Syiah Kuala Law Journal
FAKULTAS HUKUM UNIVERSITAS SYIAH KUALA
Vol.8 (3) Desember 2024, pp. 346-360
ISSN : 2580-9059 (online)
2549-1741 (print)

# THE INTERRELATION BETWEEN PERSONAL DATA PROTECTION AND COMPETITION LEGAL REGIME IN THE INDONESIAN DIGITAL MARKET

**Moch. Marsa Taufiqurrohman[1], Helza Nova Lita[2], Gress Gustia Adrian Pah[3]**
[1, 2)] Faculty of Law Universitas Padjadjaran [3)] Faculty of Law Universitas Airlangga

**Article Info**
Received: 09/10/2024
Approved: 30/11/2024

**Keywords:**
Personal Data Protection, Competition, Digital Market, Technology, Disruption

**Abstract**
Indonesia's rapidly expanding digital market presents both opportunities and challenges, particularly in balancing innovation with the protection of personal data and fair competition. This research examines the intersection of personal data protection and competition law within the Indonesian legal framework, analyzing the foundational concepts of each and their interrelation in the digital market. Indonesia has taken steps to address these concerns through Law No. 27 of 2022 on Personal Data Protection and Law No. 5 of 1999 on Competition. However, the research argues that these frameworks require strengthening to address the unique challenges posed by data-driven dominance. The reliance on user consent for data processing is challenged, given the potential for exploitation by dominant players. The research highlights the limitations of traditional competition metrics in the digital age and advocates for a more nuanced approach. This includes recognizing data-driven barriers to entry, rethinking the efficacy of consent, and empowering consumers through data portability and digital literacy initiatives. By strengthening legal frameworks and adopting a more comprehensive approach, Indonesia can foster a digital ecosystem that is both innovative and fair, benefiting all stakeholders.



***Corresponding Author:***
Moch. Marsa Taufiqurrohman
Email: moch23009@mail.unpad.ac.id

## I. INTRODUCTION

The Indonesian archipelago, home to a vibrant tapestry of cultures and a rapidly developing economy is undergoing a profound digital transformation. With over 270 million people, Indonesia boasts one of the world's largest and fastest-growing digital markets, fueled by widespread smartphone penetration, a burgeoning e-commerce sector, and a voracious appetite for digital content and services. This digital revolution holds immense promise for economic growth, social inclusion, and improved quality of life. However, it also presents a unique set of challenges, particularly in balancing the dynamism of innovation with the imperative to safeguard fundamental rights, especially in the realm of personal data protection and fair competition (Wachter & Mittelstadt, 2019).

This research delves into a crucial intersection within this evolving digital landscape: the interrelation between personal data protection and competition law. Traditionally viewed as distinct areas of law, they are becoming increasingly intertwined in the digital age, where personal data has emerged as a valuable commodity, a source of economic value, and a potential tool for establishing and entrenching market dominance. The digital market, characterized by platform-based business

models, network effects, and data-driven innovation, challenges traditional notions of competition. The ability to collect, analyze, and leverage vast datasets, often gleaned from users in exchange for "free" services, has become a key driver of market power. This raises concerns about data exploitation, unfair competition, and the potential for dominant players to stifle innovation and harm consumer welfare (Li et al., 2021).

Indonesia has taken commendable steps to address both data protection and competition concerns. Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a significant milestone in establishing a comprehensive data protection regime, while Law No. 5 of 1999 on the Prohibition of Monopolistic Practices and Unfair Business Competition (Competition Law) provides the legal basis for regulating anti-competitive conduct. However, the rapid evolution of the digital market necessitates a constant reassessment of existing legal frameworks. This research argues that while Indonesia's current laws provide a crucial foundation, they require further strengthening and a more nuanced approach to effectively address the unique challenges posed by data-driven dominance (Jain, Gyanchandani, & Khare, 2016).

This research aims to contribute to the ongoing discourse surrounding data protection and competition in the digital age, offering valuable insights and recommendations for policymakers, regulators, businesses, and consumers in Indonesia. By fostering a deeper understanding of the complex interplay between data, innovation, and competition, this research seeks to promote a digital future that benefits all stakeholders while safeguarding fundamental rights and fostering a more inclusive and dynamic digital economy. This article examines the interaction between data privacy and competition law regimes within the Indonesian legal framework. The research seeks to answer two key questions. First, Fundamental Concepts: What are the foundational legal concepts of the digital market, data privacy, and competition law in Indonesia? Second, Interrelation of Regimes: How do the legal regimes governing data privacy and competition law interrelate within Indonesia's digital market?

