Journal of Law and Legal Reform
Vol. 6 Issue 4 (2025) 2015–2058
DOI: https://doi.org/10.15294/jllr.v6i4.22388
Online since: October 30, 2025

Journal of Law & Legal Reform
https://journal.unnes.ac.id/journals/jllr

Hybrid Model of Personal Data Protection for Consumers in Digital MSMEs: A Comparative Study of Indonesian and China Regulations

Yosia Hetharie [a] ✉, Isis Ikhwansyah [b], Ema Rahmawati [b], Valentino Dinatra Soplantila [c]

[a] Doctoral Program of Law, Universitas Padjadjaran, Indonesia
[b] Department of Law, Universitas Padjadjaran, Indonesia
[c] Birmingham Law School, University of Birmingham, United Kingdom

✉ corresponding email: josephushetharie@gmail.com

Abstract

The protection of consumers' personal data in digital MSME (Micro, Small, and Medium Enterprises) businesses poses a significant challenge in the era of digital transformation, particularly amid the rising cases of data breaches in Indonesia. Although Law No. 27 of 2022 on Personal Data Protection (PDP Law) has come into effect, its implementation still faces numerous obstacles, especially for MSMEs that are limited in terms of resources and technological understanding. By comparison, China, through its Personal Information Protection Law (PIPL), enforces strict supervision combined with AI-driven compliance technologies. This study aims to analyze the effectiveness of personal data protection frameworks in Indonesia and China and to propose a hybrid model that integrates government regulations with technological solutions. The research employs a normative juridical method using statutory, conceptual, and comparative law approaches, relying on secondary data such as regulations, academic journals, and policy documents. The findings indicate that adopting a hybrid model for the protection of consumers' personal data in digital MSME businesses could serve as an effective solution. This model merges a compliance-based approach, as adopted under Indonesia's PDP Law, with the strict oversight mechanisms implemented under China's PIPL. By adapting mechanisms such as mandatory registration, periodic audits, and technology-based compliance incentives, Indonesia could enhance transparency, accountability, and data security within its digital MSME ecosystem.

Keywords

Model Hybrid, Personal Data Protection, Consumer, Digital MSMEs.

HOW TO CITE:

Chicago Manual of Style Footnote:

[1] Yosia Hetharie, Isis Ikhwansyah, Ema Rahmawati, Valentino Dinatra Soplantila, "Hybrid Model of Personal Data Protection for Consumers in Digital MSMEs: A Comparative Study of Indonesian and China Regulations," *Journal of Law and Legal Reform 6*, no 4 (2025): 2015-2058, https://doi.org/10.15294/jllr.v6i4.22388.

Chicago Manual of Style for Reference:

Hetharie, Yosia, Isis Ikhwansyah, Ema Rahmawati, Valentino Dinatra Soplantila. "Hybrid Model of Personal Data Protection for Consumers in Digital MSMEs: A Comparative Study of Indonesian and China Regulations." *Journal of Law and Legal Reform 6*, no 4 (2025): 2015-2058. https://doi.org/10.15294/jllr.v6i4.22388.

Introduction

In the era of digital transformation, Micro, Small, and Medium Enterprises (MSMEs) are increasingly reliant on digital technology to manage their businesses and engage with consumers.[1] This digitalization, while offering significant opportunities for MSMEs' growth, also poses substantial risks to the protection of consumers' personal data.[2] In Indonesia, personal data protection regulations are still in the developmental stage with the enactment of the Personal Data Protection Law (PDP Law), which aims to regulate the management of data by various entities[3], including MSMEs. However, the implementation of data protection within the MSME sector still faces various challenges[4], particularly in terms of regulatory compliance and technological readiness.[5] This highlights the real challenges faced by Indonesian MSMEs in the era of digital transformation, particularly concerning the protection of consumers' personal data. Although the enactment of the PDP Law marks a significant step forward, its implementation in the MSME sector remains suboptimal, as most business actors are still unprepared in terms of regulatory compliance and technological capacity. Many MSMEs either do not understand the importance of data security or lack the resources to implement adequate data protection

[1] Muhammad Arbani, "Aspek Hukum Perlindungan Umkm Dalam Penjualan Di E-Commerce: Tantangan Dan Solusi Di Era Digital," *Jurnal Syntax Admiration* 6, no. 2 (2025): 1166–75.

[2] Jeffriansyah Dwi Sahputra Amory, Muhtar Mudo, and J Rhena, "Transformasi Ekonomi Digital Dan Evolusi Pola Konsumsi: Tinjauan Literatur Tentang Perubahan Perilaku Belanja Di Era Internet," *Jurnal Minfo Polgan* 14, no. 1 (2025): 28–37.

[3] Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–55.

[4] Moody Rizqy Syailendra and Inayah Fasawwa Putri, "Tinjauan Hukum Mengenai Perlindungan UMKM Serta Efektivitas Permendag No. 31 Tahun 2023 Terhadap Social Commerce Tiktok Shop," *INNOVATIVE: Journal of Social Science Research* 3, no. 6 (2023): 5087–5100.

[5] Henro Prayitno Nento et al., "Peningkatan Literasi Hukum Dalam Pengelolaan Keuangan: Strategi Edukasi Bagi UMKM Modern Di Kecamatan Dungingi," *Abdimas Awang Long* 8, no. 1 (2025): 137–50.

systems. This poses a serious risk to consumer trust, which serves as the foundation of the digital ecosystem.

By comparison, China has adopted a stricter approach to personal data protection through the Personal Information Protection Law (PIPL). This approach is top-down, whereby the government exercises full control over the regulation, supervision, and enforcement of personal data protection laws. Furthermore, China has integrated artificial intelligence-based (AI-driven) compliance technologies to enhance the effectiveness of data protection, particularly for business actors, including MSMEs. With such technology, automated monitoring systems can detect and mitigate the risks of data breaches and ensure business compliance with applicable regulations. On the other hand, Indonesia's approach tends to be more hybrid, where government regulation operates alongside private sector and industry efforts to develop data protection mechanisms. This approach allows MSMEs flexibility to adopt data protection strategies according to their capacities; however, it also risks creating disparities in compliance levels and the standards of data protection applied. The low level of awareness regarding the importance of data protection, limited technological resources, and the lack of strict law enforcement remain major challenges in implementing data protection policies for MSMEs in Indonesia.

Given the differing approaches between Indonesia and China, a critical question arises regarding the most effective and adaptive model of personal data protection for MSMEs. China's top-down model has succeeded in establishing a strict compliance system; however, this model may be difficult to implement in Indonesia, which has a more diverse business ecosystem and more flexible regulatory frameworks. Therefore, a hybrid model is needed—one that combines the strength of government regulation with technology-based compliance automation—to ensure better data protection for MSMEs without imposing an excessive burden on them.

A study conducted by Endah Fuji Astuti, Achmad Nizar Hidayanto, Sabila Nurwardani, and Ailsa Zayyan Salsabila[6] focuses on

[6] Endah Fuji Astuti et al., "Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001: 2013.," *International Journal of Safety & Security Engineering* 14, no. 5 (2024).

the level of awareness and compliance of Indonesian MSMEs with the PDP Law and the international standard ISO/IEC 27001:2013. Using a quantitative survey-based approach, the study reveals that most MSME actors still possess a limited understanding of the importance of personal data protection. The research underscores the need for education and regulatory outreach, even though it does not provide a comparative analysis with practices in other countries or offer a comprehensive legal examination of data protection approaches.

Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga[7] address the issue of personal data protection in Indonesia through a comparative legal analysis of practices in China, South Korea, and Singapore. Although the study does not specifically examine digital MSMEs, it offers strategic insights into how Indonesia can adopt best practices from countries with more advanced personal data protection regulations. Its contribution lies in outlining a roadmap for strengthening national policy based on cross-country learning. Meanwhile, Ninne Zahara Silviani, Rina Shahriyani Shahrullah, Vanessa Riarta Atmaja, and Park Ji Hyun[8] conduct a comparative study of personal data protection legal systems in the private sector between Indonesia and South Korea. This research primarily focuses on electronic systems within the business sector, without specifically addressing MSMEs. Nevertheless, it provides an in-depth understanding of the challenges faced by the private sector in implementing personal data protection systems, including issues related to regulatory frameworks and legal infrastructure.

A study by Muhammad Fadel Adhyputra, Thoriq Ahmadi, and Mohammad Rifqi[9] offers an institutional approach by designing a model

[7] Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 95–109.

[8] Ninne Zahara Silviani et al., "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea," *Jurnal Hukum Dan Peradilan* 12, no. 3 (2023): 517–46.

[9] Muhammad Fadel Adhyputra, Thoriq Ahmadi, and Mohammad Rifqi, "Analisis Komparatif Rancangan Lppdp Indonesia Dengan Otoritas Pelindungan Data Singapura Dalam Penegakan Hukum Pelanggaran Data Pribadi: The Notion Of Personal Data Protection By Indonesia's LPPDP: A Comparative Study With The Singapore Personal Data Prot," *Jurnal Nomokrasi* 2, no. 2 (2024): 56–74.

for a data protection supervisory authority in Indonesia, referring to the authority structure in Singapore. This study is conceptual and makes a significant contribution to the establishment of an independent body responsible for overseeing and enforcing personal data protection laws. The focus is not on the protection model itself, but rather on the institutional framework that supports the sustainability of the data protection system. Another study by Al Sentot Sudarwanto and Dona Budi Kharisma[10] compares personal data protection regulations in the digital economy sector among Indonesia, Hong Kong, and Malaysia. This research adopts a general legal approach and does not specifically address digital MSMEs. However, its findings provide insights into the complexity of personal data protection in the cross-border digital economy context, as well as the potential for policy harmonization to support secure and sustainable digital economic growth.

Based on the aforementioned previous studies, this article presents a unique focus on a hybrid model of personal data protection specifically tailored for consumers of digital MSMEs and a comparative analysis of regulations in Indonesia and China. In contrast, the five studies discussed above offer different perspectives in terms of geographical focus, methodological approach, and sectors analyzed. Nevertheless, they all make important contributions to the understanding of the personal data protection landscape in the digital era.

The development of digital technology in the era of Industry 4.0 towards Society 5.0 has enabled the application of artificial intelligence and blockchain-based solutions to enhance data security.[11] China has utilized such technologies to manage business compliance with data regulations, whereas in Indonesia, the application of similar technologies remains limited. By adopting AI-driven compliance principles, MSMEs in Indonesia can improve the efficiency of managing consumers' personal data while simultaneously reducing the risk of legal violations.

[10] Al Sentot Sudarwanto and Dona Budi Budi Kharisma, "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia," *Journal of Financial Crime* 29, no. 4 (2022): 1443–57.

[11] Blassyus Bevry Sinaga and Raia Putri Noer Azzura, "Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan Di Era Society 5.0," *Padjadjaran Law Review* 12, no. 1 (2024): 71–82.

The success of a hybrid model for personal data protection in MSMEs also heavily depends on the synergy between the government, industry, and academia. The government must strengthen policies and supporting infrastructure, the industry should play a role in providing accessible technological solutions for MSMEs, while academia can contribute through research and innovations that support evidence-based policymaking. A comparative study with China can offer valuable insights into strategies that have proven effective in data protection oversight, enabling Indonesia to adapt relevant elements that suit its local needs and conditions.

In the context of increasingly complex regulations, MSMEs often face difficulties in understanding their legal obligations regarding personal data protection.[12] Therefore, a more systematic and technology-based educational approach is necessary, such as application-based compliance systems that can provide MSMEs with automated guidance on how to manage personal data securely. A hybrid model that integrates such technology with government regulation could offer a more practical and sustainable solution for MSMEs in Indonesia.

The urgency of this research is grounded in the legal rationale that legal protection of consumers' personal data in Indonesia's digital MSME sector remains weak. Although the PDP Law has been enacted, its implementation is still uneven, particularly among MSMEs that lack adequate legal and technological resources. In contrast, China has developed a comprehensive regulatory approach through the PIPL, which effectively integrates state supervision mechanisms with the accountability of digital enterprises. A comparative study between Indonesia's and China's regulations is therefore essential as a basis for formulating a hybrid model that can more effectively and sustainably accommodate the needs of personal data protection within Indonesia's digital MSME sector.

Philosophically, personal data protection reflects a respect for human rights[13], particularly the right to privacy, which is an integral part

[12] Yuyut Prayuti, "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik e-Commerce Dan Perlindungan Data Konsumen Di Indonesia," *Jurnal Interpretasi Hukum* 5, no. 1 (2024): 903–13.

[13] Hari Sutra Disemadi et al., "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?," *Sang Sewagati Journal* 1, no. 2 (2023): 66–90.

of human dignity. In practice, many digital MSME actors in Indonesia still lack an understanding of ethical principles in managing consumer data, making violations of the right to personal information more likely. This research is grounded in the values of justice, individual autonomy, and social responsibility, highlighting the need for a data protection system that not only relies on formal regulation but also cultivates a culture of ethical compliance in business practices. The proposed hybrid model aims to create a balance between state legal approaches and ethical corporate practices, thereby contributing to the development of a legal order that is humane, adaptive, and responsive to digital dynamics.

From a sociological perspective, the rapid digitalization of MSME activities has transformed consumer behavior in Indonesia, with online transactions becoming the primary choice.[14] However, this development has not been accompanied by a corresponding increase in digital literacy, particularly concerning personal data protection. Many consumers still lack awareness of their rights over personal information,[15] MSME actors often overlook data security aspects in their digital business operations. This situation risks undermining public trust in the digital economy ecosystem. Therefore, this research is essential to respond to these social realities by developing a personal data protection framework that is not merely legalistic but also considers Indonesia's social and cultural context while drawing lessons from China's regulatory system, which has successfully integrated law, technology, and social awareness.

This research aims to propose a hybrid personal data protection model that combines government regulation with artificial intelligence-based technological approaches, drawing lessons from China's experience in managing data protection through a top-down approach. This model is expected to create a balance between regulatory compliance and ease of implementation for MSMEs, thereby ensuring the protection of consumers' personal data without hindering digital

[14] Christian Napitupulu et al., "Peranan Ekonomi Digital Dalam Pertumbuhan Ekonomi Di Indonesia," *Jurnal Penelitian Ilmiah Multidisipliner* 1, no. 03 (2025): 138–45.

