Jurnal Bina Mulia Hukum
Volume 9, Number 1, September 2024, P-ISSN: 2528-7273, E-ISSN: 2540-9034
Submitted 24 April 2024; Accepted 29 September 2024; Available online 30 September 2024
Publication Page: https://jurnal.fh.unpad.ac.id/index.php/jbmh/issue/archive
DOI: https://doi.org/10.23920/jbmh.v9i1.1679

Tech Giants' Non-Negotiable Privacy Policies Strategy *versus* Indonesian Competition Law

Moch. Marsa Taufiqurrohman[a], Helza Nova Lita[b], Gress Gustia Adrian Pah[c]

ABSTRACT

This article aims to explore the tension between non-negotiable privacy policies of giant tech companies and Indonesian competition law. It scrutinizes the prevalent practice of imposing standard agreements on users, which often leads to an erosion of privacy and market competition. This article employs a normative legal research methodology complemented by Reform-Oriented Research. This method is used to evaluate the practice of non-negotiable privacy policies against the suitability of existing competition law regulations and to recommend changes to the regulations as deemed necessary. The study queries whether such non-negotiable privacy policies constitute an exploitative abuse of dominance under Article 25 of Law 5/1999. The analysis delves into the relationship between personal data exploitation and competition law, suggesting that the accumulation and control of user data by giant techs may strengthen their market dominance, potentially resulting in anticompetitive practices. The research offers insights into the intersection of data protection and competition law, advocating for an integrated approach to address the challenges of the digital economy. It recommends policy changes, including the adoption of Codes of Conduct, data mobility, and open standards to foster competition. Furthermore, the manuscript suggests leveraging the Small But Significant And Non-Transitory Decrease In Quality (SSNDQ) method for market analysis in the digital domain. In conclusion, this research calls for Indonesian competition law to adapt and proactively respond to the use of non-negotiable privacy policies and the complex dynamics of data-centric digital market business models, ensuring that markets remain competitive and consumer rights are protected.

Keywords: abuse of dominant; competition law; digital market; privacy data; privacy policy.

INTRODUCTION

As our society and economy become more reliant on online platforms that provide free services while amassing consumer data, the established premises of competition law policy are being questioned. The absence of explicit rules concerning digital marketplace competition leads to growing confusion about the extent of competition law enforcement's role in regulating major giant techs. These giant tech' data-centric operations could violate numerous aspects of competition law.[1] It is worth considering in this digital age whether we need to reassess and adapt our conventional competition perspectives to keep up with the advent of innovative business models and their data-dependent commercial behaviors.[2]

[a] Universitas Padjadjaran, Kampus Jakarta Menara Danareksa Lt. 2 Jl. Medan Merdeka Selatan No.14, Gambir, Kota Jakarta Pusat, 10110, Indonesia. Email: moch23009@mail.unpad.ac.id.
[b] Faculty of Law, Universitas Padjadjaran. Jl. Ir. Soekarno KM. 21 Jatinangor, Sumedang, 45363, Indonesia.
[c] Universitas Airlangga, Jl. Dharmawangsa Dalam Selatan, Airlangga, Kec. Gubeng, Surabaya, Jawa Timur 60286, Indonesia.
[1] Roberto Augusto Castellanos Pfeiffer, "Digital economy, big data and competition law", HeinOnline *Mkt. & Competition L. Rev.*, Vol. 3, No. 1, 2019, p. 53.
[2] *Ibid*, p. 53.

The rise of the data-centric economy has led to growing calls in competition policy circles for reevaluating competition law enforcement aimed at data-related commercial practices that could potentially exploit and harm consumers directly.[3] Debates are heated regarding whether the Indonesia Competition Commission (ICC) should break away from its conventional approach and command competition law enforcement to penalize unjust privacy practices as abusive actions by giant tech.

It is fitting to describe personal data as the new engine powering online businesses in today's digital economy. In this digital age, giant tech heavily depends on collecting, storing, analyzing, and monetizing vast volumes of personal data. Accessing and monetizing (personal) data is essential to secure a competitive advantage and compete effectively in the digital economy.[4] In this scenario, the amassed personal data serves many purposes, from simply enabling giant tech and delivering their products/services to improving the relevance and quality of services, products, and targeted advertising. It is undeniable that giant tech have positively impacted the economy, yielding substantial benefits for businesses, consumers, and the broader society.[5]

On the other hand, digital platforms, which are giant tech, are increasingly capable of collecting massive amounts of personal data from many different sources.[6] They gather data via their services and collect personal data from other third-party websites and mobile apps through tracking practices.[7] Advanced tracking technologies like browser cookies and pixels have made it possible to track users' online activities across various websites and mobile apps, leading to the collection and storage of extensive user- and device-related data. When users visit websites or use mobile apps, these giant techs use technologies, such as cookies, which are small text files stored in the user's browser, needed for the site's proper functioning, like login authentication and language preferences, as well as for purposes like website audience measurement and analysis. However, tracking technologies can be placed on websites by the website's operator and third parties. These third parties, or trackers, embed the same technologies across various websites and mobile apps, allowing them to monitor a single user's online browsing behaviour. Consequently, trackers can gather and connect a wide array of personal information, enabling them to create detailed and comprehensive profiles of users and their activities, interests, and viewpoints.[8]

In Indonesia, this issue arose when several academics questioned using personal data through consent to the Standard Agreement regarding the Privacy Policy conducted by Tokopedia.[9] Tokopedia

---

[3] Andrea De Mauro, Marco Greco, and Michele Grimaldi, "*A Formal Definition of Big data based on its Essential Features*", Emerald Group Publishing Limited *Library Review* Vol. 65, No. 3, 2016, p. 129.
[4] Viktoria HSE Robertson, "Excessive data collection: privacy considerations and abuse of dominance in the era of big data", *Common Market Law Review*, Vol. 57, No. 1, 2020, p. 162.
[5] Moch Marsa Taufiqurrohman *et al.*, "Meninjau Perang Siber: Dapatkah Konvensi-Konvensi Hukum Humaniter Internasional Meninjau Fenomena Ini?," *Jurnal Kawruh Abiyasa,* Vol. 1 No. 2, 2021, p. 21.
[6] Faizal Kurniawan, Moch Marsa Taufiqurrohman, and Xavier Nugraha, "Legal Protection of Trade Secrets Over the Potential Disposal of Trade Secrets Under The Re-Engineering Precautions," *Jurnal Kebijakan Ilmiah Hukum* Vol. 16, No. 2, 2021, p. 17.
[7] Moch Marsa Taufiqurrohman and Elisatris Gultom, "Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan Teknologi Digital dalam Bisnis Perusahaan" *Humani (Hukum dan Masyarakat Madani)* Vol. 13, No. 2, 2023, p. 311.
[8] Anwar Aridi and Urska Petrovcic, *Big Tech, Small Tech, and the Data Economy*, Washington: World Bank, 2019, p. 19.
[9] Mohammad Bernie, "Tokopedia Ubah Kebijakan Privasi, Apa Dampaknya ke Data Pribadi?," tirto.id, accessed April 11, 2023, https://tirto.id/tokopedia-ubah-kebijakan-privasi-apa-dampaknya-ke-data-pribadi-gadU.