The article is structured as follows: following an introduction and a description of the research methodology, the subsequent section will delve into the fundamental legal concepts of the digital market, data privacy, and competition law in Indonesia. This discussion is crucial, guided by the legal maxim "*Ad Recte docendum oportet primum inquirere nomina, quia rerum cognitio a nominibus rerum dependet,*" a classical legal postulate emphasizing the importance of establishing clear definitions as a prerequisite for legal understanding. Therefore, it is essential to begin the research by establishing a clear understanding of the fundamental concepts related to the digital market, data privacy, and competition law in Indonesia.

The following section will discuss the core issue: the interrelation between data privacy and competition law regimes in Indonesia's digital market. This section will address the primary research

question. Finally, the article will conclude by presenting key findings and offering recommendations for further consideration.

## II. METHOD

This research employs a doctrinal legal research method, specifically normative legal research, combined with a Reform Oriented Research approach. Normative legal research involves examining legal products, legal principles, legal systematics, legal synchronization, both vertically and horizontal legal synchronization, and comparative law, including historical legal analysis. This research also incorporates the Reform Oriented Research method. This method evaluates the adequacy of existing regulations and recommends necessary changes (Taufiqurrohman, Jayus, & Efendi, 2022). This method empowers researchers to propose new legal principles that can be incorporated into the legal framework, potentially informing future law enforcement practices.

## III. RESULTS AND DISCUSSION

### 3.1. The Concept of the Digital Market, Personal Data Protection, and Business Competition

The digital market has emerged as a significant economic force, reshaping the traditional business landscape and unlocking countless new opportunities. Driven by widespread internet penetration and rapid technological adoption, the digital market is transforming how we transact, interact, and access information (Whish & Bailey, 2021).

The digital market possesses unique characteristics that distinguish it from traditional markets. Firstly, it transcends geographical boundaries. Transactions can occur anytime, anywhere, surpassing geographical limits and time zones. This enables businesses to reach global customers without establishing physical infrastructure in each location. Secondly, it offers abundant information. Users have access to comprehensive and transparent information about products and services. They can readily compare prices, read reviews, and make more informed purchasing decisions. Thirdly, it reduces transaction costs. The digital market can lower operational expenses like rent and logistics, allowing businesses to offer more competitive prices and reach wider market segments (Martin, Borah, & Palmatier, 2017).

The digital market presents numerous opportunities for businesses, consumers, and the economy as a whole. Businesses can access international markets with greater ease and cost-effectiveness. Global e-commerce platforms and social media enable businesses to market their products and services to users worldwide. The digital market fosters innovation by creating opportunities to develop new products and services that cater to evolving consumer needs. New business models, such as the sharing economy and on-demand services, are flourishing in the digital age. The digital market can enhance the efficiency of supply chains, payment processes, and customer service. Technologies like cloud computing, big data analytics, and artificial intelligence (AI)

empower businesses to optimize their operations and deliver superior customer experiences (Taufiqurrohman, 2022).

However, the digital market also presents challenges that require attention. Ease of access to the global market translates to increased competition. Businesses must innovate and adapt rapidly to remain competitive in the dynamic digital landscape. Online transactions are vulnerable to cybersecurity threats like data breaches and fraud. Businesses and consumers must implement robust security measures to safeguard their sensitive data. The digital market raises new challenges regarding consumer protection, such as data privacy, transaction security, and online dispute resolution. Effective regulations and robust law enforcement are crucial for protecting the rights of both consumers and businesses in the digital age (Taufiqurrohman & Gultom, 2023).

One of the most critical aspects of the digital market is the protection of personal data belonging to users of digital services. Personal data protection is grounded in several theories. Firstly, the theory of Human Rights (hereinafter referred to as "HR") forms a cornerstone in shaping the theory of personal data protection. HR principles, such as the right to privacy, freedom of expression, and access to information, underpin the argument for safeguarding personal data. The right to privacy is a fundamental right recognized in various international HR instruments. Personal data is an integral part of an individual's private life. Unauthorized collection, processing, and dissemination of personal data constitute a violation of this right. Article 12 of the Universal Declaration of Human Rights states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (Liang, Weller, Luo, Zhao, & Dong, 2018).

