersecurity Law and Data Security Law create additional layers of protection for big data while establishing data localization requirements. Article 37 of Cybersecurity Law requires critical information infrastructure operators to store personal information and important data within China, potentially enhancing trade secret protection through jurisdictional control.

Table 1. Comparative Analysis of Trade Secrets Protection Frameworks for Big Data Across Major Jurisdictions

Aspect	European Union	United States	China	Indonesia

[36] Defend Trade Secrets Act of 2016, 18 USC § 1836 (2016).

[37] David S Almeling et al, "A Statistical Analysis of Trade Secret Litigation in Federal Courts" (2010) 45:2 Gonzaga Law Review 291.

Legal Basis	Trade Secrets Directive (EU) 2016/943 + GDPR	Defend Trade Secrets Act (DTSA) 2016 + Uniform Trade Secrets Act (UTSA)	Anti-Unfair Competition Law 2019 + Data Security Law 2021	Law No. 30/2000 on Trade Secrets + Law No. 27/2022 on Personal Data Protection
Definition Requirements	Secret, commercial value due to secrecy, reasonable steps to maintain secrecy	Not generally known, derives economic value from secrecy, reasonable efforts to maintain secrecy	Not known to public, has commercial value, subject to confidentiality measures	Not known to public, has economic value, maintained in secrecy by owner
Big Data Specific Provisions	Explicit recognition in Recital 35 of intersection with data protection	Case-by-case judicial recognition of data analytics as trade secrets	Article 9 includes technical and business information covering algorithmic processes	No explicit big data provisions, relies on broad “other information” clause
Data Protection Integration	Comprehensive coordination with GDPR through Article 1(2)	Limited federal coordination, primarily state-level privacy laws	Integrated framework through Cybersecurity Law and Data Security	Emerging coordination between trade secrets and personal

	and Recital 35		Law	data protection laws
Protection Standards	Harmonized EU-wide standards with member state implementation flexibility	Federal minimum standards with state law variations	Unified national standards with provincial implementation	National standards with limited implementing regulations
Enforcement Mechanisms	Civil remedies, injunctive relief, damages, corrective measures	Civil remedies (DTSA) + criminal penalties under Economic Espionage Act	Civil remedies + criminal penalties under Criminal Law Article 219	Primarily civil remedies including injunctions and damages
Cross-Border Framework	EU-wide jurisdiction with international adequacy decisions	Federal jurisdiction for interstate/international cases	Data localization requirements with controlled cross-border transfers	Limited international enforcement framework
Economic Value Threshold	Commercial value because of secrecy	Independent economic value from not being generally known	Has commercial value and can bring economic benefits	Economic value because useful in business activities
Reasonable	Steps under	Reasonable	Confidential	Appropriat

Protection Measures	circumstances to keep information secret	efforts considering circumstances	ity measures corresponding to commercial value	e and proper steps to maintain secrecy
Reverse Engineering	Explicitly permitted under Article 3	Generally permitted under independent discovery doctrine	Permitted for lawfully obtained products	Not explicitly addressed in current law
Digital Market Focus	Strong emphasis on digital single market integration	Technology sector leadership with flexible adaptation	State-led digital economy development with security priorities	Emerging digital economy with regulatory development needs

Indonesian legal framework shares foundational similarities with all three jurisdictions, particularly in basic trade secret requirements. However, Indonesia can benefit from the EU's approach to data protection integration, the US emphasis on practical enforcement mechanisms, and China's consideration of data sovereignty issues. A hybrid approach incorporating elements from all three jurisdictions could strengthen Indonesia's position in the global digital economy while maintaining regulatory sovereignty.

VI. BIG DATA CHARACTERISTICS AND TRADE SECRET REQUIREMENTS ANALYSIS

A. Secrecy Requirement in the Big Data Context

Big data typically satisfies the secrecy requirement through multiple layers of protection and access control that go beyond traditional information security measures. Modern big data systems employ sophisticated technical measures, including encryption, access controls, authentication systems, and network security protocols, to prevent unauthorized access or disclosure. These technical measures align with the "reasonable steps" requirement outlined in international trade secret frameworks and Indonesian law.

The secrecy of big data is further enhanced by the aggregative nature of the information. While individual data points might be discoverable through public sources or independent collection efforts, the specific combination, organization, and analytical insights derived from big data typically remain proprietary to the collecting organization.[38] This concept of "compilation secrecy" has been recognized in various jurisdictions as sufficient to satisfy trade secret requirements, even when underlying data elements might be individually discoverable.

Italian courts have construed secrecy as a relative rather than absolute concept, meaning that secrecy is present notwithstanding the fact that a third party may recreate the confidential information as long as efforts in time and economic resources are necessary.[39] This interpretation is crucial for big data protection, as competitors might theoretically be able to collect similar data through independent efforts, but the specific methodologies, algorithms, and insights developed by the original collector remain secret.