compelled users to agree to the Privacy Policy through the Standard Agreement. Among them, Tokopedia was authorized to regulate users' personal data portability by disclosing it to its subsidiaries and affiliates, including third parties, to process the data.[10] Facebook conducted similar cases. Facebook implemented the Privacy Policy through the Standard Agreement instrument.[11] Facebook compelled service users to grant authorization to transfer, transmit, and process data to Facebook's affiliated companies, such as WhatsApp and Instagram.[12]

The escalating accumulation of personal data through third-party tracking techniques triggers significant concerns regarding the erosion of privacy and individual independence. This is primarily because the centralization of tracking activities within the online ecosystem lies within a handful of technologically advanced firms with conglomerate and/or vertically integrated structures, which practically control the marketplace. As Commissioner Vestager aptly stated, these companies resemble robot vacuum cleaners, navigating into every corner of the digital world and absorbing data. The capacity of online businesses to amass vast quantities of personal data, coupled with sophisticated data processing technologies, including machine learning and artificial intelligence, produces various insights into their users' preferences.[13] Consequently, giant tech may exploit consumers' behavioural biases, making them susceptible to targeted advertising, microtargeting and manipulation, and even individualized offers that come close to perfect price discrimination.[14]

This widespread data collection commercial practice is intrinsically linked to several market failures in the data-driven economy, further complicating the issue of data accumulation. Notably, digital markets are characterized by economic traits like network effects and economies of scale and scope, resulting in a few firms possessing significant market power.[15] As a result, users are left with the choice to either accept the privacy policies laid out by giant tech or opt for less desirable services offered by the giant tech's competitors (known as the “take it or leave it” privacy policies), making individual control over personal data processing seem illusory.[16] Moreover, power and information asymmetries inherent in data-processing relationships are exacerbated by a lack of transparency in privacy policies regarding personal data collection and use, preventing consumers from making

[10] Mohammad Bernie, “Ketika Kebijakan Privasi Terbaru Tokopedia Ancam Data Pengguna,” tirto.id, accessed April 11, 2023, https://tirto.id/ketika-kebijakan-privasi-terbaru-tokopedia-ancam-data-pengguna-gae9.
[11] Grahanusa Mediatama, “Benarkah kebijakan privasi baru WhatsApp serahkan data ke Facebook? ini penjelasannya,” PT. Kontan Grahanusa Mediatama, April 10, 2021, https://lifestyle.kontan.co.id/news/benarkah-kebijakan-privasi-baru-whatsapp-serahkan-data-ke-facebook-ini-penjelasannya-1.
[12] “8 Poin Kebijakan Privasi Baru WhatsApp Paksa Setor Data Ke Fb,” accessed April 11, 2023, https://www.cnnindonesia.com/teknologi/20210107140044-185-590685/8-poin-kebijakan-privasi-baru-whatsapp-paksa-setor-data-ke-fb.
[13] Moch. Marsa Taufiqurrohman, “Otomatisasi dan Kecerdasan Buatan pada Profesi Hukum: Kerangka Teoritis dan Narasi Ideal Di Masa Depan,” *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* Vol. 13, No. 2, 2024, p. 224.
[14] Marco Botta and Klaus Wiedemann, “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*, Nos. 18–08, 2018, p. 28.
[15] Ariel Ezrachi, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge: Harvard University Press, 2016, p. 20.
[16] Christophe Samuel Hutchinson, Gulnara Fliurovna Ruchkina, and Sergei Guerasimovich Pavlikov, “Tacit collusion on steroids: The potential risks for competition resulting from the use of algorithm technology by companies”, MDPI *Sustainability,* Vol. 13, No. 2, 2021, p. 951.

informed decisions.[17] These failures are reinforced by the so-called "privacy paradox", a contradictory situation where consumers express deep concern for privacy protection, yet their marketplace behaviour does not align with their stated privacy preferences.[18]

As network effects come into play, user data becomes indispensable for online services that primarily earn their income from advertising. This makes user data a crucial component for these services, sparking competition between companies regarding data gathering and utilization.[19] Nevertheless, the acquisition, processing, and application of personal data are governed by legal constraints, as businesses must ensure these activities do not infringe on users' data rights.[20] While some argue that data protection measures alone can adequately tackle these issues, the question of whether intervention through competition law will be necessary arises when there is an inappropriate exercise of dominance involving the collection and processing of user data. While data protection prioritizes users' concerns as data entities, the stress of competition law is distinct. Even though it eventually caters to the interests of consumers, the crux of competition law is to ensure parity in market competition by removing barriers to entry facilitating free and fair competition. This paper delves into the issue of whether and in what manner competition law should competition law should intercede in situations involving breaches of personal data protection rules.[21]

The method of effectively tackling excessive data collection is part of a lively and more comprehensive discussion involving the interplay between privacy and competition law. On one side, numerous academic perspectives advocate for addressing excessive data collection under exploitative abuse of dominance according to Article 25 of the Indonesian Law Number 5 of 1999 regarding Monopoly Practices and Unfair Business Competition (Law 5/1999). This necessitates investigating whether and how competition enforcement can promote consumer welfare in markets driven by personal data. Specifically, it should be analyzed whether the non-negotiable privacy terms and conditions that giant techs depend on to collect a vast amount of personal data could be considered unfair trading conditions and penalized as exploitative abuse under Article 25 Law 5/1999.

This research seeks to address the issue of non-negotiable privacy policy from the perspective of conditions imposed by giant techs. Specifically, this research attempts to answer the question of to what extent a non-negotiable privacy policy can be qualified as exploitative abuse of a dominant position based on Article 25 of Law 5/1999. This research aims to answer two questions. First, what are the practices surrounding the use of non-negotiable privacy policies in digital markets in Indonesia? Second, how can the use of a non-negotiable privacy policy be established as an abuse of a dominant position based on Article 25 of Law 5/1999?

---

[17] Silvan Gabathuler, Roland Müller, and Walter Brenner, 2018, *Big data Management in Theorie und Praxis aus rechtlicher Sicht*, Thesis, Universität St. Gallen, p. 19.
[18] *Ibid.*
[19] Antitrust: Commission fines Google €2.42 billion, *European Commission - European Commission*, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784, accessed April 24, 2023.
[20] Sinta Dewi Rosadi, *Pembahasan UU Perlindungan Data Pribadi (UU RI No. 27 Tahun 2022)*, Jakarta: Sinar Grafika, 2023, p. 24.
[21] Viktoria HSE Robertson, "Excessive data collection: privacy considerations and abuse of dominance in the era of *big data*", *Common Market Law Review* Vol. 57, No. 1, 2020, p. 162.

METHODS

This research utilizes normative legal research, doctrinal in nature, combined with the Reform Oriented Research method. Normative legal research involves examining legal products, legal principles, legal systematics, legal synchronization, both vertically and horizontally, and comparative law, including historical legal analysis.[22] Doctrinal research is conducted to examine policies regarding the enforcement procedures for abuse of dominant positions under competition law in Indonesia. This research begins by examining existing laws (doctrinal), followed by consideration of issues affecting the law and the underlying legal politics. This research also incorporates the Reform Oriented Research method. This method evaluates the adequacy of existing regulations and recommends necessary changes.[23] This model is based on a legal reform research methodology to recommend changes to existing laws. Ultimately, this model directs researchers to propose legal principles in the law enforcement process.