Article 17 of the International Covenant on Civil and Political Rights (hereinafter referred to as "ICCPR") further states: "(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks."

Personal data protection is also closely intertwined with the right to freedom of expression and access to information. Excessive collection and use of personal data can have a chilling effect on individuals' ability to express themselves freely, especially if they fear potential misuse of their data. Individuals have the right to know how their personal data is collected, processed, and used. They also have the right to access, correct, and delete their personal data (Taufiqurrohman, Fahri, Wijaya, & Wiranata, 2021a).

The theory of HR provides a normative framework for developing laws and policies on personal data protection. Several HR principles underpin this protection: (1) Principle of Legality: Personal data collection and processing must have a clear and lawful basis. (2) Principle of Proportionality and Necessity: Data collection and processing must be for legitimate purposes and proportionate to those purposes. (3) Principle of Transparency and Accountability: Individuals must

receive clear and understandable information about how their data is collected, processed, and used. (3) Principle of Data Security: Data controllers must implement appropriate measures to protect personal data from unauthorized access, use, or disclosure (Botta & Wiedemann, 2018).

While HR theory offers a strong foundation for personal data protection, its real-world implementation faces challenges. Rapid technological advancements, like AI and big data, enable large-scale personal data collection and analysis. Furthermore, public awareness of their data rights remains limited, and weak law enforcement and data protection mechanisms persist in some countries (Jones & Sufrin, 2016).

The Second Theory: Contract Theory. Contract theory offers a compelling perspective for understanding and regulating the relationship between individuals as data subjects and entities seeking to process their personal data. This theory posits that interactions between individuals and data controllers constitute a form of agreement or contract. When an individual provides personal data, whether knowingly or unknowingly, an implicit or explicit agreement is deemed to exist regarding the data's collection, processing, and use. (1) Explicit consent is given consciously and clearly through written or electronic documents, such as Terms of Service agreements on online platforms or data collection consent forms. (2) Implicit consent is inferred based on the context of the interaction, even if not explicitly stated in writing. For instance, providing a phone number to an online store during checkout is considered implicit consent to receive promotional information via text message (Thoben, Wiesner, & Wuest, 2017).

Contract theory empowers individuals as holders of their personal data, allowing them to "accept" or "reject" contracts with data controllers. This approach enables more dynamic and specific arrangements tailored to the type of data, processing purposes, and potential risks involved. Furthermore, contract theory promotes: (1) Transparency and Informed Consent: Data controllers must provide clear, concise, and easily understandable information about their data collection, use, and sharing practices. (2) Individual Choice and Control: Individuals must have meaningful choices and greater control over their data, including the right to withdraw consent, access, rectify, and erase their data (Xu, Jiang, Wang, Yuan, & Ren, 2014).

Despite its limitations, contract theory provides a useful framework for understanding and regulating the data subject-controller relationship. However, its implementation must carefully balance individual interests with business needs while ensuring individuals maintain adequate control over their personal data (Lloyd, 2020).

The Third Theory: Economic Analysis of Law. Economic Analysis of Law (hereinafter "EAL") offers a unique lens through which to examine personal data protection by analyzing it through an economic framework. Rather than solely focusing on ethical or rights-based aspects, EAL evaluates data protection regulations and policies based on economic efficiency and the incentives they create. EAL views personal data as a commodity with economic value. Individuals possess

"property rights" to their data and can choose to "sell" or "exchange" it for specific services or benefits. Market mechanisms, such as contracts and consent, are deemed the most efficient means of regulating personal data collection, use, and disclosure (Taufiqurrohman, 2020b).

Key considerations within the EAL framework include: (1) Balancing Privacy and Innovation: Data protection regulations must weigh the compliance costs for businesses against the societal benefits of enhanced privacy. The goal is to achieve an optimal balance between privacy protection and innovation. (2) Compensation for Data Use: EAL supports the notion that individuals should receive compensation for third-party use of their personal data. This can be achieved through market mechanisms like data brokerage or data dividends. (3) Internalizing Negative Externalities: EAL recognizes that data breaches and misuse of personal data can create negative externalities, including financial losses, reputational damage, and erosion of trust. Regulations are necessary to internalize these costs and deter harmful behavior (Mantelero, 2016).