[15] ROAG Pardosi and Yuliana Primawardani, "Perlindungan Hak Pengguna Layanan Pinjaman Online Dalam Perspektif Hak Asasi Manusia (Protection of the Rights of Online Loan Customers from a Human Rights Perspective)," *Jurnal Ham* 11, no. 3 (2020): 353–67.

economic growth in Indonesia. This study will focus on three main aspects: (1) a comparative analysis of the top-down legal approach in China and the hybrid approach in Indonesia in the context of personal data protection for MSMEs; (2) an analysis of the implementation of technology-based regulations to improve MSME compliance with personal data protection requirements; and (3) recommendations for an adaptive personal data protection model for MSMEs in the digital era. Through a comprehensive approach, this research is expected to make a significant contribution to the development of more effective and innovative personal data protection policies in Indonesia.

This article uses a normative legal research[16], with a statutory approach[17], a conceptual approach, and a comparative law approach.[18] The statutory approach is employed to examine the regulations governing personal data protection for consumers in Indonesia and China, particularly in the context of digital MSME actors. The conceptual approach is used to understand the fundamental concepts of personal data protection, legal protection models, and the position of consumers as legal subjects in the digital transformation era. Meanwhile, the comparative law approach is utilized to compare the legal frameworks and the implementation of personal data protection between Indonesia and China, in order to identify the strengths and weaknesses of each system, which can serve as the basis for formulating a hybrid model of consumer data protection in the digital MSME sector. The research is conducted in two main regions: Indonesia and China. In Indonesia, the research focuses on national regulations such as the PDP Law, EIT Law, and sectoral regulations related to digital MSMEs. In China, the research examines the PIPL and other relevant regulations.

[16] Muhammad Zainuddin and Aisyah Dinda Karina, "Penggunaan Metode Yuridis Normatif Dalam Membuktikan Kebenaran Pada Penelitian Hukum," *Smart Law Journal* 2, no. 2 (2023): 114–23.

[17] Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer," *Gema Keadilan* 7, no. 1 (2020): 20–33.

[18] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 8, no. 8 (2021): 2463–78.

The data used in this research is secondary data, consisting of primary legal materials (legislation), secondary legal materials (scientific literature, journals, books, and previous research findings), and tertiary legal materials (legal dictionaries, legal encyclopedias).[19] Data collection techniques are carried out through library research (documentation), with limited observation of data protection practices by digital MSMEs to address the issues under study. The collected data is then analyzed using a descriptive qualitative approach, which involves examining the legal substance, comparing practices across countries, and formulating a hybrid model of personal data protection that is relevant to the characteristics of Indonesia's national legal framework and the development of digital MSMEs. The results of this analysis are expected to contribute both theoretically and practically to the development of consumer personal data protection policies.

A. Legal Framework for Consumer Personal Data Protection under the National Legal System of Indonesia

Personal data protection constitutes a fundamental human right[20] as part of the protection of individual privacy; therefore, it requires a legal basis to ensure the security of personal data in accordance with the 1945 Constitution of the Republic of Indonesia (Constitution 1945). The current legislative framework for personal data regulation has been established under the PDP Law to enhance the effectiveness of personal data protection implementation.[21] The aspects of personal data protection in Indonesia are reflected in several statutory regulations, which the author outlines as follows:

[19] Sholahuddin Al-Fatih, *Perkembangan Metode Penelitian Hukum Di Indonesia* (UMMPress, 2023).

[20] Nela mardiana Parihin, "Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia," *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 5, no. 1 (2023): 16–23.

[21] Faiz Rahman, "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia," *Jurnal Legislasi Indonesia* 18, no. 1 (2021): 81–102.

1. Law Number 8 of 1997 concerning Company Documents

   Complementing the provisions on Archival Principles, which primarily regulate public aspects, the scope of company-related matters is further regulated under Law Number 8 of 1997 concerning Company Documents.[22] Article 1 defines Company Documents as data, records, and/or information created or received by a company in the course of carrying out its activities, whether written on paper or other media, or recorded in any form that can be seen, read, or heard.
2. Law Number 7 of 1992, in conjunction with Law Number 10 of 1998 concerning Banking

   Provisions related to personal data protection in the Banking Law concern the issue of bank secrecy. Pursuant to Article 40 of Law Number 10 of 1998, banks are obligated to maintain the confidentiality of information regarding depositors and their deposits, except in circumstances as stipulated in Articles 41, 41A, 42, 43, 44, and 44A. These exceptions include matters related to taxation, settlement of bank receivables, judicial proceedings in criminal cases, and, upon the request, consent, or authorization of the depositor, under which the bank may disclose confidential information, provided that specific procedures are followed.[23]
3. Law Number 36 of 1999 concerning Telecommunications

   According to the Government Regulation of 2000 on the Implementation of Telecommunications, which serves as the implementing regulation of Law Number 36 of 1999 concerning Telecommunications, the internet is classified as a type of multimedia service, identified as a telecommunications

[22] Benjamin Lemta Luntungan and Andhika Arthawijaya, "Legal Analysis of Law No. 27 of 2022 Concerning Personal Data Protection (Decision No. 597/Pid. Sus/2021/Pn. Jkt. Pst)," *Formosa Journal of Sustainable Research* 4, no. 3 (2025): 553–60.

[23] Vicky Katiandagho, Diana Darmayanti Putong, and Isye Junita Melo, "Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia," *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 1 (2023): 106–14.

service provider offering services based on information technology. This indicates that internet regulation falls within the scope of telecommunications law. Law Number 36 of 1999 concerning Telecommunications regulates several matters relating to the confidentiality of information. Article 22 stipulates that any person is prohibited from unlawfully, without authorization, or through manipulation: (a) accessing telecommunications networks; and/or (b) accessing telecommunications services; and/or (c) accessing special telecommunications networks. Violation of these provisions is subject to a maximum imprisonment of six years and/or a maximum fine of IDR 600 million. Furthermore, Article 40 provides that any person is prohibited from intercepting information transmitted through telecommunications networks in any form. Violation of this provision is subject to a maximum imprisonment of fifteen years.

The Telecommunications Law also regulates the obligation of telecommunications service providers to maintain the confidentiality of information transmitted and/or received by customers through telecommunications networks and/or telecommunications services provided by them (Article 42, paragraph 1). Any service provider who violates this obligation is subject to a maximum imprisonment of two years and/or a maximum fine of IDR 200 million. Furthermore, telecommunications service providers are obliged to record information required for criminal justice proceedings upon written request by the Attorney General and/or the Chief of the Indonesian National Police for specific criminal offenses, namely offenses punishable by imprisonment of five years or more, life imprisonment, or the death penalty. Investigators may also submit such requests.