DISCUSSION

Practices of Using Non-Negotiable Privacy Policy in Digital Market in Indonesia

This article examines Tokopedia, one of the largest service providers in the Indonesian digital market, as a case study. Tokopedia, a dominant service provider in Indonesia, implements a non-negotiable Privacy Policy and User Preferences framework.[24] The Tokopedia case illustrates how a dominant service provider in Indonesia can leverage personal data through its controversial Privacy Policy and User Preferences. This compulsory and non-negotiable policy has drawn criticism for potentially infringing upon user rights. Specifically, Tokopedia's Privacy Policy, which mandates user consent without offering any opportunity for negotiation, has been criticized for restricting user control over their personal data. Of particular concern is Tokopedia's authority to share user data with subsidiaries, affiliates, and third parties without providing users the option to opt out. This "take it or leave it" approach raises concerns about the potential for data exploitation for commercial purposes.[25]

Tokopedia's comprehensive privacy policy is available on its official website and is divided into two parts. The first, the Privacy Notice (https://www.tokopedia.com/privacy?lang=id), and the second, the Cookies Policy (https://www.tokopedia.com/Cookies?lang=id), which details Tokopedia's user personalization practices. Within the Privacy Notice, Tokopedia collects various categories of personal data, encompassing both "Specific Personal Data" and "General Personal Data" as defined under Article 4(2) and 4(3) of Law 27/2022. Specific Personal Data collected includes bank account and credit card details, vehicle data, health data, financial data, phone numbers of users and non-

[22] Aan Efendi, Dyah Ochtorina Susanti, and Rahmadi Indra Tektona, *Penelitian Hukum Doktrinal*, Yogyakarta: LaksBang Justitia, 2019, p. 34.
[23] *Ibid.*
[24] Mohammad Bernie, *tirto.id*, https://tirto.id/tokopedia-ubah-kebijakan-privasi-apa-dampaknya-ke-data-pribadi-gadU, diakses pada 11 Agustus 2023.
[25] *Ibid*.

users within a user's mobile contact list, and biometric data (including, but not limited to, fingerprint and facial recognition). General Personal Data collected includes name, address, date of birth, occupation, phone number, email address, gender, and nationality:

Figure 1. Types of Personal Data Collected by Tokopedia

Tokopedia's terms of service stipulate that users will not receive full functionality of services if they decline to provide personal data:

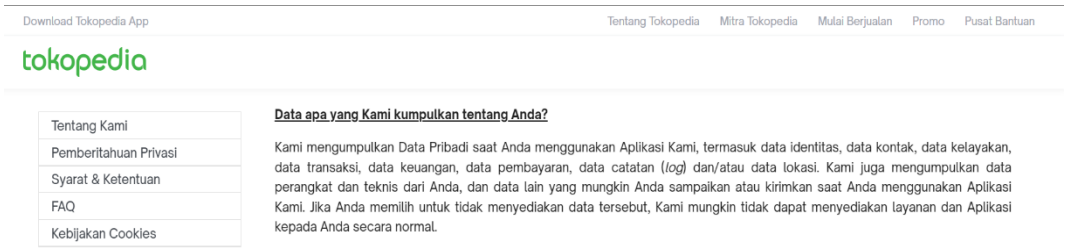


Figure 2. Termination of Services without Personal Data by Tokopedia

In addition to the Privacy Notice, Tokopedia's Cookies Policy governs the use of personal data. Cookies, small text files stored by a user's web browser, allow Tokopedia to collect information such as IP address, browser type, and user activity on the platform. This data enables Tokopedia to remember user preferences, personalize the user experience, and track user behavior for service improvement. Tokopedia explicitly acknowledges using cookies for tracking purposes, including monitoring popular pages, user navigation patterns, and collecting user demographics and interests. This data collection, arguably excessive, enables Tokopedia to gain insights into user behavior and optimize content delivery:

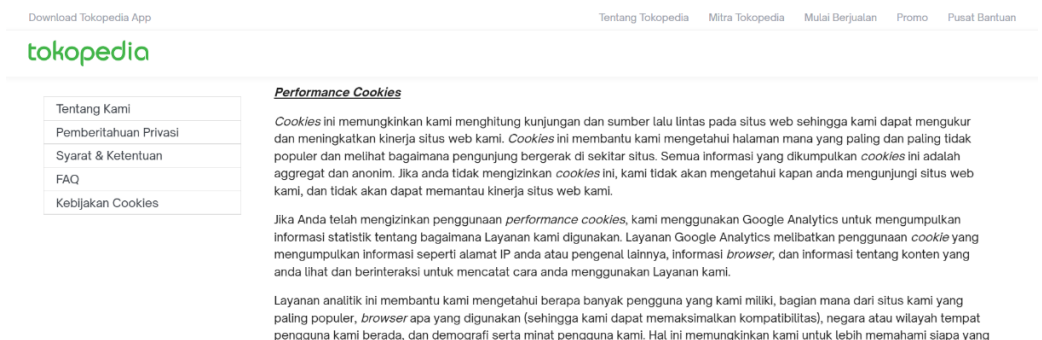


Figure 3. *Tokopedia Performance Cookies* Policy

Under its Targeting Cookies policy, Tokopedia utilizes personalized advertising based on user interests, delivered through designated third-party partners:

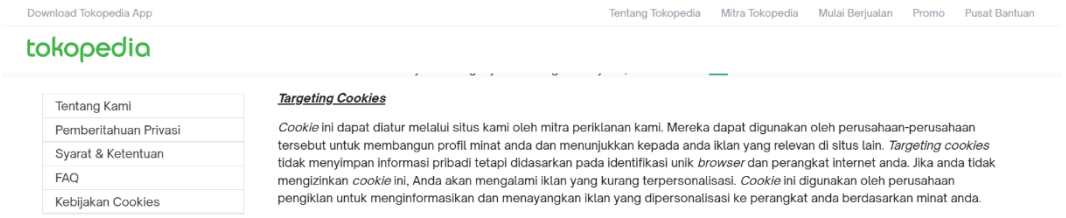
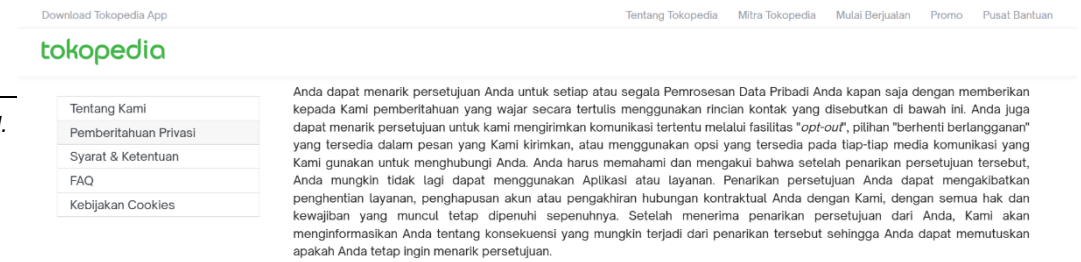


Figure 4. *Tokopedia* Cookies Targeting Policy

Penyedia Layanan akan memberikan ketentuan privasi yang dibuat secara *non-negotiable.* Artinya Pengguna Layanan hanya akan dapat menggunakan layanan, apabila mereka bersedia memberikan data pribadi mereka. Apabila tidak bersedia, maka Pengguna Layanan secara terpaksa harus menggunakan layanan yang kurang disukai.