EAL offers valuable insights into the complexities of personal data protection in the digital age. By considering economic aspects, EAL can help design effective and efficient policies to: (1) Protect privacy; (2) Foster innovation; and (3) Create a fair and transparent data market. EAL can also contribute to: (1) Designing effective and efficient regulations by considering the costs and benefits for all stakeholders; (2) Encouraging the development of innovative technologies and solutions to enhance privacy, such as privacy-enhancing technologies (hereinafter "PETs"); and (3) Creating a framework for a fair and transparent data market where individuals have greater control over their data and receive fair compensation for its use (Lloyd, 2020).

The enactment of Law No. 27 of 2022 (hereinafter "Law 27/2022") marks a significant step towards comprehensive data protection in Indonesia. Prior to this, personal data protection was fragmented across various regulations, including Law No. 11 of 2008, which defines personal data as "data concerning an individual who is identified or identifiable, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." However, unlike the European Union's General Data Protection Regulation (hereinafter "GDPR"), Law 27/2022 lacks a comprehensive list of data elements that constitute "identifiable" information (Kurniawan, Taufiqurrohman, & Nugraha, 2022).

Law 27/2022 establishes a clear legal framework for the collection, storage, and use of personal data by companies. It mandates companies to obtain consent from data subjects, grants individuals rights to access and control their data, and imposes data breach reporting obligations on companies.

However, when analyzed through the lens of fair competition in the digital market, Law 27/2022 falls short of providing adequate safeguards against the potential abuse of personal data to

gain an unfair competitive advantage. The phenomenon of personal data exploitation in the digital market, particularly its potential to facilitate abuse of dominant market positions, necessitates a more nuanced approach within the personal data protection regime.

Currently, Law 27/2022 lacks provisions to address how personal data exploitation can be leveraged to strengthen a dominant market player's position. Article 25 of Law No. 5 of 1999, which prohibits the abuse of dominant market positions, along with its implementing regulations, including the Business Competition Supervisory Commission Regulation No. 6 of 2010 (PKPPU 6/2010), remains largely focused on traditional forms of anti-competitive conduct and fails to adequately address the nuances of data-driven dominance in the digital market.

While certain provisions within Law 27/2022 offer some level of protection, they primarily revolve around consent and agreements between data subjects and data controllers. This is evident in Articles 20, 21, and 22, which emphasize the requirement for explicit consent and adherence to agreed-upon purposes, legality, data types, and details of processing. Article 23 further invalidates contractual clauses that lack explicit consent for personal data processing.

This framework creates a potential loophole: Service providers can comply with the letter of the law by implementing Privacy Policies and User Preferences that ostensibly obtain consent for data practices that might still be deemed exploitative or anti-competitive. As long as these practices are disclosed within these documents, they may not technically violate Law 27/2022.

Furthermore, Chapter XIII of Law 27/2022, which outlines prohibited acts related to personal data use, focuses primarily on unlawful acquisition, collection, disclosure, and use (Article 65). As long as service providers obtain, collect, disclose, and use personal data based on the consent mechanisms outlined in their Privacy Policies and User Preferences, their actions may not be considered unlawful under the current framework.

This highlights the need for further legal development to address the intersection of data protection and competition law in the digital market. Law 27/2022, while a significant step forward, requires strengthening to prevent its provisions from being used as a shield for anti-competitive data practices that could harm both individual rights and market fairness.

Sweeping economic reforms initiated in Indonesia during the 1980s led to the rise of conglomerates controlled by families and political parties, often at the expense of small and medium-sized enterprises (SMEs). This sparked discussions about the urgent need for anti-monopoly legislation, gaining momentum by 1989.

The Asian Financial Crisis of 1997 proved to be a catalyst for the formalization of competition law in Indonesia. As part of the financial assistance package agreed upon with the International Monetary Fund (hereinafter “IMF”) on January 15, 1998, Indonesia committed to enacting competition legislation. This commitment was enshrined in the “Letter of Intent and Memorandum of Economic and Financial Policies” addressed to the IMF (Mantelero, 2016).

Consequently, on March 5, 1999, Indonesia issued its first competition law, titled the Law on the Prohibition of Monopolistic Practices and Unfair Business Competition (hereinafter "Law 5/1999"), which came into effect on September 5, 2000. This legislation formed a crucial part of Indonesia's economic reform agenda, aiming to create a more open, competitive, and efficient market.