Furthermore, the processing and analytical capabilities applied to big data often involve proprietary algorithms, machine learning models, and analytical frameworks that are independently protectable as trade secrets.[40] The combination of raw data with sophisticated analytical tools creates layers of secrecy that extend beyond the underlying data to encompass the methods and insights derived from data analysis.

The challenge of maintaining secrecy in an era of increasing data transparency requirements presents unique considerations for Indonesian

[38] Radoń, *Supra* note 20.

[39] Banterle, *Supra* note 47.

[40] Kalin Hristov, "AI-Generated Works and Copyright Authorship: Reinterpreting the Made for Hire Doctrine" (2016) 25 *Stanford Technology Law Review* 440-441.

businesses. The implementation of personal data protection laws creates potential conflicts between the need to maintain data secrecy for trade secret purposes and the obligation to provide transparency about data processing activities to data subjects.[41] Companies must develop sophisticated approaches that can satisfy both trade secret protection requirements and data protection transparency obligations.

B. Economic Value Demonstration in Big Data

The economic value of big data has been extensively documented in academic literature and business practice across multiple dimensions. Martin et al.'s global study demonstrates that data-enabled customer value leads to significant behavioral rewards including increased share of wallet, enhanced loyalty, and reduced switching intentions.[42] The study's findings across four countries show that companies using customer data for personalized experiences achieve measurable competitive advantages and financial returns.

The economic value of big data manifests in multiple forms that clearly satisfy the Indonesian trade secret law requirements. Direct monetization occurs through data licensing, sales, or subscription services where organizations provide access to their datasets for commercial use.[43] Companies like Bloomberg, Reuters, and various market research firms generate billions of dollars in revenue by licensing access to their proprietary datasets and analytical insights.

Indirect monetization involves using data for internal business optimization, customer acquisition, product development, or operational efficiency improvements.[44] The advertising industry exemplifies both forms of monetization, with companies like Google and Facebook generating substantial revenue from data-driven advertising platforms that leverage user behavioral data to deliver targeted advertisements.

[41] Taufiqurrohman, Lita, and Pah, "Tech Giants' Non-Negotiable Privacy Policies," 165.

[42] Martin et al, *Supra* note 2.

[43] OECD, *Supra* note 3.

[44] Banterle, *Supra* note 47.

In the Indonesian context, the economic value of big data is increasingly recognized across various sectors. E-commerce platforms such as Tokopedia and Shopee utilize customer data for personalized recommendations and targeted marketing campaigns that significantly improve conversion rates and customer retention.[45] Financial services companies employ big data for credit scoring, fraud detection, and risk assessment, enabling them to make more accurate lending decisions and reduce operational costs.[46] Telecommunications providers analyze usage patterns for network optimization and service development, resulting in improved service quality and operational efficiency.

The competitive advantage derived from big data analytics represents a form of economic value that extends beyond direct revenue generation. Companies that can effectively analyze large datasets to identify market trends, consumer preferences, or operational inefficiencies gain significant advantages over competitors who lack similar analytical capabilities.[47] This competitive advantage translates into market share gains, premium pricing opportunities, and improved operational performance that clearly demonstrate economic value.

C. Reasonable Protection Measures Implementation

The protection of big data typically involves comprehensive security measures that exceed the "reasonable steps" requirement under trade secret law. Modern data protection practices include technical, administrative, and physical safeguards designed to prevent unauthorized access, use, or disclosure of sensitive information.[48] These measures demonstrate the systematic approach to maintaining secrecy that courts typically require for trade secret protection.

Technical measures commonly employed for big data protection include encryption of data at rest and in transit, access controls with role-based permissions, authentication and authorization systems, network security

[45] Disemadi, *Supra* note 19.

[46] *Ibid.*

[47] Taufiqurrohman, Lita & Pah, *Supra* note 11.

[48] Radoń, *Supra* note 20.

protocols, and monitoring systems for detecting unauthorized access attempts. Advanced security measures such as data masking, tokenization, and differential privacy techniques are increasingly being implemented to protect sensitive information while maintaining analytical utility.[49]

Administrative measures include employee training programs, confidentiality agreements, data handling policies, and incident response procedures. Organizations typically implement comprehensive data governance frameworks that specify how data should be collected, stored, processed, and shared within the organization and with external parties. These administrative controls demonstrate the systematic approach to maintaining secrecy that courts typically require for trade secret protection.[50]

The intersection with data protection law also strengthens the reasonable protection measures analysis. Indonesia's Law Number 27 Year 2022 concerning Personal Data Protection imposes specific security requirements for organizations processing personal data, including risk assessments, security measures proportionate to the risk level, and notification requirements for data breaches.[51] Compliance with these data protection requirements typically satisfies or exceeds the reasonable protection measures required for trade secret protection.