4. Law Number 24 of 2013 concerning the Amendment to Law Number 23 of 2006 on Population Administration

The definition of personal data is regulated under Article 84 paragraph (1) of this Law, which includes: information concerning physical and/or mental disabilities, fingerprints, iris scans, signatures, and other data elements that may constitute a person's disgrace. Article 86 stipulates that the Minister, as the responsible authority, grants access rights to Personal Data for provincial officers and officers of the Implementing Agencies. These officers are prohibited from disseminating Personal Data beyond their authorized capacity. Furthermore, Article 95A provides that:

> *"Any person who unlawfully disseminates Population Data as referred to in Article 79 paragraph (3) and Personal Data as referred to in Article 86 paragraph (1a) shall be subject to imprisonment for a maximum of 2 (two) years and/or a maximum fine of IDR 25,000,000.00 (twenty-five million rupiahs)."*

5. Law Number 43 of 2009 concerning Archiving

   Unlike the previous laws, this replacement law now regulates not only the management of archives within government institutions but also the management of archival systems by state institutions, local governments, educational institutions, companies, political organizations, community organizations, individuals, and archival institutions. Within this archival system, personal data and/or personal information of individuals may also be included. The term 'archive' here refers to records of activities or events in various forms and media, in accordance with developments in information and communication technology. Regarding personal data protection, this law stipulates that archival institutions and archive creators may restrict access to archives if their disclosure to the public could reveal secrets or personal data.[24]

   This law also regulates data security, including provisions on criminal sanctions for any person who intentionally provides dynamic archives to unauthorized archive users. Article 3 stipulates that the purposes of archiving include,

[24] Alifia Jasmine, Benny Djaja, and Maman Sudirman, "Tanggung Jawab Notaris Dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi.," *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 5, no. 1 (2024).

among others, ensuring the protection of state interests and citizens' civil rights through the management and utilization of authentic and reliable archives, as well as ensuring the safety and security of archives as evidence of accountability in social, national, and state life. Furthermore, it is also stated that one of the principles established under this law is the principle of safety and security.

6. Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions

   Regulations regarding the protection of personal data of internet users are further stipulated in the Law on Electronic Information and Transactions (EIT Law). Although this Law does not yet contain specific provisions on personal data protection, it implicitly introduces a new understanding regarding the protection of the existence of electronic data or information, whether of a public or private nature. Personal data protection within an electronic system under the EIT Law includes protection from unauthorized use, protection by electronic system providers, and protection against illegal access and interference. In relation to the protection of personal data from unauthorized use, Article 26 of the EIT Law requires that any use of personal data within electronic media must obtain the consent of the data owner concerned. Any person who violates this provision may be subject to a lawsuit for any losses incurred.

   Article 26 of the EIT Law stipulates the following:

   > " 1) *The use of any information through electronic media that involves a person's personal data must be carried out with the consent of the person concerned.*
   > 2) *Any person whose rights as referred to in paragraph (1) are violated may file a lawsuit for any losses incurred based on this Law."*

   The Elucidation of Article 26 of the EIT Law states that personal data is part of an individual's personal rights.

Meanwhile, Article 1 of Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions defines personal data as specific individual data that is stored, maintained, and ensured for its accuracy, and whose confidentiality is protected. If interpreted generally, data protection is actually regulated in subsequent articles of the EIT Law, namely Articles 30 to 33 and Article 35, which are part of Chapter VII on Prohibited Acts. The EIT Law explicitly prohibits any unlawful access to another person's personal data through an electronic system to obtain information by breaching security systems.

7. Law Number 27 of 2022 on Personal Data Protection

   Personal data protection in Indonesia now has a strong legal basis through Law Number 27 of 2022 on Personal Data Protection. One of the key provisions in this Law is the classification of personal data as stipulated in Article 3. Personal data is classified into two categories, namely general personal data and specific personal data. General personal data includes information such as full name, gender, nationality, religion, and other data that can identify an individual. Meanwhile, specific personal data covers sensitive information, including health data, biometric data, genetic data, sexual orientation, political views, criminal records, personal financial data, children's data, and other data protected under statutory regulations. This classification is essential because it determines the level of protection and the procedures that must be followed in processing personal data.

The PDP Law also explicitly regulates the rights of personal data subjects, as set forth in Chapter III (Articles 4 to 16). These rights include the right to obtain clear information regarding the processing of their personal data, the right to access, rectify, and erase their personal data. Data subjects also have the right to withdraw consent previously given to the personal data controller, and the right to claim compensation in the event of a data breach. These rights position individuals as fully protected subjects over their own data, while also imposing obligations on data controllers to maintain the integrity and security of personal data.

The regulation of personal data processing receives significant attention under the PDP Law, which is specifically set out in Chapter IV (Articles 17 to 22). Personal data processing must adhere to the principles of prudence, fairness, and transparency. This process includes the collection, storage, use, disclosure, and deletion of personal data. The PDP Law emphasizes that any data processing must be based on legitimate and clear purposes. It must be carried out in accordance with ethical standards and the protection of data subjects' rights. In the context of digital MSMEs, these provisions present specific challenges, considering that many business actors have yet to understand the fundamental principles of personal data protection fully.

The PDP Law also comprehensively regulates the obligations of personal data controllers and processors. These provisions are set out from Article 23 to Article 50, comprising a total of 28 articles that detail their responsibilities and duties. Data controllers and processors are required to provide transparent information regarding the lawfulness of data processing, the purpose of processing, the type of data being processed, and the consent obtained from the data subject. Moreover, they must be able to demonstrate evidence of such consent when necessary. These provisions also include strict regulations on the transfer of personal data to third parties or abroad, as well as administrative sanctions for violations, in order to anticipate and prevent potential misuse of data that could harm the personal data subject.

The PDP Law also contains provisions on prohibitions in the use of personal data, including a ban on any party processing or collecting personal data without proper authority or valid consent. This prohibition also applies to the use of personal data processing tools, such as cameras or other data collection devices, when used for personal interests that may harm the data subject. Thus, this provision aims to prevent the exploitation of personal data by irresponsible parties, especially in the digital sphere, which is vulnerable to data misuse.

To strengthen the implementation of personal data protection, the PDP Law also encourages the establishment of a code of conduct for personal data controllers, which is to be formulated by business associations.[25] This code of conduct must be formulated considering the purposes and principles of personal data processing and the interests of personal data owners. The objective is to establish uniform ethical and operational standards among business actors.[26], including MSMEs, to ensure compliance with legal provisions and to provide optimal protection for consumers.

The PDP Law also regulates the dispute resolution mechanism concerning personal data breaches, as stipulated in Article 56. Dispute resolution can be carried out through various channels, including arbitration, court proceedings, or other alternative dispute resolution (ADR) mechanisms. This provision grants personal data owners the opportunity to seek justice and claim compensation for damages suffered as a result of personal data breaches. Moreover, it aims to promote legal certainty in personal data protection disputes in Indonesia.[27]

The PDP Law recognizes the importance of international cooperation in addressing cross-border personal data protection issues. Therefore, Article 57 stipulates that the Indonesian government may cooperate with foreign governments or international organizations to achieve better protection of personal data. This cooperation aims to harmonize data protection standards and strengthen efforts to prevent cybercrimes involving cross-border personal data. Additionally, the PDP Law also provides for legal consequences for violations of personal data protection provisions, including imprisonment for up to 7 years and a maximum fine of up to IDR 70 billion.

The enactment of the PDP Law represents a significant breakthrough in the efforts to protect personal data in Indonesia, particularly amid the challenges of digitalization and the increasing

[25] Jelvica Meiceline Tampi, "Tinjauan Yuridis Terhadap Pelanggaran Privasi Berdasarkan UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Tokopedia)," *LEX ADMINISTRATUM* 13, no. 1 (2025).

[26] Dasep Suryanto and Slamet Riyanto, "Implementasi Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dalam Industri Ritel Tinjauan Terhadap Kepatuhan Dan Dampaknya Pada Konsumen," *VERITAS* 10, no. 1 (2024): 121–35.