Law 5/1999 was drafted with international support and consultation from various bodies, including the German Technical Assistance Agency, USAID, CIDA, AusAID, and the World Bank. The drafting process adhered to standards set by the United Nations Conference on Trade and Development (UNCTAD).

The law comprises eleven chapters, three of which specifically regulate business activities: (1) Chapter III: Prohibited Agreements; (2) Chapter IV: Prohibited Conduct; and Chapter V: Abuse of Dominant Position. Law 5/1999 is further complemented by various implementing regulations and guidelines detailing each prohibited activity. To ensure effective enforcement, Law 5/1999 mandated the establishment of a competition authority. This led to the creation of the Business Competition Supervisory Commission (Komisi Pengawas Persaingan Usaha, hereinafter "KPPU"), an independent body reporting directly to the President of the Republic of Indonesia.

Formally established through Presidential Decree No. 75 of 1999, KPPU is tasked with maintaining fair competition in Indonesia. Its mandate, as defined by Law 5/1999, includes: (1) Assessing agreements and business activities for potential monopolistic practices and/or unfair business competition; (2) Investigating potential abuse of dominant market positions that could violate Law 5/1999 (Article 35); (3) Providing recommendations on government policies related to competition (Articles 36-48); and (4) Developing guidelines for the implementation of Law 5/1999; (5) Submitting regular reports to the President and the House of Representatives of the Republic of Indonesia.

Law 5/1999 grants KPPU a range of powers to effectively fulfill its mandate: (1) Conducting investigations into alleged unfair business competition, either independently or based on reports from the public or businesses (Article 35); Summoning suspected businesses, witnesses, experts, and related parties involved in alleged unfair business competition (Article 36); and Determining the existence and extent of harm suffered by other businesses or the public. This robust legal framework, coupled with KPPU's enforcement powers, demonstrates Indonesia's commitment to fostering a fair and competitive market that benefits businesses and consumers alike.

### 3.2. The Interplay Between Personal Data Protection and Competition Law

The dominance of digital platforms like social media, e-commerce, search engines, and digital entertainment, coupled with their reliance on personal data, underscores the critical role of personal data and privacy in shaping the contours of modern competition. This section examines the interplay between personal data, privacy, and competition dynamics within digital markets (Wallace, Pollack,

Roederer-Rynning, & Young, 2020). A direct link between dominant market position and personal data exploitation is absent in the current language of Law 5/1999 and Law 27/2022. However, a nuanced relationship emerges when considering the criteria for determining dominance and the economic advantages derived from data practices.

Article 25 of Law 5/1999, along with the elucidation on abuse of dominance in pages 26-31 of PKPPU 6/2010, outlines a three-pronged approach to establishing abuse of dominance: (1) Imposition of Trading Terms; (2) Market Restriction and Use of Technology; and (3) Barriers to Entry for Existing and Potential Competitors.

The nexus between competition law and personal data protection hinges on the economic benefits derived from data exploitation and its contribution to strengthening a service provider's dominant position in the digital market. Data leverage emerges as a pivotal factor within the criteria of technology and innovation, potentially creating barriers to entry for new players. This, in turn, strengthens the presumption of dominance held by certain companies (Taufiqurrohman, Priambudi, & Octavia, 2021).

Several scenarios illustrate how personal data exploitation can contribute to market dominance, particularly within the context of dominance criteria. First, Data as a Source of Dominance. As Lubyova argues, control and processing of data can be a catalyst for dominance, particularly when access to data becomes a strategic lever in market competition. Second, Data-Driven Revenue and Targeted Advertising (Hildebrandt, 2019). Many digital businesses are increasingly reliant on personal data for service enhancement and revenue generation. In 2023, Alphabet (Google's parent company) generated over 80% of its revenue from targeted advertising. Similarly, Facebook attributed nearly 98% of its 2023 revenue to targeted advertising. This reliance on data-driven revenue models incentivizes companies to maximize data collection (Jones & Sufrin, 2016).