D. Cross-Border Data Transfer and Trade Secret Protection

Globalised digital business operations present intricate challenges for maintaining trade secret protection when big data crosses international borders. Indonesian companies increasingly operate within multi-jurisdictional environments where data collection, processing, and storage occur across different legal systems with varying intellectual property protection standards and data security requirements. Such complexity becomes particularly pronounced within ASEAN regions, where Indonesia functions as a major digital hub while maintaining distinct legal

[49] *Ibid.*

[50] *Ibid.*

[51] Indonesian Personal Data Protection Law, *Supra* note 10 arts 29-30.

frameworks that may not consistently align with neighboring countries' approaches to data protection and intellectual property rights.[52]

Article 22 mandates that personal data of Indonesian citizens be processed within Indonesian territory, establishing limited exceptions for cross-border transfers meeting specific adequacy requirements. While these localization requirements potentially enhance trade secret protection by limiting jurisdictions where sensitive data is stored and processed, they simultaneously create operational challenges for multinational companies relying on global data processing infrastructure.[53]

European Union's General Data Protection Regulation adequacy framework provides valuable guidance for harmonizing data protection standards across jurisdictions while maintaining high security levels. European Commission adequacy decisions recognize certain third countries as providing essentially equivalent data protection levels, enabling free personal data flow without additional safeguards. Indonesia's development of similar adequacy standards could facilitate international data transfers while ensuring trade secret protection measures remain effective across borders.

Maintaining secrecy during cross-border data transfers requires sophisticated technical and legal approaches. Companies must implement end-to-end encryption, secure transmission protocols, and jurisdictional analysis to ensure data remains protected throughout international border crossings. Legal frameworks governing such transfers must account for differences in trade secret protection standards, enforcement mechanisms, and judicial systems across various jurisdictions.[54]

International arbitration mechanisms provide crucial avenues for resolving cross-border trade secret disputes involving big data. Singapore International Arbitration Centre and Indonesian National Board of Arbitration (BANI) have developed specialized procedures for intellectual

[52] Faiz Rahman, "Safeguarding Personal Data In The Public Sector: Unveiling The Impact Of The New Personal Data Protection Act In Indonesia" (2025) 16:1 *UUM Journal of Legal Studies* 1–18.

[53] GR 71/2019 allows private entities to store data outside Indonesia, unlike government systems which must keep data local, online: Conventus Law https://conventuslaw.com/report/indonesia-cross-border-data-transfer.

[54] Ebtihal Althubiti & Michele Sevegnani, "Modelling Privacy Compliance in Cross-border Data Transfers with Bigraphs" (2025) 417 *Electronic Proceedings in Theoretical Computer Science* 20–38.

property disputes accommodating big data cases' technical complexity. These arbitration frameworks offer significant advantages including confidentiality, technical expertise, and enforceability across multiple jurisdictions through international conventions.[55]

Cloud service providers' role in cross-border data transfers creates additional complexity for trade secret protection. Major cloud platforms including Amazon Web Services, Microsoft Azure, and Google Cloud Platform operate data centers across multiple jurisdictions, raising questions about data processing locations and applicable legal frameworks. Indonesian companies must carefully evaluate cloud service agreements to ensure trade secret protection requirements are maintained regardless of data processing's physical location.

Data sovereignty considerations intersect with trade secret protection in complex ways requiring careful policy coordination. While data sovereignty aims to ensure national control over territorially generated data, trade secret protection seeks to provide legal certainty for companies investing in data-driven innovations. Tension between these objectives requires nuanced approaches accommodating both national security concerns and commercial innovation incentives.

Regional data governance frameworks emergence, including ASEAN Digital Data Governance Framework and Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) digital trade provisions, creates opportunities for harmonizing cross-border data transfer rules while maintaining trade secret protection. These frameworks recognize digital trade facilitation importance while preserving legitimate regulatory autonomy over data protection and intellectual property rights.[56]

Practical implementation of cross-border trade secret protection requires companies to develop comprehensive data governance strategies accounting for multiple legal jurisdictions. Such strategies must include jurisdictional mapping of data flows, risk assessments for each transfer destination,

[55] Thomas D. Halket, Arbitration of International Intellectual Property Disputes, 2nd ed (2021, ArbitrationLaw.com).

[56] Supatsara Chaipipat, ASEAN governance on data privacy : challenges to regional protection of data privacy and personal data in cyberspace (Master's Degree, Chulalongkorn University, 2019).

contractual safeguards with international partners, and incident response procedures for potential breaches occurring in foreign jurisdictions.[57] Companies must also maintain detailed protection measures documentation to demonstrate compliance with trade secret requirements across all relevant jurisdictions.

VII. IMPLEMENTATION CHALLENGES AND LEGAL HARMONISATION

The implementation of big data protection through trade secrets mechanisms in Indonesia faces several challenges that require careful consideration and strategic planning. These challenges span legal, technical, and practical dimensions that must be addressed to ensure effective protection and enforcement.