[27] Iran Sahril and Dhody A R Widjaja Atmadja, "Perlindungan Data Pribadi Konsumen, Dokumen Dan Tanda Tangan Elektronik Yang Dipergunakan Oleh Pihak Ketiga Dalam Transaksi E-Commerce," *CENDEKIA: Jurnal Penelitian Dan Pengkajian Ilmiah* 2, no. 2 (2025): 173–89.

number of data breaches. The PDP Law serves as a national legal framework that fills previous regulatory gaps and affirms the rights and obligations of both data subjects (owners) and data controllers and processors. Although its implementation still faces challenges, especially for MSMEs that are limited in terms of technology and legal understanding, the PDP Law has established a solid foundation for the personal data protection system in Indonesia. Therefore, serious commitment from the government, business actors, and society is required to optimize the enforcement of this law, including by adopting best practices such as hybrid models that combine strict supervision and AI-based technology, as implemented in China.

Law serves as an instrument that regulates the relationships between individuals as well as between individuals and the state, in order to prevent chaos in social interactions. The purpose of law is to establish order, justice, and utility in societal life.[28] The three main pillars of the purpose of law, as proposed by Gustav Radbruch—justice (*Gerechtigkeit*), legal certainty (*Rechtssicherheit*), and utility (*Zweckmäßigkeit*)—serve as the fundamental basis for the formulation and application of law across various fields.[29] In the context of digital transformation, the law is also required to be adaptive to technological developments in order to remain relevant and capable of protecting the rights of citizens, including the right to personal data as part of fundamental private rights.

In this context, the purpose of law can be viewed from legal, philosophical, and sociological perspectives. The legal objective of consumer personal data protection is to establish a solid legal foundation for the management of personal data in a lawful manner, particularly within the digital MSME sector. In Indonesia, the PDP Law serves as the primary legal framework that regulates the rights and obligations of data subjects and data controllers. However, its implementation in MSMEs still faces structural challenges and low legal awareness. In the hybrid

[28] Dino Rizka Afdhali and Taufiqurrohman Syahuri, "Idealitas Penegakkan Hukum Ditinjau Dari Perspektif Teori Tujuan Hukum," *Collegium Studiosum Journal* 6, no. 2 (2023): 555–61.

[29] Renaldy Afriyanto et al., "Eksistensi Asas Kepastian Hukum, Kemanfaatan Hukum Dan Keadilan Hukum Sebagai Tujuan Hukum Di Indonesia Dalam Perspektif Para Filsuf," *Unizar Law Review* 7, no. 2 (2024): 203–11.

model, which is compared with the Chinese system, where the state plays a more central role, the Indonesian legal approach seeks to combine the role of the state and the responsibility of business actors in a proportional manner. This aims to provide effective legal protection while remaining contextual with the capacity of MSME actors.

From a philosophical perspective, consumer personal data protection reflects respect for dignity and human rights in the digital world. The law not only functions normatively but also reflects core values within society, such as justice, protection of individual vulnerabilities, and social responsibility. In the context of digital MSMEs, many consumers come from groups with low digital literacy, making legal protection based on humanistic values crucial. Meanwhile, the sociological objective of this protection is to create social stability and public trust in the digital economy. Strong data protection will enhance the participation of consumers and MSME actors in the digital ecosystem, while also fostering inclusive economic growth. This hybrid model demonstrates that a collaborative and adaptive data protection approach, responsive to social dynamics, has a positive impact on the sustainable digital societal order.

B. Issues of Consumer Personal Data Protection in the Era of Digital Transformation in Indonesia

In line with the rapid advancement of information technology, data has become an exclusive commodity.[30] The protection of data has now become an important phenomenon, as preventive measures against the destruction of data and information require careful consideration for their legal protection.[31] The security and confidentiality of data within computer networks have now become crucial and continuously evolving

[30] Yulu Jin and Yu Wang, "Balancing Smart City Development and Personal Data Protection: A Regulatory Framework," *International Review of Economics & Finance*, 2025, 104022.

[31] Thomas C King et al., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions," *Science and Engineering Ethics* 26 (2020): 89–120.

issues.[32] Various cases related to system security today require significant handling and protection costs.[33] Vital systems, such as defense systems, banking systems, and other systems of similar importance, demand extremely high levels of security.[34] This need arises primarily due to advances in computer networking, particularly with the open system concept, which allows anyone, anywhere, and at any time, to access these critical areas potentially.

To maintain the security and confidentiality of data within a computer network, various types of encryption are required so that the data cannot be read or understood by unauthorized persons, except for the rightful recipient. The purpose of data protection, in addition to enhancing data security, also serves to:[35]

a. Protect the data from being read by unauthorized individuals;
b. Prevent unauthorized individuals from inserting or deleting data.

This concept applies to the security and confidentiality of data within computer networks and to the security and confidentiality of data on the Internet.[36] This is due to the significant advancements achieved in the development of computer operating systems and their utilities, where performance, reliability, and software flexibility have become primary criteria, making the information highly valuable. Supported by the

[32] Naeem AllahRakha, "Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds," *Lex Scientia Law Review* 8, no. 1 (2024): 405–32.

[33] Junaidi Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil, "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory," *Journal of Law and Legal Reform* 5, no. 2 (2024).

[34] Susilowati Suparto et al., "Consumer Protection of Girls from Cybercrime in a Gender Perspective," *Journal of Law and Legal Reform* 5, no. 4 (2024): 2045–70.

[35] Purwanto Putra, "Menyelamatkan Dan Potensi Penyelamatan Ekonomi Pasca Covid-19:: Adopsi Kebijakan Literasi Digital Untuk Sektor UMKM," *IKOMIK: Jurnal Ilmu Komunikasi Dan Informasi* 2, no. 1 (2022): 21–28.

[36] Badhan Chandra Das, M Hadi Amini, and Yanzhao Wu, "Security and Privacy Challenges of Large Language Models: A Survey," *ACM Computing Surveys* 57, no. 6 (2025): 1–39.

capability to develop software, this situation naturally attracts the interest of hackers and intruders.[37]

The issue of data security and confidentiality is one of the most critical aspects of an information system.[38] This relates to the significance of ensuring that information is sent and received only by authorized parties. Information loses its value if it is intercepted or hijacked by unauthorized individuals. Therefore, security within information systems has become a prominent issue since the introduction of electronic transactions.[39] Without strict and sophisticated security measures, the development of information technology will not provide optimal benefits to society.[40]

The rapid development of information technology has turned data into a highly valuable commodity while simultaneously creating new challenges in terms of its protection, especially in the context of personal data protection.[41] In the business sector, particularly for MSMEs, the management and protection of consumers' personal data have become critical issues.[42] MSMEs often rely on digital systems to support their business operations, such as marketing, payment, and customer relationship management. However, advancements in computer network technology, with its open system concept, make access to such

[37] Depavath Harinath et al., "Enhanced Data Security and Privacy in IoT Devices Using Blockchain Technology and Quantum Cryptography," *Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793)* 34, no. 6 (2024).

[38] Claudio Novelli et al., "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," *Computer Law & Security Review* 55 (2024): 106066.

[39] Anil Kumar Yadav Yanamala, Srikanth Suryadevara, and Venkata Dinesh Reddy Kalli, "Balancing Innovation and Privacy: The Intersection of Data Protection and Artificial Intelligence," *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence* 15, no. 1 (2024): 1–43.

[40] Tayssir Bouraffa and Kai-Lung Hui, "Regulating Information and Network Security: Review and Challenges," *ACM Computing Surveys* 57, no. 5 (2025): 1–38.

[41] Mohd Javaid et al., "Digital Economy to Improve the Culture of Industry 4.0: A Study on Features, Implementation and Challenges," *Green Technologies and Sustainability*, 2024, 100083.