Third, Profiting from “Free” Services. The UK's Competition and Markets Authority (CMA), in its 2020 market report, highlighted how service providers can generate substantial profits despite offering services for “free.” The CMA explained that these business models hinge on collecting and monetizing user data through targeted advertising (Floridi, 2018). This underscores the prevalence of multisided markets in the digital landscape, where one user group (consumers) enjoys free services while their data is leveraged to generate revenue from another group (advertisers). Fourth, Barriers to Entry and Network Effects. Data exploitation can create significant barriers to entry for new players lacking comparable data access and control (Stucke, 2017). Dominance becomes entrenched when data becomes a prerequisite for market entry and competition. Additionally, network effects and economies of scale derived from data further solidify the dominant player's position (Tikkinen-Piri, Rohunen, & Markkula, 2018).

Fifth, Data-Driven Market Power and Barriers to Entry. As discussed previously, the lack of alternatives in digital markets often compels users to consent to expansive terms of service and privacy policies (Bradford, 2020). This lack of choice stems from network effects amplified by the digital market's dependence on personal data. Network effects, where a service's value increases with the number of users, can stifle competition by making it difficult for new entrants to gain traction (Chalmers, Davies, Monti, & Heyvaert, 2024).

Network effects, categorized as direct and indirect, play a crucial role in shaping digital market dynamics. Direct network effects occur when an increase in users directly enhances the platform's value for all users (Voigt & Von Dem Bussche, 2017). For instance, users gravitate towards platforms with larger networks to maximize connectivity and reach. Indirect network effects are prevalent in multisided markets with distinct user groups. Here, the growth of one user group (e.g., consumers) attracts another (e.g., advertisers) due to increased potential for exposure and engagement (Yang, Liu, Chen, & Tong, 2019).

These network effects, coupled with high switching costs, contribute to user lock-in. First, Switching Costs and Lock-in. Users hesitate to switch platforms due to the fear of losing existing content, connections, and network benefits. This inertia, amplified by network effects, limits platform mobility (Hoofnagle, Van Der Sloot, & Borgesius, 2019). Second, Limited Alternatives and Data-Driven Lock-in. The lack of viable alternatives, often a consequence of network effects and data-driven personalization, leaves users with limited choices, forcing them to accept potentially imbalanced terms of service and privacy policies imposed by dominant service providers (Anginer, Demirguc-Kunt, & Zhu, 2014).

The Australian Competition Commission, in its 2019 report on digital platforms, emphasized how network effects amplify market power and create formidable barriers to entry, particularly in markets like internet search. Data as a Barrier to Entry: Incumbent players with vast data troves gain a significant advantage, using this data to further enhance their services, attract users, and solidify their dominance. This creates a challenging landscape for new entrants who struggle to compete with established data-driven offerings (Taufiqurrohman, 2020a).

The process of leveraging data exploitation into a dominant market position can be understood through the concept of feedback loops. First, Data Advantage and Monetization. Companies with access to and expertise in exploiting data can monetize it through targeted advertising and personalized services (Solove & Hartzog, 2014). Second, Investment in Services and Innovation. Revenue generated from data monetization fuels investments in service improvements and innovation, further enhancing the platform's appeal (Craig & De Búrca, 2021). (1) User Retention and Network Effects: Enhanced services and increased value proposition attract and retain users, reinforcing network effects and driving further data accumulation. (2) Reinforcing the Loop: This cyclical process creates a powerful feedback loop, solidifying the dominant player's

position and making it increasingly difficult for competitors to gain traction (Porter & Heppelmann, 2014).

However, this feedback loop can be disrupted by two criteria. First, Substitution Effects. Users switching to competitors offering comparable or superior services, particularly if data-driven advantages are not exclusive and can be replicated (Bennett & Raab, 2017). Second, Independent Data Providers. The emergence of independent data providers, unaffiliated with specific tech giants, could offer alternative avenues for data access and potentially level the playing field. However, the specificity and contextual nature of personal data might limit the effectiveness of such alternatives (Albrecht, 2016).

Furthermore, the low marginal cost of data processing for established players creates an uneven playing field. Companies with existing data processing infrastructure and automated workflows incur minimal additional costs for processing large datasets. This cost advantage, especially prevalent in concentrated markets like social media and search, further solidifies their position (Taufiqurrohman, Fahri, Wijaya, & Wiranata, 2021b).