Tokopedia's Cookies Policy acknowledges that personalized data collected via cookies is used for tracking purposes. From a competition law perspective, understanding the nature and implications of this tracking, particularly the use of data obtained through potentially exploitative practices, is crucial. Tracking enables the collection of vast amounts of personal data to construct comprehensive user profiles, potentially reinforcing market dominance. Collected data can range from visited websites and user interactions to geographical locations, purchased items, expressed interests, personal communications, and user-generated content like photos and messages.[26]

While Article 9 of Law 27/2022 grants data subjects the right to withdraw their personal data, Tokopedia ties this withdrawal to service termination. Tokopedia's Privacy Notice states that users may lose access to the application or services upon withdrawing consent. This withdrawal can lead to service termination, account deletion, or contract termination, although existing rights and obligations remain in force. This linkage underscores Tokopedia's dependence on user data:



[26] *Ibid.*

Figure 5. Impact of Withdrawal of Personal Data from Tokopedia

Tokopedia utilizes personal data for various purposes. Two uses are particularly relevant to this analysis. First, Tokopedia uses data to generate statistical and analytical data for testing, research, product development, commercial partnerships, and collaborations. This suggests data usage to strengthen market position. Second, Tokopedia uses data to facilitate business asset transactions, including mergers, acquisitions, and asset sales. This raises concerns about potentially anti-competitive practices driven by data analysis:

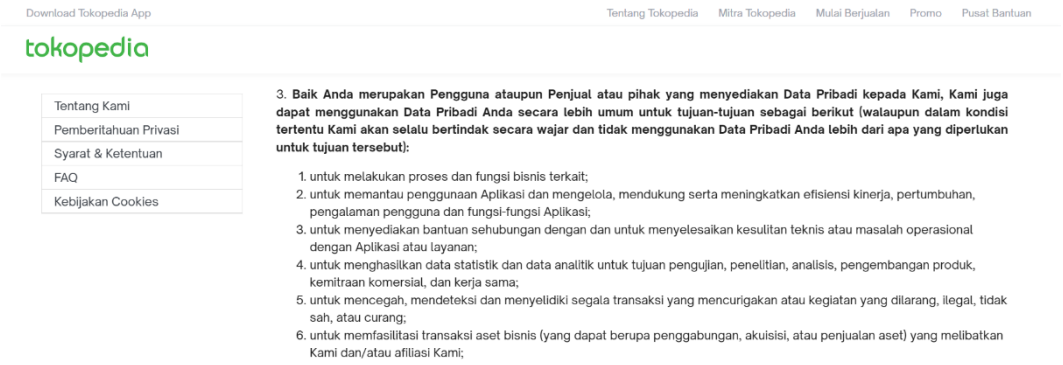


Figure 6. Use of Personal Data by Tokopedia

The use of personal data for business asset transactions (acquisitions, mergers, and asset sales) has the potential to further solidify Tokopedia's dominant position in the digital market. The merger between Tokopedia and Gojek, a US$18 billion transaction involving two of the largest technology companies in Indonesia and Asia, exemplifies this. Both Tokopedia and Gojek operate multi-sided markets, connecting service providers and consumers.[27]

It is essential to initiate research with a clear understanding of the correlation and connection between the exploitation of personal data and competition law. Based on the definition of dominant position in Law No. 5/1999,[28] no direct relationship is formed between the dominant position and the

[27] Kilas Balik Merger Gojek dan Tokopedia Menjadi GoTo - Bisnis Tempo.co, https://bisnis.tempo.co/read/1735427/kilas-balik-merger-gojek-dan-tokopedia-menjadi-goto, accessed on July 4, 2024.

[28] Article 25 of Law 5/1999 stipulates: (1) Business actors are prohibited from using their dominant position, both directly and indirectly, to: a. establish trade conditions with the aim of preventing and/or obstructing consumers from obtaining competitive goods and/or services, both in terms of price and quality; or b. limiting markets and technological development; or c. obstructing other business actors who have the potential to become competitors from entering the relevant market. (2) Business actors have a dominant position as referred to in paragraph (1) if: a. one business actor or one group of business actors controls 50% (fifty percent) or more of the market share of a particular type of goods or services; or b. two or three business actors or groups of business actors control 75% (seventy-five percent) or more of the market share of a particular type of goods or services.

non-negotiable privacy policy. However, the relationship between the dominant position and the exploitation of personal data begins to form in the criteria of a more modern dominant position, where there are four criteria commonly used: market share, barriers to entry, buyer power, and technological innovation.

Consumers should be the primary beneficiaries of competition, receiving benefits such as low prices, high quality, and various market choices. Users lose their right to negotiate and participate in contract formation when a non-negotiable privacy policy is imposed.[29] If users can't easily switch platforms due to lock-in problems, such as lack of data portability and high dependence on the platform services, they are forced to accept the privacy terms offered by giant tech to use the services, terms they would otherwise resist. While user consent to privacy terms can be evaluated based on data protection rules, competition law intervention requires a different rationale.

User data has become valuable to companies for its profit potential, including its use for targeted marketing. Online platforms typically offer services to users at zero cost, generating revenue from other customers such as advertisers.[30] Although users provide their personal data on online platforms, they should not be treated as businesses that supply data. Users do not intend to sell their data to the platform when they upload their personal data; instead, this action is seen as a necessity to use the service or gain access that enables the use of the service.

Even though user data is under the control of the giant tech to which it is submitted, it is not the property of the data controller. Hence, it cannot be used, processed, transferred, traded to, or shared with any third party without the individual user's prior consent. If competition law treats personal data as it does other types of company assets, the aforementioned differences must be considered.[31] However, competition law doesn't focus on whether a user's personal data rights have been violated. Instead, as suggested by Geradin and Kuschewsky, competition law addresses whether giant techs have employed anti-competitive practices in data collection and processing or obstructed competitors from acquiring user data against the users' will to port it.[32]

Despite being distinct areas of law, data protection and competition law share common concerns and objectives, including market integration, consumer protection, and power asymmetries. This intersection supports a more comprehensive approach to the implementation of both policies and the integration of data protection principles in competition reasoning. Competition

---

[29] Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility: Data as Essential Facility*, Zuid-Holland: Kluwer Law International BV, 2021, p. 90.
[30] Dian Parluhutan, "Analisis Hukum Kompetisi terhadap "Big Data" dan Doktrin "Essential Facility" dalam Transaksi Merger di Indonesia", *Jurnal Persaingan Usaha* Vol. 1, No. 1, 2021, p. 85.
[31] Marsinta Simanjuntak, "Disgorgement Fund to Create Corrective Justice as a Legal Protection Measure for Investors in The Capital Market (Legal Protection of Investors Against Disgorgement Fund to Realize Corrective Justice)," *Jurnal Penelitian Hukum De Jure* Vol. 23, No. 4, 2023, p. 473.
[32] Moch. Marsa Taufiqurrohman, Zaki Priambudi, and Avina Nakita Octavia, "Mengatur Petisi Di Dalam Peraturan Perundang-Undangan: Upaya Penguatan Posisi Masyarakat Terhadap Negara Dalam Kerangka Perlindungan Kebebasan Berpendapat," *Jurnal Legislasi Indonesia* Vol. 18, No. 1, 2021, p. 12.

law also seeks to contribute to the functioning of the internal market by preventing interstate trade barriers. Thus, market integration is a concern in both legal fields.[33]

The mastery of personal data, which is then processed into Big data, can be a critical factor in the criteria of technology and innovation and can be a barrier for new entrants to enter the market so that both aspects can strengthen the suspicion of the existence of a dominant position by certain companies. There are several possibilities as to how the exploitation of personal data can affect a company's dominant position, especially in the context of dominant position criteria. According to Lubyova, the control and processing of data can trigger the emergence of a dominant position, especially when access to data becomes a strategic factor in market competition.[34]

Another possibility is that exploiting personal data can be a barrier for new businesses that cannot access or control the same data. In other words, the possibility of a dominant position forming will increase when data access and control become vital for companies to enter and compete in the market. On the other hand, the network effects and economies of scale from data mastery can also strengthen a company's dominant position.