One primary challenge involves the intersection between trade secret protection and data protection laws. While Law Number 30 Year 2000 concerning Trade Secrets and Law Number 27 Year 2022 concerning Personal Data Protection are not inherently contradictory, they establish different frameworks with potentially conflicting requirements.[58] Trade secret law emphasizes maintaining secrecy and restricting access to protected information, while data protection law emphasizes individual rights including access, portability, and erasure of personal data.

The challenge becomes particularly acute when individuals exercise their rights under data protection law in ways that could compromise trade secret protection. For example, the right to data portability might require organizations to provide structured, machine-readable copies of personal data to individuals, potentially undermining the secrecy of proprietary data compilation and analytical methods.[59] Similarly, the right to access might require disclosure of information about data processing activities that could reveal trade secret methodologies.

[57] Eugénie Coche, Ans Kolk & Václav Ocelík, "Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business" (2024) 7:1 *Journal of International Business Policy* 119.

[58] Taufiqurrohman, Lita & Pah, *Supra* note 16.

[59] *Ibid.*

The dominance of certain technology companies in data collection and processing creates additional challenges for trade secret protection and competition law enforcement. When a small number of companies control vast amounts of data and the analytical tools to process them, the traditional balance between trade secret protection and competition may be disrupted.[60] Indonesian regulators must develop approaches that can protect legitimate trade secrets while preventing the use of trade secret claims to maintain anticompetitive market positions.

Another significant challenge involves the enforcement mechanisms available under Indonesian law. While Law Number 30 Year 2000 concerning Trade Secrets provides civil remedies including injunctive relief and damages, the practical enforcement of these remedies in the context of big data requires specialized technical expertise and sophisticated investigative capabilities.[61] Courts and enforcement agencies may lack the technical knowledge necessary to evaluate complex big data systems and determine whether unauthorized access or use has occurred.

Rapid digital technology evolution presents ongoing challenges for legal frameworks designed to protect big data as trade secrets. Artificial intelligence and machine learning systems increasingly operate as autonomous agents discovering patterns and generating insights without direct human intervention, raising fundamental questions about secrecy nature and trade secret rights attribution. Traditional human-generated trade secrets concepts must evolve to accommodate AI-generated insights that may possess significant commercial value but lack clear human authorship.[62]

Machine learning algorithms present particular challenges for trade secret protection due to their dynamic and evolving nature. Unlike traditional trade secrets remaining relatively static, machine learning models continuously update and improve through new data exposure. This evolutionary characteristic raises questions about whether protection extends to algorithm current state, training data, learning methodology, or

[60] Taufiqurrohman, Lita & Pah, *Supra* note 11.

[61] Indonesian Trade Secrets Law, *Supra* note 9 art 11.

[62] Katarina Foss-Solbrekk, "Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly" (2021) 16:3 *Journal of Intellectual Property Law & Practice* 249.

all combined elements. Indonesian courts and policymakers must develop frameworks accommodating AI-generated trade secrets' dynamic nature while maintaining clear protection boundaries.

Algorithmic transparency concepts, increasingly demanded by regulators and consumers, create tension with AI systems trade secret protection. European Union regulations including proposed AI Act require certain explainability and transparency levels for AI systems used in high-risk applications. Indonesia's AI governance frameworks development must balance transparency requirements with legitimate business needs to protect proprietary algorithms and training methodologies as trade secrets.[63]

Internet of Things (IoT) devices create new data categories potentially qualifying for trade secret protection, including sensor data from industrial equipment, behavioral patterns from smart home devices, and location intelligence from connected vehicles.[64] Distributed IoT data collection nature requires sophisticated approaches to maintaining secrecy across multiple devices, networks, and processing systems. Each IoT device represents potential vulnerability points where trade secret information could be compromised, necessitating comprehensive security architectures extending protection to edge computing environments.[65]

Industrial IoT applications in Indonesia's manufacturing sector demonstrate sensor-generated big data commercial value. Companies operating in automotive, textile, and electronics manufacturing use IoT sensors to collect detailed operational data enabling predictive maintenance, quality optimization, and supply chain efficiency improvements. Aggregated insights derived from sensor data often constitute valuable trade secrets providing competitive advantages in global markets.

Blockchain and distributed ledger technologies present unique trade secret protection challenges due to their inherently transparent and decentralised nature. While blockchain systems provide strong security and immutability

[63] Ulla-Maija Mylly, "Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information" (2023) 54:7 *IIC-International Review of Intellectual Property and Competition Law* 1013–1043.

[64] Adi Ahmad, Riyan Maulana & Khairul Akmal, "Data Privacy and Security in the Age of IoT A Comprehensive Study on Information System Vulnerabilities" (2024) 6:2 *Journal Informatic, Education And Management (JIEM)* 1–7.

[65] *Ibid.*

guarantees, many blockchain networks' public nature conflicts with trade secret law secrecy requirements. Companies must develop innovative approaches leveraging blockchain benefits while maintaining necessary confidentiality, including private blockchain networks, zero-knowledge proofs, and selective disclosure mechanisms.