The exploitation of personal data by service providers can amplify existing market power imbalances, leading to a "winner-take-most" scenario, as described by Ciuriak. This dynamic is starkly illustrated by the contrasting market capitalizations of former rivals Google (currently around US$600 billion) and Yahoo (a mere US$4.5 billion at its last sale). This disparity fuels strategic behavior, as Solomon observes: "Facebook and its elite peers will do whatever it takes to avoid becoming the next Yahoo or Radio Shack, casualties of disruption and a failure to innovate." This stark contrast underscores the high stakes of competition in digital markets, where dominance yields extraordinary rewards while lagging behind can lead to irrelevance or even failure. This incentivizes companies like Facebook to leverage all available means, even ethically questionable or legally ambiguous tactics, to maintain their dominance and thwart competition (Zarsky, 2016).

Furthermore, restricting access to data, particularly by dominant players controlling essential services or processes, can stifle competition: (1) Denial of Access: Refusing competitors access to data deemed essential for effective competition can create significant disadvantages, hindering market entry and innovation. (2) Discrimination and Vertical Integration: Discriminatory practices, especially by vertically integrated companies or those with affiliated Over-the-Top (OTT) services, can further distort competition. For instance, leveraging user data collected through one service to gain an unfair advantage in another market segment where competitors lack access to similar insights (Thoben et al., 2017).

This reliance on personal data has led some companies to perceive robust data protection regulations as a threat. Businesses like Facebook, Apple, and Amazon have, on multiple occasions, claimed that data protection regulations impede their revenue streams, highlighting the perceived tension between data-driven business models and privacy regulations. This underscores the central

role of personal data as a valuable asset in the digital economy, intricately linked to business models and market valuations (Martin & Murphy, 2017). Consequently, privacy has emerged as a critical non-price parameter in competition analysis: (1) Privacy as a Competitive Parameter: Personal data, as a key input for production and a strategic asset, has become a commodity exchanged between platforms and users. Users often relinquish personal data in exchange for access to services; (2) Privacy and Market Power: Traditionally, market power is defined as the ability to control prices above competitive levels without losing significant sales. However, in digital markets where many services are offered for "free," the ability to erode user privacy can be seen as analogous to raising prices, indicating significant market power (Wachter, Mittelstadt, & Floridi, 2017). The US Congress, in its 2020 investigation into digital market competition, highlighted this dynamic, suggesting that the ability to lower privacy standards, in the absence of monetary pricing, can signal substantial market power (Solove & Schwartz, 2020).

## IV. CONCLUSION

This legal research underscores the need for Indonesia to adapt its legal frameworks to the unique challenges posed by the data-driven digital market. While Law 27/2022 provides a crucial foundation for data protection, its reliance on user consent requires reevaluation given the potential for dominant players to exploit data and stifle competition. Strengthening Law 27/2022 to explicitly address data-driven dominance and promoting greater synergy between data protection and competition authorities are essential steps towards a more balanced digital economy.

Furthermore, this research highlights the limitations of traditional competition metrics in the digital age. The ability to collect and leverage data has become a powerful tool for establishing and entrenching market dominance, often at the expense of user privacy. Therefore, Indonesia must adopt a more nuanced approach that recognizes data-driven barriers to entry, rethinks the efficacy of consent, and empowers consumers through measures like data portability and digital literacy. By addressing these challenges head-on, Indonesia can foster a digital ecosystem that is both innovative and fair, benefiting businesses and consumers alike.

## REFERENCES

### 1. Book

Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, USA.

Chalmers, D., Davies, G., Monti, G., & Heyvaert, V. (2024). *European Union law: Text and materials*. Cambridge University Press.

Craig, P., & De Búrca, G. (2021). *The evolution of EU law*. Oxford University Press.

Jones, A., & Sufrin, B. (2016). *EU competition law: Text, cases, and materials*. Oxford University Press.

Lloyd, I. (2020). *Information technology law*. Oxford University Press, USA.

Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law*. Aspen Publishing.

Voigt, P., & Von Dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing.

Wallace, H., Pollack, M. A., Roederer-Rynning, C., & Young, A. R. (2020). *Policy-making in the European Union*. Oxford University Press, USA.

Whish, R., & Bailey, D. (2021). *Competition law*. Oxford University Press.

**2. Journal Article**

Albrecht, J. P. (2016). How the GDPR Will Change The World. *Eur. Data Prot. L. Rev*., 2, 287.

Anginer, D., Demirguc-Kunt, A., & Zhu, M. (2014). How does competition affect bank systemic risk? *Journal of Financial Intermediation*, 23(1), 1–26.