Service users who have access to and exploit data have the potential to utilize it through transactions with personalized advertising providers.[35] Companies can use the revenue generated from such transactions to invest in the services and innovations needed. The improvement in these services and innovations becomes a factor that encourages service users to transact again with the relevant company (user retention). Therefore, the role of independent or non-affiliated data providers and managers with specific technology companies is crucial. Although there are third-party alternatives to provide data, the question remains as to how much information can be utilized by many companies, considering that personal data is generally specific to particular purposes.[36]

Service providers with the infrastructure needed to process data, including automated processing processes, practically do not add significant costs to consumers. Companies' primary focus is to retain customers or obtain repeat purchases from target consumers rather than to generate additional revenue from processing that data. Such conditions are widespread, especially in the markets of social networking products and search engines, which generally have highly concentrated market structures.[37]

Service providers can consider exploiting personal data to enhance market power, which is already relatively high. This condition then encourages the strengthening of a dominant position by the respective business players, as described by Ciuriak as "winner takes the most."[38] Competition in the market will be disrupted if access to data is restricted, especially by dominant companies that control the service or process. Access denial practices for competitors would be highly detrimental,

---

[33] Berkay Kurdoglu and Caglar Deniz Ata, "Data Economics and Competition Law," *Digital L. Rev.* Vol. 3 No. 1, 2021, p. 23.
[34] Linda Holková Lubyová, "*Big data* in the EU Competition Law," *SSRN,* Vol. 18*, No.* 2, 2018, p. 19.
[35] Cassey Lee, "Competition Policy in the Age of Algorithms: Challenges for Indonesia," *Bulletin of Indonesian Economic Studies* Vol. 58, No. 3, 2022, p. 19.
[36] Juan Manuel Sanchez-Cartas and Gonzalo León, "Multisided Platforms and Markets: A Survey of The Theoretical Literature," *Journal of Economic Surveys* Vol. 35, No. 2, 2021, p. 16.
[37] Noby Thomas Cyriac, *Big Data and the Abuse of Dominance by Multi-Sided Platforms: An Analysis of Art. 102 TFEU*, Baden: Nomos Verlag, 2022, p. 18.
[38] *Ibid.*

especially if the data is considered a crucial facility for the relevant company.[39] Besides access denial, discrimination can also hinder competition, especially by vertically integrated companies or core companies with Over the Top (OTT) services affiliated with the unaffiliated. Service users who utilize personal data at the retail level can process data to understand consumer behavior and accurately estimate demand. This information can provide an advantage for these service users, while competitors from the same company cannot access similar information.[40]

Therefore, when consumers are required to provide their personal data in exchange for using giant tech services, competition law might intervene with the question of whether there has been an exploitation of dominance in data collection and processing.[41] This question could arise, for instance, when users are required to provide more personal data than necessary for using the giant tech services or when users are not adequately informed about the use and processing of the collected data. Exclusionary behavior occurs, for instance, when there is an element of excluding competition in the data collection and processing process, and hindering data portability.

The Non-Negotiable Privacy Policy as an Abuse of Dominant Position

Before delving into the main topic of this chapter, it's crucial to first consider the classification of privacy policies agreed upon between users and giant techs as trading conditions. It's worth noting that multi-sided giant techs depend on the collection and processing of personal data to deliver and execute the services they aim to offer.[42] In this scenario, giant techs require the collection of specific information from users, such as names, email addresses, phone numbers, profile pictures, among others, depending on the case.[43] This processing is essential for the performance of the services and thus, privacy policies form part of the relevant terms and conditions of the services rendered by ad-supported giant techs. Privacy policies establish the conditions under which online services are provided in exchange for users' personal information. If a user refuses the terms of the privacy policy, they are barred from using the platform's services. In this regard, the transaction between the giant tech and the users is finalized once the users give their consent to the subsequent data processing. For instance, LinkedIn's terms of use state that by clicking “Join Now”, “Join LinkedIn”, “Sign Up” or similar, registering, accessing or using their services, users are agreeing to a legally binding contract with LinkedIn.[44] This agreement is applicable even if the services are being used on behalf of a

[39] David J. Teece et al., “Managing Multi-Sided Platforms: Platform Origins and Go-to-Market Strategy,” *California Management Review* Vol. 64, No. 4, 2022, p. 12.
[40] James Alleman, Edmond Baranes, and Paul N. Rappoport, “Multisided Markets and Platform Dominance,” in *Applied Economics in the Digital Era*, ed. James Alleman, Paul N. Rappoport, and Mohsen Hamoudia, New York City: Springer International Publishing, 2020, p. 21.
[41] David J. Teece et al., “Managing Multi-Sided Platforms: Platform Origins and Go-to-Market Strategy,” *California Management Review* Vol. 64 No. 4, 2022, p. 12.
[42] Barry Doherty, “Just what are essential facilities?”, *Common Market Law Review* Vol. 38, No. 2, 2001, p. 16.
[43] Moch Marsa Taufiqurrohman, “Adopting Osman Warning in Indonesia: An Effort To Protect Potential Victims Of Crime Target,” *Jurnal Hukum dan Peradilan* Vol.11, No. 3, 2022, p. 479.
[44] Brett Frischmann and Spencer Weber Waller, “Revitalizing essential facilities”, HeinOnline *AntitrUSt lJ* Vol. 75, No. 1, 2008, p. 17.

company. Their use of LinkedIn's services is also subject to their Cookie Policy and Privacy Policy, which cover how they collect, use, share, and store personal information. Similarly, Amazon's terms of use dictate that users must review their Privacy Notice, which also governs the usage of Amazon Services, to understand their practices.[45]

Despite the recognition of user data as a valuable resource for companies in the digital market, quantifying its role for the purposes of competition law analysis remains a complex issue. If we endorse this notion and apply it broadly, it would suggest that data utilized for specific purposes could establish a relevant market. The challenge with this idea is that even though user data is recognized as a business asset, treating it as a tradeable commodity could pose problems, particularly from a data protection regulations perspective. Therefore, while user data may contribute to the formation of a specific market, such as a social network market, it is not solely responsible for the creation of that market.