[42] Prayuti, "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik e-Commerce Dan Perlindungan Data Konsumen Di Indonesia."

data vulnerable to hacking threats, potentially creating opportunities for irresponsible parties to misuse consumers' personal data.

The systems used by MSMEs may not be as complex as banking or national defense systems; however, they still store sensitive data that requires protection. The risks of cyberattacks, data interception, and information theft pose significant challenges for MSMEs[43], particularly when they lack sufficient resources to adopt the advanced security measures necessary.[44] Therefore, the concept of data security, which involves encryption and other protective measures, becomes highly relevant for MSMEs to ensure that consumer data remains secure and inaccessible to unauthorized parties.

The protection of personal data within computer networks in MSMEs must also be addressed with due seriousness, as data breaches or misuse can severely undermine consumer trust and damage business reputation. When consumers do not feel confident that their personal data is secure, they are likely to hesitate in conducting further transactions. This situation will have adverse effects on the growth and sustainability of MSMEs, which heavily rely on maintaining good relationships with consumers. Therefore, safeguarding consumers' personal data through the implementation of appropriate policies and technologies must be a priority for MSMEs. This challenge becomes increasingly complex with the existence of regulations on personal data protection, which require every business actor, including MSMEs, to comply with specific standards in the management and protection of personal data. MSMEs must recognize that, despite their small scale, legal obligations concerning data protection remain fully applicable to them. Without the implementation of appropriate data protection policies, MSMEs may face legal risks and sanctions that could jeopardize the continuity and sustainability of their businesses.

[43] Sabri Balafif, "Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework," *Jurnal Informatika: Jurnal Pengembangan IT (JPIT)* 8, no. 291 (2023).

[44] Nita Maharani Harahap, "Resiko Kejahatan Teknologi Informasi Dan Komunikasi Cyber Crime Dan Analisi Inovasi Pencegahan Resiko Cyber Crime Di Indonesia," *Jurnal Teknologi Dan Manajemen Sistem Industri* 3, no. 1 (2024): 52–59.

C. Legal Framework on MSMEs Through Personal Data Protection in China

China, as a current global economic powerhouse, has articulated its vision through the "China Grand Strategic Goal: A Leading High-end Manufacturing Superpower." The rapid growth of China's MSMEs is closely linked to the country's unique social characteristics. The development of MSMEs in China reflects a form of grassroots capitalism, which has fostered the emergence of collaborative policies that successfully create a supportive ecosystem for MSMEs. This ecosystem is formed through the synergy between the Chinese government, characterized by strong institutional capacity within a market economy system, and MSME actors. Rather than exploiting market power solely for the benefit of dominant economic forces, China deliberately strives to build a conducive environment for MSME growth, enabling the country to maintain its competitive advantage in the global economic arena. To promote MSME development, China has implemented four main policy focuses: (1) investment in technological innovation to enhance productivity, (2) development of industries based on local resources to ensure contextual relevance and efficiency, (3) establishment of strategic industrial network ecosystems to expand access to technology and markets, and (4) application of monopolistically competitive trade policies that encourage fair competition among MSMEs operating in similar yet non-identical sectors.[45]

The Chinese government promotes the growth of MSMEs through a variety of strategic policies, including the provision of credit and financial support, the establishment of special economic zones, and the enhancement of market access. The government offers low-interest credit schemes, credit guarantees, and special funding for certified MSMEs, accompanied by bureaucratic reforms aimed at facilitating business development. Special economic zones are also created with fiscal incentives to encourage high-tech MSMEs certified as "Specialized MSMEs," alongside a classification system for MSMEs based on sector,

[45] Cindy Pramita, Sudarmiatin Sudarmiatin, and Ludi Wishnu Wardhana, "Consumer Satisfaction with Non-Halal Culinary MSMEs at PIK through a Chinese-Themed Atmosphere and Stakeholder Involvement," *Jurnal of Management and Social Sciences* 3, no. 1 (2025): 1–8.

size, and assets to ensure more targeted policymaking. Moreover, the government expands MSMEs' access to both domestic and international markets through trade fair support, e-commerce platforms, and export promotion programs designed to strengthen domestic industrial value chains.

In addition, China enhances MSME skills and innovation capacity through training programs, entrepreneurship education, and research and development support, while continuing to develop essential infrastructure such as transportation, energy, and information technology. The government also enforces stricter personal data protection policies through the PIPL to safeguard consumer data security and promote cybersecurity awareness among MSMEs. However, despite the implementation of these various policies, challenges remain, including complex bureaucratic processes, unequal access to resources, and low awareness of data protection issues — all of which need to be addressed to optimize MSME growth in China's digital economy era.

The protection of personal data in China has increasingly become a crucial issue, not only for large corporations but also for MSMEs. The PIPL, which came into effect on November 1, 2021, constitutes a significant part of China's new regulatory framework governing the processing of personal information by entities or individuals within the country. This implies that MSMEs are also required to pay serious attention to personal data protection in the course of their business activities, particularly when handling consumer information. Although MSMEs operate on a smaller scale compared to large corporations, they are nonetheless legally obliged to comply with the provisions set forth under PIPL.

Consumer data protection has become increasingly important, as violations may lead to serious legal consequences, including fines and administrative sanctions. As part of the digital economic ecosystem, MSMEs in China are required to adopt appropriate security measures, including ensuring that consumer data is securely stored and processed.[46]

[46] Lin Liang and Yan Li, "How Does Government Support Promote Digital Economy Development in China? The Mediating Role of Regional Innovation Ecosystem Resilience," *Technological Forecasting and Social Change* 188 (2023): 122328.

The data protection regime in China is currently undergoing significant transformation with the introduction of the Personal Information Protection Law (PIPL), the Cybersecurity Law of the People's Republic of China (CSL), and the Data Security Law of the People's Republic of China (DSL). These three laws operate in tandem to establish a robust regulatory framework for cybersecurity and data protection. MSMEs, as part of the broader business landscape, are required to understand and implement appropriate measures to safeguard consumers' personal data and to ensure compliance with the applicable regulations.

Articles 38 and 40 of the Constitution of China set forth rights related to privacy, such as the right to personal dignity, which prohibits acts of insult, defamation, false accusations, or dissemination of false information against Chinese citizens, and the right to freedom and confidentiality of correspondence. However, these provisions do not explicitly establish a constitutional right to privacy, even though their subject matter may be closely related to the concept of privacy.

China's data protection regime is currently undergoing a period of transformation, with significant progress achieved in the field of data protection legislation in recent years.[47] The Personal Information Protection Law (PIPL) regulates the processing of personal information carried out by entities or individuals within China and, together with two other key statutes on cybersecurity and data protection—the Cyber Security Law of the People's Republic of China (CSL) and the Data Security Law of the People's Republic of China (DSL)—introduces a new and comprehensive data protection regime for China.

The PIPL establishes the framework for personal information protection in China and is, in part, modeled after the General Data Protection Regulation (GDPR). PIPL introduces several key concepts, including personal information, sensitive personal information, and processing. It explicitly sets out its extraterritorial jurisdiction and incorporates traditional elements of data protection, such as the principles of personal information processing, the legal bases for consent

[47] Xi Lin, "A Model of Big Data-Based Governance: China's National Government Big Data Platform and an Analysis of Its Governance Competence," *Chinese Political Science Review*, 2025, 1–40.

and objection to processing, cross-border data transfer mechanisms, and data subject rights.