Botta, M., & Wiedemann, K. (2018). EU competition law enforcement vis-à-vis exploitative conducts in the data economy exploring the Terra Incognita. *Max Planck Institute for Innovation & Competition Research Paper*, (18–08).

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180081.

Hildebrandt, M. (2019). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. *Theoretical Inquiries in Law*, 20(1), 83–121.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, 28(1), 65–98.

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: A technological perspective and review. *Journal of Big Data*, 3(1), 25.

Kurniawan, F., Taufiqurrohman, M. M., & Nugraha, X. (2022). Legal Protection Of Trade Secrets Over The Potential Disposal Of Trade Secrets Under The Re-Engineering Precautions. *Jurnal Ilmiah Kebijakan Hukum* 16 (2), 267-282.

Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., Li, Y., … He, B. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, 35(4), 3347–3366.

Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2018). Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*, 10(3), 3162–3173.

Mantelero, A. (2016). Personal Data For Decisional Purposes In The Age Of Analytics: From An Individual To A Collective Dimension Of Data Protection. *Computer Law & Security Review*, 32(2), 238–255.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, 81(1), 36–58.

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135–155.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, 92(11), 64–88.

Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. *Colum. L. Rev.*, 114, 583.

Stucke, M. E. (2017). Should we be concerned about data-opolies? *Geo. L. Tech. Rev*., 2, 275.

Taufiqurrohman, M. M. (2020a). Model Konsultasi Digital Dalam Membantu Tim Pengawal, Pengamanan Pemerintahan Dan Pembangunan Daerah (TP4D) Guna Mewujudkan Kejaksaan Yang Profesional, Komunikatif, Dan Akuntabel. *Jurnal Media Komunikasi Pendidikan Pancasila dan Kewarganegaraan* 2 (2), 267-276.

Taufiqurrohman, M. M. (2022). Adopting Osman Warning In Indonesia: An Effort To Protect Potential Victims Of Crime Target. *Jurnal Hukum dan Peradilan* 11 (3), 477-498.

Taufiqurrohman, M. M., Fahri, M. T., Wijaya, K., & Wiranata, I. G. P. (2021a). Meninjau Perang Siber: Dapatkah Konvensi-Konvensi Hukum Humaniter Internasional Meninjau Fenomena Ini? *Jurnal Kawruh Abiyasa* 1 (2), 145-165.

Taufiqurrohman, M. M., & Gultom, E. (2023). Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan Teknologi Digital dalam Bisnis Perusahaan. *Humani (Hukum dan Masyarakat Madani)* 13 (2), 311-326.

Taufiqurrohman, Moch. M. (2020b). Koalisi Partai Politik Dan Implikasinya Terhadap Sistem Presidensial Multipartai Di Indonesia. *Kertha Semaya: Jurnal Ilmu Hukum* 9 (1), 131-148.

Taufiqurrohman, Moch. M., Fahri, M. T., Wijaya, R. K., & Wiranata, I. G. P. (2021b). The Use of Necessitas Non Habet Legem and Wederspanningheid in Law Enforcement for Covid-19 Vaccination in Indonesia. Jurnal Penelitian Hukum De Jure 21 (4), 473-488.

Taufiqurrohman, Moch. M., Jayus, J., & Efendi, A. (2022). Integrasi Sistem Peradilan Pemilihan Umum melalui Pembentukan Mahkamah Pemilihan Umum. Jurnal Konstitusi 18 (3), 562.

Taufiqurrohman, Moch. M., Priambudi, Z., & Octavia, A. N. (2021). Mengatur Petisi Di Dalam Peraturan Perundang-Undangan: Upaya Penguatan Posisi Masyarakat Terhadap Negara

Dalam Kerangka Perlindungan Kebebasan Berpendapat. *Jurnal Legislasi Indonesia* 18 (1), 1-17.

Thoben, K.-D., Wiesner, S., & Wuest, T. (2017). "Industrie 4.0" and smart manufacturing-a review of research issues and application examples. *International Journal of Automation Technology*, 11(1), 4–16.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34(1), 134–153.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev*., 494.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. *International Data Privacy Law*, 7(2), 76–99.

Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information Security In Big Data: Privacy And Data Mining. *Ieee Access*, 2, 1149–1176.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.

Zarsky, T. Z. (2016). Incompatible: The GDPR in the Age of Big Data. *Seton Hall L. Rev*., 47, 995.