A privacy policy might encompass a wide range of issues, from data collection and processing to its usage. The focus of competition law isn't whether a user's privacy rights have been infringed upon by the policy per se, a matter better suited for privacy protection scrutiny.[46] Rather, it examines if a dominant position has been abused in implementing a specific privacy policy, which wouldn't have been feasible without the giant tech's market dominance.[47]

Moreover, this article investigation is concentrating on two other issues: the accusation of enforcing exclusive obligations in its advertising contracts and of technically hindering data portability. With regards to exclusive agreements, the competition law's concern is preventing Google's advertising partners from 'displaying certain types of competitive ads on their websites' and on computer and software vendors 'with the intention of excluding competing search tools'. Regarding data portability restrictions, the question is whether Google has limited the portability of 'online advertising campaign data' from its platform to its competitors.

As previously noted, effective competition aims to deliver benefits to consumers, including low prices, high-quality goods and services, a broad range of product choices, and innovation. Consequently, the parameters on which market players compete include price, quality, quantity, choice, and innovation. In traditional offline markets, where goods and services are traded against monetary consideration, businesses primarily compete on lower prices. As a result, the assessment of practices in these markets is based on the consumer welfare standard's emphasis on price, and competition authorities tend to examine factors that are easily measurable, such as short-term pricing effects and short-term proactive efficiencies.[48]

---

[45] Catherine Tucker, "Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility", *Review of Industrial Organization* Vol. 54, No. 4, 2019, p. 683.

[46] Lisa Mays, "The Consequences of Search Bias: How Application of the Essential Facilities Doctrine Remedies Google's Unrestricted Monopoly on Search in the United States and Europe", HeinOnline *Geo. Wash. L. Rev.* Vol. 83, No. 3, 2014, p. 721.

[47] Marina Lao, "Search, Essential Facilities, and the Antitrust Duty to Deal", HeinOnline *Nw. J. Tech. & Intell. Prop.* Vol. 11, No. 3, 2012, p. 275.

[48] Moch. Marsa Taufiqurrohman et al., "The Use of Necessitas Non Habet Legem and Wederspanningheid in Law Enforcement for Covid-19 Vaccination in Indonesia," *Jurnal Penelitian Hukum De Jure* Vol. 21, No. 4, 2021, p. 473.

However, in today's digital economy, focusing on price effects is not an ideal measure of the competitive conditions of digital products and services, which are offered for free but actually paid for by users providing access to their personal data. In this regard, competition policy's price-centered approach should shift to assess harms to consumer welfare that relate to non-price dimensions of competition, such as choice, quality, quantity, and innovation. There is a need for a stronger emphasis on other parameters of competition, such as quality, choice, and innovation, particularly in digital markets that involve services provided at zero price and monetized through advertising.[49]

In this context, worries about the erosion of user privacy due to extensive data collection might be viewed as consumer harm in competition terms if privacy is considered a component of the quality of online services. Privacy has been recognized as a facet of quality, and thus a non-price dimension of competition. To sum up, it can be deduced that competition enforcement may step in to prevent consumer harm in the form of privacy violation, when privacy is viewed as an aspect of quality or choice. However, there are obstacles in formulating a practical theory of harm, necessitating a cautious approach by competition authorities. [50]

To classify a non-negotiable privacy policy as an abuse of dominance, once the element of dominance is proven, the element of abuse must also be demonstrated. This occurs when the privacy policy is non-negotiable, hence limiting the user's ability to alter the policy, even when such alteration is feasible, due to the giant tech's dominant position. This abuse could manifest in various terms within the policy, either to exclude competitors or to exploit the market dominance. The case presents at least two conceivable scenarios of exclusionary behavior. The first scenario is when a privacy policy limits users from supplying the same personal data or the same quality of data to competitors or restricts users' choice to utilize services provided by the giant tech's competitors. In the second scenario, the restriction is placed on the user's freedom to transfer their data to competitors.[51]

Generally, the competition enforcement toolkit encompasses the levying of fines and the implementation of structural or behavioral remedies. Typically, antitrust fines are paired with a cease-and-desist order, requiring the concerned undertaking to halt the disputed conduct. However, administrative fines coupled with a cease-and-desist order may not be the most effective solution, as the anti-competitive harm has already taken place and such a sanction wouldn't effectively “rewind the clock” to restore conditions to the pre-violation scenario. It also might not be sufficient to deter privacy-related violations.[52] Additionally, the deterrent effect of the fines may be questionable considering the revenues large giant techs can generate.

---

[49] Edy Santoso and Andriana Andriana, “Insecurity to Consumer Data Protection in the eHealth Sector,” *Jurnal Penelitian Hukum De Jure* Vol. 23, No. 1, 2023, p. 115.
[50] Inge Graef, “Rethinking the essential facilities doctrine for the EU digital economy”, HeinOnline *RJT ns*, Vol. 53, No. 1 2019, p. 33.
[51] *Ibid.*
[52] Marulak Pardede, “Investment Regulatorly Reform in Indonesia (an Effort to Increase the Competitiveness Climate of Investment),” *Jurnal Penelitian Hukum De Jure* Vol. 23, No. 2, 2023, p. 231.

Apart from levying administrative fines, competition authorities could implement structural or behavioral remedies. Moreover, a data separation policy (or data use breakup) appears to be a suitable remedy for the mass data accumulation facilitated within the third-party ecosystem of giant tech. An internal divestiture could require giant tech not to use and combine personal data collected from third-party sources, and not through their own services, unless they obtain the explicit, informed, and freely given consent of the concerned users.

Such a data separation remedy was adopted in the Facebook case, where the Bundeskartellamt ordered Facebook to separate the consent for using its core social network services and to combine data generated outside the platform. Despite ongoing contentious discussions on the feasibility of such an approach adopted by the Bundeskartellamt, it can be confirmed that at least theoretically this kind of remedy could be included in the competition authorities' toolkit. Implementing mandatory data unbundling as a default mode in the initial stage of personal data collection by giant techs could specifically address the behavioral biases that may impact consumers' choices, such as the power of default discussed in the previous section.

In addition to, and closely related with, the above unbundling of consent and sets of personal data, another behavioral remedy could involve requiring giant techs to offer their services to users with two options: either free services in exchange for data collection through third-party tracking, or a fee-based subscription if users do not want their data harvested and subjected to targeted advertising.[53] However, determining the competitive monetary value of the data required to access the services in question is not a straightforward decision. It is unclear what the competitive price in monetary terms should be, given that it has not emerged in the market for most services under consideration.

Overall, the aforementioned remedies could mitigate the negative effects of the data-collecting conduct of giant tech by increasing the choices available to users and offering alternatives that cater to the diverse privacy preferences of users related to the quality of the services offered.[54] However, it should also be taken into account that the information collected is used not only to improve advertising efficiency but also serves as a critical input to enhance the services. Limits to the combination and integration of data may lead to a loss of service efficiency, and users who do not provide data may individually receive lower service quality levels. Therefore, efficiency effects may challenge the design of appropriate remedies and lead to negative implications for consumer welfare, questioning the effectiveness of competition enforcement.[55]

Furthermore, special consideration should be given to the existence of behavioral biases and information and power asymmetries, as explained in the previous sections, that may render these additional choices ineffective. In this respect, competition authorities may need to decide on remedies that contribute to increasing information and transparency, ensuring that users indeed

[53] Tasya Safiranita et al., "The Role of E-Commerce in Escalation of Digital Economy in The New Normal Era Based on Law Number 27 of 2022 Concerning Personal Data Protection," *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 4, 2022, p. 437.
[54] *Ibid.*
[55] Faiz Rahman and Dian Agung Wicaksono, "Researching References on Interpretation of Personal Data in the Indonesian Constitution," *Jurnal Penelitian Hukum De Jure* Vol. 21, No. 2, 2021, p. 187.

make rational and well-informed decisions, e.g., imposing requirements for minimum standards for transparency.