Quantum computing technologies' emergence poses both opportunities and threats for big data context trade secret protection. Quantum computers' potential ability to break current encryption standards could undermine existing technical protection measures for trade secrets, requiring the development of quantum-resistant security protocols. Conversely, quantum technologies may enable new data analysis and pattern recognition forms, generating valuable trade secrets requiring protection.[66]

Edge computing architectures, processing data closer to sources rather than centralised cloud facilities, create new trade secret protection considerations. While edge computing can enhance security by reducing data transmission and third-party facility storage, it also distributes sensitive processing across multiple locations, potentially having varying physical and technical security levels.[67] Companies must develop edge computing strategies, maintaining trade secret protection while capitalising on distributed processing performance and latency benefits.[68]

5G networks integration and advanced telecommunications infrastructure enable new real-time data processing and analysis forms, potentially generating protectable trade secrets. 5G networks' low latency and high bandwidth capabilities facilitate applications, including autonomous vehicle coordination, smart city management, and industrial automation, relying on real-time big data analytics. Insights generated by these applications often constitute valuable trade secrets requiring protection frameworks adapted to high-speed, distributed processing environments.

Digital twin technologies, creating virtual representations of physical systems using real-time data feeds, represent another trade secret protection

[66] Aykut Karakaya & Ahmet Ulu, A Survey on Post-Quantum Based Approaches for Edge Computing Security (2024) WIREs Computational Statistics.

[67] *Ibid.*

[68] Anum Nawaz et al, "Edge computing to secure IoT data ownership and trade with the Ethereum blockchain" (2020) 20:14 *Sensors* 3965.

frontier. Mathematical models, simulation algorithms, and predictive analytics embedded in digital twins often constitute valuable proprietary information enabling companies to optimise operations, predict failures, and design improvements. Indonesian manufacturing and infrastructure companies increasingly rely on digital twin technologies, generating trade secret-protected insights about operational efficiency and performance optimisation.[69]

VIII. POLICY RECOMMENDATIONS AND IMPLEMENTATION FRAMEWORK

A. Regulatory Framework Enhancement and Legal Harmonisation

Indonesian policymakers must prioritise developing comprehensive implementing regulations that specifically address big data protection under trade secret law to provide clarity for businesses and legal practitioners. Current regulatory gaps create uncertainty about how traditional trade secret principles apply to modern data-driven business models, potentially discouraging investment in data analytics capabilities and hindering Indonesia's digital transformation goals. Proposed implementing regulations should establish clear guidelines for determining when big data qualifies for trade secret protection, specify documentation requirements for demonstrating reasonable protection measures, and provide safe harbour provisions for companies implementing recognised best practices.

The Ministry of Law and Human Rights should collaborate with the Ministry of Communication and Informatics to develop joint regulations addressing the intersection between trade secret protection and data protection requirements. Such collaboration ensures regulatory consistency and prevents conflicting obligations that could undermine both trade secret protection and individual privacy rights. The joint regulatory development process should include extensive stakeholder consultation with technology companies, legal practitioners, academic institutions, and civil society organisations to ensure balanced approaches that accommodate diverse interests and perspectives.

[69] *Ibid.*

Regulatory sandbox mechanisms could provide valuable testing environments for new approaches to big data protection under trade secret law. Similar to fintech regulatory sandboxes that allow controlled testing of innovative financial services, data protection sandboxes could enable companies to experiment with novel protection mechanisms while providing regulators with practical insights about implementation challenges and effectiveness. Sandbox participants could receive temporary regulatory relief from certain requirements in exchange for detailed reporting about protection measures, economic impacts, and potential risks or benefits.[70]

Legislative amendments to Law Number 30 Year 2000 concerning Trade Secrets may be necessary to explicitly address digital age challenges, including AI-generated insights, cross-border data flows, and automated protection systems. While current law provides sufficient flexibility for protecting big data as trade secrets, explicit recognition of digital applications could enhance legal certainty and provide a stronger foundation for enforcement actions.[71] Proposed amendments should clarify application to algorithmic processes, specify requirements for protecting dynamically generated insights, and establish frameworks for international cooperation in trade secret enforcement.

B. Industry-Specific Implementation Guidelines

Different industrial sectors require tailored approaches to implementing big data protection for trade secrets, given varying data types, business models, regulatory environments, and competitive dynamics. The financial services sector faces unique challenges in balancing trade secret protection with prudential regulations that require transparency into risk management systems and credit scoring methodologies. Bank Indonesia and Financial Services Authority (OJK) should develop sector-specific guidelines addressing how financial institutions can protect proprietary analytical

[70] Deirdre Ahern, "Operationalising AI Regulatory Sandboxes under the EU AI Act: The Triple Challenge of Capacity, Coordination and Attractiveness to Providers" (2025) arXiv 3.