On November 7, 2016, the Cybersecurity Law (CSL), which came into force on June 1, 2017, was enacted in China. The CSL contains personal information protection requirements applicable to all companies operating computerized information network systems. The CSL serves as the fundamental law governing cyberspace, with a primary focus on multi-level cybersecurity protection, critical information infrastructure protection, cybersecurity reviews and inspections, as well as the certification of key network devices and specialized cybersecurity products. Although the CSL, enacted in 2017, is conceptually specific to cybersecurity contexts, it also functions to protect personal information. Following the enactment of the Personal Information Protection Law (PIPL), the CSL's primary focus has shifted toward cybersecurity.[48]

The DSL serves as the fundamental law for data security. It establishes a set of policies, including policies on data categorization and classification, data risk control, data security contingency response, data security review, export control, and anti-discrimination measures, to ensure the proper development and utilization of data and the advancement of the data industry.[49]

The Civil Code of the People's Republic of China, which took effect on January 1, 2021, also explicitly grants the right to privacy and the right to personal information protection under Chapter VII, Part IV on Personality Rights. The explicit protection of personal information under the Civil Code marks a new era in privacy and personal information protection. For the first time, the right to privacy and the protection of personal information are codified as a single, dedicated chapter within the legislation. The right to privacy and personal information is categorized as a personality right, thus providing legal remedies from the perspective of tort law in cases of violations of privacy and/or personal information. Furthermore, for the first time, privacy is defined by law as referring to the peaceful private life of a natural person

[48] Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity* 8, no. 1 (2022): tyac011.

[49] Igor Calzada, "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)," *Smart Cities* 5, no. 3 (2022): 1129–50.

and personal spaces, private activities, and personal information that an individual does not wish to be known to others.

At the end of 2012, the Standing Committee of the National People's Congress enacted a Resolution on Strengthening the Protection of Information on the Internet. Although the Resolution appears primarily aimed at addressing the security of internet usage, it also contains provisions governing the collection and processing of personal information. Furthermore, given its substantive focus—namely, the processing of electronic personal information via the Internet—the Resolution holds potential for broader application compared to many other sector-specific regulations.[50]

The PIPL establishes seven principles governing the processing of personal information, namely: legality, which emphasizes that processing must be lawful, necessary, and conducted in good faith; purpose specification, under which processing must be carried out for specific purposes, be relevant, and minimize interference with individual rights; data minimization, which limits the collection to only the data necessary for the intended purpose; storage limitation, which requires that data be retained only for as long as necessary to fulfill the processing purpose; transparency, which mandates openness in data processing activities; accuracy, to ensure the quality and correctness of data so as to prevent harm to individuals; and data security, which obligates data controllers to safeguard the security of personal data they process.

Under the PIPL, the regulators responsible for personal information protection include the Cyberspace Administration of China (CAC), relevant provincial-level cyberspace administrations, relevant departments of the State Council, and relevant local government departments at the county level and above. In practice, public security authorities (police) are responsible for practical enforcement, the imposition of administrative sanctions, and handling criminal offenses related to privacy violations.

Sector-specific regulators are responsible for overseeing compliance within their respective industries. Examples of such sector-specific supervisory authorities include the National Financial

[50] Emmanuel Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way between the US and the EU?," *Penn St. JL & Int'l Aff.* 8 (2020): 49.

Regulatory Administration (NFRA) (formerly the China Banking and Insurance Regulatory Commission), the National Health and Family Planning Commission (NHFPC), the National Medical Products Administration (NMPA), the Ministry of Science and Technology (MOST), the State Administration for Market Regulation (SAMR), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Transportation (MOT).[51]

If data processing activities are related to national security, several authorities may be involved in the relevant security assessment depending on the specific case. These authorities include the Cyberspace Administration of China (CAC), the National Development and Reform Commission (NDRC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), the Ministry of State Security (MSS), the Ministry of Finance (MOF), the Ministry of Commerce (MOC), the People's Bank of China (PBC), the State Administration for Market Regulation (SAMR), the National Radio and Television Administration (NRTA), the China Securities Regulatory Commission (CSRC), the National Administration of State Secrets Protection (NASSP), and/or the State Cryptography Administration (SCCA).

Government authorities supervising specific sectors are responsible for monitoring compliance with data protection obligations within their respective sectors. The relevant regulators oversee data protection-related activities in their respective industries. The CAC is responsible for the overall planning and coordination of personal information protection efforts, as well as for supervision and management in this area.[52] The relevant departments of the State Council are responsible for personal information protection, supervision, and management within the scope of their respective authorities.[53] The MPS

[51] Florian Kessler, Jost Blöchl, and Yahui Mao, "Data Collection, Use, and Security: Developments in China," in *Standardization Strategies in China and India: Industrial Policy and Geopolitics and Implications for Europe* (Springer, 2025), 231–62.

[52] Lothar Determann et al., "China's Draft Personal Information Protection Law," *Journal of Data Protection & Privacy* 4, no. 3 (2021): 235–59.

[53] Zhen Meng and Lu Wang, "Personal Data Trusts in China: A Balance between Data Sharing and Privacy Protection," *Trusts & Trustees* 31, no. 1 (2025): 15–23.

is responsible for supervising and managing the security and inspection of public information systems, overseeing the protection of classified cybersecurity, and enforcing penalties for cybercrimes.[54] The MIIT is responsible for supervising the cybersecurity of telecommunications and internet enterprises.[55] The NFRA is responsible for overseeing compliance with data protection obligations within the banking and financial industries.[56] The NHFPC is responsible for ensuring compliance with data protection obligations by medical institutions.[57] The NMPA is responsible for ensuring compliance with regulations governing medical products and healthcare services, while the State Administration oversees data protection compliance in the consumer sector for Market Regulation (SAMR).

Under the PIPL, data subjects are granted several fundamental rights, one of which is the right to be informed. Prior to processing personal data, data controllers are obligated to provide a notice that includes information on the identity and contact details of the data controller, the purpose, method, category, and duration of data processing, as well as details regarding any third parties who may access the data. This notice must also cover the use of automated decision-making, processing of sensitive personal data, handling of children's data under the age of 14, cross-border data transfers, and contact information of the data protection officer (DPO). Additionally, individuals have the right to lawfully access their data and to request corrections in cases of errors or incomplete information. PIPL also grants the right to request deletion of personal data under specific circumstances, such as when the processing purpose has been fulfilled or when consent has been withdrawn. Moreover, individuals have the right to object to the processing of their data and the right to data portability, which allows

[54] Daoli Huang, *Research on the Rule of Law of China's Cybersecurity* (Springer, 2022).

[55] Sameer Ullah Khan et al., "The Role of China-Pakistan Relations in the Global Tech Competition, Especially in Areas like 5G, AI, and Cybersecurity," *Review of Education, Administration & Law* 8, no. 1 (2025): 73–85.

[56] Pernot-Leplay, "China's Approach on Data Privacy Law: A Third Way between the US and the EU?"

[57] Juan Cui et al., "National Patient Satisfaction Survey as a Predictor for Quality of Care and Quality Improvement–Experience and Practice," *Patient Preference and Adherence*, 2025, 193–206.

them to request the transfer of their data to another controller. Furthermore, individuals are entitled not to be subjected to automated decision-making that significantly affects their rights and interests. They have the right to seek explanations or object to such decisions. In the context of automated decision-making for marketing purposes, data controllers are required to provide individuals with an option to refuse or to choose an alternative that does not rely on personal profiling.