Several policy recommendations are proposed to ensure that competition continues to operate in the digital market. The theory of harm approach describes the methodology used by competition supervisory authorities to test behavior suspected of violating competition law, including elaborating on the (potential) impacts on competition and consumers. This article suggests three important roles or functions that must operate optimally.[56] First, a Code of Conduct ensures competition and other principles, such as consumer protection. Second, data mobility and open standards ensure user freedom principles. Mobility will reduce switching costs for users while reducing transaction costs in aggregate. Open standards relate to technology specifications, ensuring universal standards so that technology providers do not encounter barriers to platform access. Besides ensuring technology provider freedom, open standards will reduce business unit dependence on specific companies with non-standard specifications. Third, data openness ensures that all platforms and big data providers can access essential data for business.

Furthermore, technically, this article recommends several points deemed capable of minimizing the potential for abuse of dominant positions by companies that control Big Data technology. First, maintaining multi-homing access for users maintains requirements exclusively related to user access. Second, opening the necessary access for complementary businesses. Third, prevention against defensive acquisition and entry for buyout practices.[57]

In addition to the above, in the practice of enforcing competition law in the digital era, the SSNDQ (Small But Significant And Non-Transitory Decrease In Quality) method can be used as a substitute for the SSNIP (Small but Significant and Non-transitory Increase in Price) method used by the ICC.[58] This is especially the case when determining markets and assessing Big Data concerning dominant positions in the digital market, which usually involve non-financial transactions. This allows the ICC, as the Business Competition Supervisory Commission, to carry out its duties as a competition law enforcer by monitoring to what extent quality suffers when customers or users switch from one digital business actor to another, both operating in the digital market.[59]

Based on the above explanation, the ICC must establish regulations regarding digital mergers in Indonesia in general, as well as regulations regarding ownership of Big Data and its impacts on competition effectiveness (effective competition) in the digital market, both direct and indirect impacts, such as provisions regarding Essential Facility, in particular. In the context of digital

---

[56] Huta Disyon and Elisatris Gultom, "Critical Review of the Implementation of the Making of SOE as a Holding from Anti-Monopoly and Unfair Business Competition Perspective," *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 2, 2022, p. 191.
[57] *Ibid,* p. 89.
[58] Ayup Suran Ningsih, "Implikasi Undang-Undang Nomor 5 Tahun 1999 Tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat Pada Pelaku Usaha Mikro Kecil Dan Menengah (UMKM)," *Jurnal Penelitian Hukum De Jure* Vol. 19, No. 2, 2019, p. 207.
[59] Mosgan Situmorang, "Measuring the Effectiveess of Consumer Dispute Resolution on Small Value E-Commerce Transaction," *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 4, 2022, p. 537.

competition regulation, there is a positive correlation between competition analysis and the increasing dominant position of business actors with merger analysis in the digital market. In other words, the ICC can make comprehensive prognoses as to whether, with the implementation of mergers in the digital market, a business actor will gradually acquire a dominant position or increase the intensity of such dominant positions.[60] This proposition aligns with the mandate given to the ICC based on Article 2 and Article 3 paragraph (a) of Indonesia Competition Commission Regulation No. 01 of 2014 concerning the Organization and Working Procedures of the Indonesia Competition Commission and Presidential Decree No. 75 of 1999 concerning the Business Competition Supervisory Commission, which explicitly states that the ICC has the function of overseeing and enforcing the law against monopoly practices and unhealthy business competition and preventing and monitoring the occurrence of monopoly practices and unhealthy business competition, in the context of maintaining effective competition in the digital market in Indonesia.

CLOSING

This analysis of service providers in the Indonesia digital market reveals how dominant digital platforms in Indonesia leverage non-negotiable privacy policies to collect extensive user data, raising competition concerns. The lack of user control, coupled with broad data-sharing provisions and the platform's dependence on user data for service provision and strategic decisions, potentially reinforces Tokopedia's market dominance. This case study underscores the need for Indonesian competition law to address the exploitative potential of non-negotiable privacy policies within data-centric digital markets to protect consumer rights and maintain fair competition.

The non-negotiable privacy policies can constitute an abuse of dominance by giant tech companies. These policies, a prerequisite for service access, function as trading conditions where user data is exchanged for service use. While user data's value in competition analysis remains complex, the focus is on whether a dominant position enables the implementation of exploitative or exclusionary privacy terms. This can manifest as restrictions on data sharing with competitors or data portability limitations. In digital markets where services are often “free” but data-driven, the traditional price-centric competition analysis needs to incorporate non-price factors like privacy as a component of service quality. Potential remedies include not only fines but also structural interventions like data separation or behavioral changes such as mandatory data unbundling and offering paid, data-collection-free service options. However, balancing privacy protection with maintaining service quality and innovation presents ongoing challenges.

REFERENCES

Book

[60] *Ibid.*

Alleman, James, et al, "*Multisided Markets and Platform Dominance," in Applied Economics in the Digital Era*, ed. James Alleman, Paul N. Rappoport, and Mohsen Hamoudia, New York City: Springer International Publishing, 2020.

Efendi, Aan, et al, *Penelitian Hukum Doktrinal*, Yogyakarta: LaksBang Justitia, 2019.

Ezrachi, Ariel, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge: Harvard University Press, 2016.

Graef, Inge, EU Competition Law, *Data Protection and Online Platforms: Data as Essential Facility: Data as Essential Facility*, Zuid-Holland: Kluwer Law International BV, 2021.

Rosadi, Sinta Dewi, *Pembahasan UU Perlindungan Data Pribadi (UU RI No. 27 Tahun 2022*), Jakarta: Sinar Grafika, 2023.

Thomas Cyriac, Noby, B*ig Data and the Abuse of Dominance by Multi-Sided Platforms: An Analysis of Art.* 102 TFEU, Baden: Nomos Verlag, 2022.

Journal

Aridi, Anwar and Petrovcic, Urska, Big Tech, Small Tech, and the Data Economy, Washington: World Bank, 2019.

David J. Teece et al., "Managing Multi-Sided Platforms: Platform Origins and Go-to-Market Strategy," *California Management Review* Vol. 64 No. 4, 2022.

De Mauro, Andrea, et al, "A Formal Definition of Big data based on its Essential Features", Emerald Group Publishing *Limited Library Review* Vol. 65, No. 3, 2016.

Disyon, Huta, and Gultom, Elisatris, "Critical Review of the Implementation of the Making of SOE as a Holding from Anti-Monopoly and Unfair Business Competition Perspective," *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 2, 2022.

Doherty, Barry, "Just what are essential facilities?", Common Market Law Review Vol. 38, No. 2, 2001.

Parluhutan, Dian, "Analisis Hukum Kompetisi terhadap "Big Data" dan Doktrin "Essential Facility" dalam Transaksi Merger di Indonesia", *Jurnal Persaingan Usaha* Vol. 1, No. 1, 2021.

Frischmann, Brett and Waller, Spencer Weber, "Revitalizing essential facilities", HeinOnline AntitrUSt lJ Vol. 75, No. 1, 2008.