[71] Camilla Alexandra Hrdy, "Trade Secrets and Artificial Intelligence" in Ryan Abbott & Elizabeth Rothman, eds, Elgar Concise Encyclopedia of Artificial Intelligence and the Law (Cheltenham, UK: Edward Elgar, forthcoming 2026).

models while complying with supervisory requirements for algorithmic transparency and fairness.[72]

The healthcare sector presents a complex intersection between trade secret protection, patient privacy rights, and public health interests. The Ministry of Health should establish guidelines for protecting medical research data, diagnostic algorithms, and treatment optimisation systems as trade secrets while ensuring compliance with medical ethics standards and patient consent requirements. Healthcare guidelines must address data sharing for public health emergencies, research collaboration requirements, and international standards for medical data protection.

E-commerce and digital platform companies require guidance on protecting customer analytics, recommendation algorithms, and marketplace optimisation systems while complying with consumer protection regulations and competition law requirements. The Ministry of Trade should develop e-commerce-specific guidelines addressing platform data protection, vendor relationship management, and cross-border marketplace operations. Such guidelines should clarify when customer data aggregation constitutes protectable trade secrets versus when it may raise competition law concerns about market dominance. [73]

The manufacturing sector increasingly relies on Industrial Internet of Things (IIoT) systems, generating valuable operational data about production processes, supply chain optimisation, and predictive maintenance. The Ministry of Industry should establish manufacturing-specific guidelines for protecting sensor data, process optimisation algorithms, and supply chain intelligence as trade secrets. Guidelines must address international supply chain data sharing, equipment vendor relationships, and integration with global manufacturing networks.

The agricultural sector faces unique challenges in protecting farm-level data, crop prediction models, and supply chain optimisation systems while participating in global food security initiatives and research collaborations.

[72] Emmanuel A. Abbe, Amir E. Khandani & Andrew W. Lo, 'Privacy-Preserving Methods for Sharing Financial Risk Exposures' (2012) 102:3 *American Economic Review* 65

[73] Tomisin Awosika, Raj Mani Shukla & Bernardi Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection" (2024) 12 *IEEE Access* 64559.

The Ministry of Agriculture should develop agricultural data protection guidelines that address farmers' data rights, research data-sharing obligations, and international agricultural trade requirements. Such guidelines must balance protecting Indonesian agricultural competitiveness with supporting global food security and climate change adaptation efforts.

C. Enforcement Mechanism Strengthening

Indonesian courts require specialised training and resources to adjudicate trade secret disputes involving big data, given the technical complexity of digital systems and the rapidly evolving technology landscape. The Supreme Court should establish specialised intellectual property chambers with judges trained in digital technology, data analytics, and cybersecurity principles. Judicial training programs should include technical education about big data systems, hands-on experience with data analytics tools, and case study analysis of international trade secret disputes involving digital assets.

Expert witness certification programs could enhance judicial decision-making quality by ensuring technical experts possess necessary qualifications and maintain independence from parties in trade secret litigation. Indonesian Institute of Sciences (LIPI) and professional organisations should develop certification standards for data science experts, cybersecurity specialists, and digital forensics investigators. Certified expert witness programs should include continuing education requirements, ethical standards, and peer review mechanisms to maintain expertise, currency and professional integrity.[74]

Alternative dispute resolution mechanisms specifically designed for trade secret disputes could provide faster, more cost-effective resolution while maintaining necessary confidentiality. Indonesian National Board of Arbitration (BANI) should develop specialised arbitration rules for intellectual property disputes involving digital assets, including expedited

[74] Direktorat Jenderal Kekayaan Intelektual, DJKI Gelar Master Training Program on IP and Geographical Indications (5 November 2024), online: DJKI https://www.dgip.go.id/artikel/detail-artikel-berita/djki-gelar-master-training-program-on-intellectual-property-and-geographical-indications?kategori=liputan-humas.

procedures for preliminary injunctions, technical expert panels, and confidentiality protections for sensitive business information. Mediation programs could help parties resolve disputes without expensive litigation while preserving ongoing business relationships.[75]

Digital forensics capabilities must be enhanced to support trade secret enforcement in big data contexts where evidence may be distributed across multiple systems, jurisdictions, and technological platforms. The National Police Cyber Crime Unit should receive advanced training in data analytics forensics, cloud computing investigations, and international evidence gathering procedures. Forensics capabilities should include specialised tools for analysing big data systems, preserving digital evidence integrity, and reconstructing data access patterns to determine potential trade secret misappropriation.[76]

Cross-border enforcement cooperation requires strengthening international relationships and developing mutual legal assistance frameworks specifically addressing digital trade secret disputes. The Ministry of Law and Human Rights should negotiate bilateral agreements with major trading partners, establishing procedures for evidence gathering, witness testimony, and enforcement action coordination in trade secret cases involving cross-border elements. International cooperation frameworks should address jurisdictional conflicts, evidence admissibility standards, and enforcement mechanism harmonisation.[77]

D. Enforcement Mechanism Strengthening

Legal education programs must incorporate comprehensive coverage of digital intellectual property issues, including big data protection, algorithmic trade secrets, and technology-driven business models. Law schools should develop specialised curricula covering the intersection

[75] I Pratama, I S Pratama & D S H Marpaung, "Perlindungan hukum dan peran Badan Arbitrase Nasional Indonesia (BANI) dalam penyelesaian sengketa hak atas merek" (2022) 9:1 *Justitia: Jurnal Ilmu Hukum dan Humaniora* 452.

[76] Mohammed I Alghamdi, "Digital forensics in cyber security—recent trends, threats, and opportunities" in Cybersecurity Threats with New Perspectives (2021) 13.

[77] Zhuan Zuo, "Cross-Border Data Forensics: Challenges and Strategies in the Belt and Road Initiative Digital Era" (2025) *Asian Social Science* 5.

between intellectual property law, data protection regulations, and competition law in digital markets. Legal education should include practical training with data analytics tools, case study analysis of technology disputes, and interdisciplinary collaboration with computer science and business programs.[78]

Professional development programs for practising lawyers should address the rapidly evolving landscape of digital intellectual property law and provide practical skills for representing clients in technology-related disputes. The Indonesian Bar Association should establish continuing legal education requirements for intellectual property practitioners, including specialised certification programs for digital IP law.[79] Professional development should include technical training, international best practices study, and networking opportunities with technology industry professionals.

Government agency capacity building requires comprehensive training programs for regulators, enforcement officials, and policymakers responsible for digital economy oversight. The Civil Service Agency should develop specialised training curricula for officials working on digital policy issues, including technical education about emerging technologies, international regulatory trends analysis, and stakeholder engagement skills. Capacity building programs should include exchange programs with leading digital economy jurisdictions and collaboration with international organisations.

Academic research capacity enhancement could support evidence-based policy development and provide a theoretical foundation for Indonesian approaches to digital intellectual property protection. The Ministry of Research and Technology should fund research programs examining the intersection between intellectual property law and emerging technologies, with particular focus on Indonesian economic development priorities. Research initiatives should include international collaboration

[78] Georg Borges & Christoph Sorge, eds, Law and Technology in a Global Digital Society: Autonomous Systems, Big Data, IT Security and Legal Tech (Cham: Springer, 2022) 28.

[79] Dina Dellyana, Nina Arina & Tribowo Rachmat Fauzan, "Digital innovative governance of the Indonesian creative economy: A governmental perspective" (2023) 15:23 *Sustainability* 162.

opportunities, industry partnership programs, and policy-relevant research dissemination mechanisms.[80]

Private sector engagement mechanisms should facilitate ongoing dialogue between government agencies and technology companies about implementation challenges, emerging issues, and policy effectiveness. Regular stakeholder consultation processes could identify practical problems with existing regulations and provide input for policy refinements. Industry engagement should include both multinational technology companies and domestic Indonesian firms to ensure balanced perspectives and support for local innovation ecosystem development.

VI. CONCLUSION

The comprehensive analysis of big data conceptualisation within Indonesia's trade secrets legal framework reveals a significant relationship between the characteristics of big data and the fundamental requirements established in Law Number 30 of 2000 concerning Trade Secrets. This research demonstrates that big data can be effectively protected as trade secrets in Indonesia, provided that organisations implement appropriate measures to satisfy the three essential criteria of secrecy, economic value, and reasonable protection measures. The secrecy requirement is fulfilled through the aggregative nature of big data, where the specific combination, organisation, and analytical insights derived from large datasets remain proprietary despite individual data points potentially being discoverable through independent means. The economic value criterion is clearly satisfied by the substantial commercial benefits that Indonesian companies across various sectors derive from big data applications, including personalised marketing, predictive analytics, fraud detection, and operational optimisation. The reasonable protection measures requirement is met through comprehensive security frameworks that typically exceed minimum legal standards, incorporating both technical safeguards such as encryption and access controls, and administrative measures including employee training and confidentiality agreements.

[80] *Ibid.*

The intersection between trade secret protection and competition law enforcement creates additional complexity that requires careful policy attention. The dominance of certain technology companies in data collection and analysis may create situations where trade secret protection could be used to maintain anticompetitive advantages, necessitating a balanced approach that protects legitimate business interests while ensuring fair competition. The policy recommendations outlined in this research provide a roadmap for addressing these challenges and enhancing Indonesia's legal framework for big data protection through the development of implementing regulations, harmonization between different legal regimes, capacity building initiatives, and international cooperation efforts

ACKNOWLEDGMENTS

None.