Graef, Inge, "Rethinking the essential facilities doctrine for the EU digital economy", *HeinOnline RJT ns*, Vol. 53, No. 1 2019.

Holková Lubyová, Linda, "Big data in the EU Competition Law," *SSRN,* Vol. 18, No. 2, 2018.

Hutchinson, Christophe Samuel, et al, "Tacit collusion on steroids: The potential risks for competition resulting from the use of algorithm technology by companies", *MDPI Sustainability*, Vol. 13, No. 2, 2021.

J. Teece, David, et al., "Managing Multi-Sided Platforms: Platform Origins and Go-to-Market Strategy," *California Management Review* Vol. 64, No. 4, 2022.

Kurdoglu, Berkay, and Deniz Ata, Caglar, "Data Economics and Competition Law," *Digital L. Rev*. Vol. 3 No. 1, 2021.

Kurniawan, Faizal Kurniawan, Taufiqurrohman, Moch. Marsa, and Nugraha, Xavier, "Legal Protection of Trade Secrets Over the Potential Disposal Of Trade Secrets Under The Re-Engineering Precautions," *Jurnal Kebijakan Ilmiah Hukum* Vol. 16, No. 2, 2021.

Lao, Marina, "Search, Essential Facilities, and the Antitrust Duty to Deal", *HeinOnline Nw. J. Tech. & Intell. Prop.* Vol. 11, No. 3, 2012.

Lee, Cassey, "Competition Policy in the Age of Algorithms: Challenges for Indonesia," *Bulletin of Indonesian Economic Studies* Vol. 58, No. 3, 2022.

Manuel Sanchez-Cartas, Juan and León, Gonzalo, "Multisided Platforms and Markets: A Survey Of The Theoretical Literature," *Journal of Economic Surveys* Vol. 35, No. 2, 2021.

Mays, Lisa, "The Consequences of Search Bias: How Application of the Essential Facilities Doctrine Remedies Google's Unrestricted Monopoly on Search in the United States and Europe", *HeinOnline Geo. Wash. L. Rev.* Vol. 83, No. 3, 2014.

Ningsih, Ayup Suran, "Implikasi Undang-Undang Nomor 5 Tahun 1999 Tentang Larangan Praktek Monopoli Dan Persaingan Usaha Tidak Sehat Pada Pelaku Usaha Mikro Kecil Dan Menengah (UMKM)," *Jurnal Penelitian Hukum De Jure* Vol. 19, No. 2, 2019.

Pardede, Marulak, "Investment Regulatorly Reform in Indonesia (an Effort to Increase the Competitiveness Climate of Investment)," *Jurnal Penelitian Hukum De Jure* Vol. 23, No. 2, 2023.

Pfeiffer, Roberto Augusto Castellanos, "Digital economy, big data and competition law", *HeinOnline Mkt. & Competition L. Rev.*, Vol. 3, No. 1, 2019.

Rahman, Faiz and Wicaksono, Dian Agung "Researching References on Interpretation of Personal Data in the Indonesian Constitution," *Jurnal Penelitian Hukum De Jure* Vol. 21, No. 2, 2021.

Robertson, Viktoria HSE, "Excessive data collection: privacy considerations and abuse of dominance in the era of big data", *Common Market Law Review* Vol. 57, No. 1, 2020.

Safiranata, Tasya et al., "The Role of E-Commerce in Escalation of Digital Economy in The New Normal Era Based on Law Number 27 of 2022 Concerning Personal Data Protection," *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 4, 2022.

Santoso, Edy, and Andriana, "Insecurity to Consumer Data Protection in the eHealth Sector," *Jurnal Penelitian Hukum De Jure* Vol. 23, No. 1, 2023.

Simanjuntak, Marsinta, "Disgorgement Fund to Create Corrective Justice as a Legal Protection Measure for Investors in The Capital Market (Legal Protection of Investors Against Disgorgement Fund to Realize Corrective Justice)," *Jurnal Penelitian Hukum De Jure* Vol. 23, No. 4, 2023.

Situmorang, Mosgan, "Measuring the Effectiveess of Consumer Dispute Resolution on Small Value E-Commerce Transaction," *Jurnal Penelitian Hukum De Jure* Vol. 22, No. 4, 2022.

Taufiqurrohman, Moch. Marsa and Gultom, Elisatris, "Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan Teknologi Digital dalam Bisnis Perusahaan" *Humani (Hukum dan Masyarakat Madani)* Vol. 13, No. 2, 2023.

Taufiqurrohman, Moch. Marsa, "Adopting Osman Warning In Indonesia: An Effort To Protect Potential Victims Of Crime Target," *Jurnal Hukum Dan Peradilan* Vol.11, No. 3, 2022.

Taufiqurrohman, Moch. Marsa, et al, "Mengatur Petisi Di Dalam Peraturan Perundang-Undangan: Upaya Penguatan Posisi Masyarakat Terhadap Negara Dalam Kerangka Perlindungan Kebebasan Berpendapat," *Jurnal Legislasi Indonesia* Vol. 18, No. 1, 2021.

Taufiqurrohman, Moch. Marsa, et al, "Meninjau Perang Siber: Dapatkah Konvensi-Konvensi Hukum Humaniter Internasional Meninjau Fenomena Ini?," *Jurnal Kawruh Abiyasa*, Vol. 1 No. 2, 2021.

Taufiqurrohman, Moch. Marsa, et al., "The Use of Necessitas Non Habet Legem and Wederspanningheid in Law Enforcement for Covid-19 Vaccination in Indonesia," *Jurnal Penelitian Hukum De Jure* Vol. 21, No. 4, 2021.

Taufiqurrohman, Moch. Marsa. "Otomatisasi dan Kecerdasan Buatan pada Profesi Hukum: Kerangka Teoritis dan Narasi Ideal di Masa Depan," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* Vol. 13, No. 2, 2024.

Tucker, Catherine, "Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility", *Review of Industrial Organization* Vol. 54, No. 4, 2019.

Legislation

Law Number 5 of 1999 regarding Monopoly Practices and Unfair Business Competition.

Indonesia Competition Commission Regulation No. 01 of 2014 concerning the Organization and Working Procedures of the Indonesia Competition Commission and Presidential Decree No. 75 of 1999 concerning the Business Competition Supervisory Commission.

Other Resources

Antitrust: Commission fines Google €2.42 billion, European Commission - European Commission, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784, accessed April 24, 2023.

Grahanusa Mediatama, "Benarkah kebijakan privasi baru WhatsApp serahkan data ke Facebook? ini penjelasannya," PT. Kontan Grahanusa Mediatama, April 10, 2021, https://lifestyle.kontan.co.id/news/benarkah-kebijakan-privasi-baru-whatsapp-serahkan-data-ke-facebook-ini-penjelasannya-1.

Mohammad Bernie, "Ketika Kebijakan Privasi Terbaru Tokopedia Ancam Data Pengguna," tirto.id, accessed April 11, 2023, https://tirto.id/ketika-kebijakan-privasi-terbaru-tokopedia-ancam-data-pengguna-gae9.

Mohammad Bernie, "Tokopedia Ubah Kebijakan Privasi, Apa Dampaknya ke Data Pribadi?," tirto.id, accessed April 11, 2023, https://tirto.id/tokopedia-ubah-kebijakan-privasi-apa-dampaknya-ke-data-pribadi-gadU.