ARTIFICIAL INTELLIGENCE USE STATEMENT

The author declares that Artificial Intelligence (AI)-based tools were used in a limited capacity during the preparation of this manuscript, submitted to *Jurnal Kajian Pembaharuan Hukum*. AI tools were used solely for grammar and language editing, as well as for assisting in drafting and outlining certain parts of the manuscript. No AI tools were used for data analysis or visualisation. The author confirms that no part of the manuscript was entirely generated by AI without human review, editing, and intellectual contribution. The author takes full responsibility for the accuracy, originality, and integrity of the content. The use of AI in the preparation of this manuscript does not violate research ethics, authorship criteria, or publication integrity.

REFERENCES

Adi Ahmad, Riyan Maulana & Khairul Akmal, “Data Privacy and Security in the Age of IoT A Comprehensive Study on Information System

Vulnerabilities" (2024) 6:2 *Journal Informatic, Education And Management (JIEM)* 1–7.

Althubiti, Ebtihal & Michele Sevegnani, "Modelling Privacy Compliance in Cross-border Data Transfers with Bigraphs" (2025) 417 *Electronic Proceedings in Theoretical Computer Science* 17–38.

Awosika, Tomisin, Raj Mani Shukla & Bernardi Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection" (2024) 12 *IEEE Access* 64551–64560.

Chaipipat, Supatsara, ASEAN governance on data privacy : challenges to regional protection of data privacy and personal data in cyberspace (Master's Degree, Chulalongkorn University, 2019).

Coche, Eugénie, Ans Kolk & Václav Ocelík, "Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business" (2024) 7:1 *Journal of International Business Policy* 112–127.

Danmadiyah, Shevierra et al, "A Party's Recall Right in the Concept of Democratic Country" (2019) 19:2 *Syariah: Jurnal Hukum dan Pemikiran* 151.

David S Almeling et al, "A Statistical Analysis of Trade Secret Litigation in Federal Courts" (2010) 45:2 *Gonzaga Law Rev* 291.

Foss-Solbrekk, Katarina, "Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly" (2021) 16:3 *Journal of Intellectual Property Law & Practice* 247–258.

Hari Sutra Disemadi, "Data Ownership in Regulating Big Data in Indonesia Through the Perspective of Intellectual Property" (2022) 13:2 *Jurisdictie: Jurnal Hukum dan Syariah* 188.

Herbert Zech, "A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data" (2016) 11:6 *Journal of Intellectual Property Law and Practice* 460.

Kalin Hristov, “AI-Generated Works and Copyright Authorship: Reinterpreting the Made for Hire Doctrine” (2016) 25 *Stanford Technology Law Review* 440-441.”

Kelly D Martin et al, “Data Privacy in Retail” (2020) 96:4 *Journal of Retailing* 474.

Konrad Zweigert & Hein Kötz, An Introduction to Comparative Law, 3rd ed (Oxford: Oxford University Press, 1998).

Meglena Kuneva, “Keynote Speech: Roundtable on Online Data Collection, Targeting and Profiling” (European Commission, Brussels, 31 March 2009), online: European Commission.

Moch Marsa Taufiqurrohman, “Otomatisasi Dan Kecerdasan Buatan Pada Profesi Hukum: Kerangka Teoritis Dan Narasi Ideal Di Masa Depan” (2024) 13:2 Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional 195.

Moch Marsa Taufiqurrohman, Helza Nova Lita & Gress Gustia Adrian Pah, “Digital Markets and Data Exploitation: Addressing Abuse of Dominance Under Indonesian Competition Law” (2024) 25:1 Jurnal Penelitian Hukum De Jure 1.

Moch Marsa Taufiqurrohman, Helza Nova Lita & Gress Gustia Adrian Pah, “Tech Giants’ Non-Negotiable Privacy Policies Strategy Versus Indonesian Competition Law” (2024) 9:1 Jurnal Bina Mulia Hukum 159.

Moch Marsa Taufiqurrohman, Helza Nova Lita & Gress Gustia Adrian Pah, “The Interrelation Between Personal Data Protection and Competition Legal Regime in the Indonesian Digital Market” (2024) 8:3 Syiah Kuala Law Journal 275.

Mylly, Ulla-Maija, “Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information” (2023) 54:7 *IIC-International Review of Intellectual Property and Competition Law* 1013–1043.

Peter Mahmud Marzuki, Penelitian Hukum (Jakarta: Kencana Prenada Media Group, 2019).

Pratama, Ilham Septian & Devi Siti Hamzah Marpaung, “Perlindungan hukum dan peran Badan Arbitrase Nasional Indonesia (BANI) dalam penyelesaian sengketa hak atas merek” (2022) 9:1 *Justitia: Jurnal Ilmu Hukum dan Humaniora* 452.

Rahman, Faiz, “Safeguarding Personal Data In The Public Sector: Unveiling The Impact Of The New Personal Data Protection Act In Indonesia” (2025) 16:1 *UUM Journal of Legal Studies* 1–18

Soerjono Soekanto & Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat (Jakarta: Rajawali Pers, 2020).

Sudikno Mertokusumo, Mengenal Hukum: Suatu Pengantar (Yogyakarta: Cahaya Atma Pustaka, 2019).