Under the PIPL, personal data controllers and processors are subject to a range of significant obligations. These include obligations related to the transfer of personal data, which requires the consent of the data subject and must be conducted in accordance with security assessments, certifications, or standard contracts issued by the Cyberspace Administration of China (CAC), particularly for cross-border transfers involving important data or large volumes of data. Furthermore, data processing records must be maintained when required as part of a Personal Information Protection Impact Assessment (PIPIA), which should cover the purposes, methods, risks, and data protection measures associated with the processing. Data controllers are also obligated to conduct a PIPIA in specific circumstances, such as when processing sensitive personal data, engaging in automated decision-making, transferring data to third parties, or where the processing may have a significant impact on individuals' rights and interests.

Personal data controllers are required to appoint a Data Protection Officer (DPO) if the volume of data processed exceeds a certain threshold. However, this threshold has not yet been clearly defined. The DPO is responsible for coordinating data security, drafting privacy policies, managing records of personal information held, and handling complaints or breaches. Another key obligation is the requirement to notify of data breaches. In the event of a data leak or security incident, controllers must promptly take remedial action, notify affected individuals, and report the incident to the relevant regulators, unless the risks have been effectively mitigated. Furthermore, data retention must be limited to what is necessary to fulfill the processing purpose, with special treatment for sensitive data and children's data, which requires parental or guardian consent.

Suppose data controllers violate the provisions of the PIPL. In that case, they may be subject to legal sanctions, including orders to rectify violations, disgorgement of unlawful gains, administrative fines, and suspension or termination of applications that breach the law. The maximum fine for serious violations may reach RMB 50 million or 5% of the controller's annual revenue. Individuals directly responsible for severe violations may face personal fines of up to RMB 1 million and may be prohibited from holding key positions for a specified period. These sanctions are designed to serve as a deterrent, encouraging personal data controllers to exercise greater caution and ensure compliance with applicable data protection laws.

D. Hybrid Model for the Protection of Consumers' Personal Data in Indonesia's Digital MSMEs

Indonesia faces significant challenges in protecting the personal data of consumers in the digital MSME sector as economic digitalization continues to expand.[58] Despite the enactment of the PDP law, the implementation of data protection measures within the MSME sector, dominated by micro and small enterprises, remains highly complex, particularly due to resource constraints and low legal awareness. Therefore, Indonesia requires a Hybrid Model that combines a strict rule-based regulatory approach, similar to China's, with an education- and empowerment-based soft approach to develop a balanced, realistic, and practical data protection ecosystem for MSMEs.

China, through the PIPL, imposes high standards on personal data management, emphasizing clarity, explicit consent, and strict supervision. Indonesia can adopt a similar approach within its PDP law by ensuring the enactment of regulations that specifically address MSMEs' practices, particularly regarding minimum standards for data collection, processing, and storage. Just as PIPL introduces specific obligations based on business scale, Indonesia can establish a risk-based classification for MSMEs to prevent excessive regulatory burdens while still ensuring data security.

China's success in creating a protected MSMEs ecosystem is largely driven by strong synergy between the state and businesses, including

[58] Setiyo Utomo and Deny Slamet Pribadi, "Kebijakan Hukum Persaingan Usaha Terhadap Usaha Mikro, Kecil Dan Menengah Di Era Digital," *Zaaken: Journal of Civil and Business Law* 5, no. 2 (2024): 307–17.

incentives for MSMEs that comply with personal data standards. Indonesia must develop active inter-agency cooperation, involving the Ministry of Communication and Digital Affairs, the Ministry of MSMEs, and the National Cyber and Crypto Agency, to provide direct technical assistance for MSMEs in securely managing personal data. This support should include free audits, standardized privacy policy templates, and access to data protection technologies, ensuring a practical and sustainable data protection framework for MSMEs.

The Hybrid Model should incorporate decentralized supervision by empowering local governments to assist and monitor MSMEs within their respective regions. China enables sectoral regulators and local authorities to implement the PIPL and related laws. Similarly, Indonesia, through regional Communication and Information Agencies and Cooperative Offices, can adopt a preventive and corrective approach, ensuring that local MSMEs handling personal data comply with standards through capacity-building rather than purely repressive measures. Beyond regulatory enforcement, education and technological innovation must be integral components. In China, the government actively promotes cybersecurity literacy among MSMEs. Indonesia should also provide regular training programs on privacy and data security, alongside supporting the development of user-friendly data protection tools tailored for MSMEs, such as automated data encryption dashboards and privacy policy notification templates. These solutions offer a pragmatic alternative for MSMEs lacking dedicated IT teams.

Referring to the PIPL, accountability is a key principle. Indonesia must encourage the implementation of minimum obligations tailored for MSMEs, such as requiring a simplified Data Protection Impact Assessment (DPIA) for MSMEs that process sensitive data (e.g., fintech, marketplaces). Additionally, data protection certification for MSMEs should be introduced as both an educational tool and a compliance recognition mechanism to enhance consumer trust. China adopts a cross-sectoral approach, involving multiple regulators such as the CAC, MIIT, MPS, and NFRA. Indonesia should implement a multi-sectoral oversight model for digital MSMEs, with clear role distribution among: financial technology MSMEs, pharmaceutical and cosmetic MSMEs, the Ministry of Communication and Digital Affairs, and the Ministry of MSMEs. A standardized, integrated supervision framework will prevent regulatory overlaps and enhance the effectiveness of personal data protection oversight.

The Hybrid Model must incorporate the principle of proportional compliance. China classifies MSMEs based on business type, assets, and data risk potential. Similarly, Indonesia should establish a classification framework differentiating between data-sensitive and data-light MSMEs. For instance, MSMEs handling financial transactions or children's data should adhere to stricter data protection standards. Small-scale businesses, such as online food stalls, should only be required to follow basic data protection guidelines. Just as China provides fiscal incentives[59]Indonesia should integrate personal data protection incentives into MSME financing programs. For example, offering low-interest loans to MSMEs that obtain data protection certification would strongly encourage businesses to take consumer privacy seriously while accelerating the adoption of data security technologies.

China maintains a balance between repressive and educational approaches in data protection enforcement.[60] Indonesia should adopt a proportional enforcement strategy to ensure compliance with personal data protection laws. For MSMEs that fail to comply, warnings and mandatory assistance should be prioritized before imposing financial penalties, except in cases of serious violations such as large-scale data breaches. A system of progressive administrative sanctions can be applied, starting with official warnings and compliance assistance, followed by minor fines, and ultimately leading to business license revocation in cases of repeated and deliberate violations. This approach prevents overly punitive measures that could harm MSMEs while still ensuring strong consumer data protection compliance.

In terms of regulatory strengthening, the Hybrid Model implemented in Indonesia should focus on developing tiered regulations as part of the implementing framework under the PDP law. This regulatory approach must align data protection obligations with the capacity and risk levels of different MSME categories, ensuring that

[59] Pinghua Chen et al., "The Impact of Sudden Public Events and Fiscal Policy Relief on the Financing Constraints of Small and Medium Enterprises: A Quasi-Natural Experiment during COVID-19," *Venture Capital* 26, no. 1 (2024): 31–46.

[60] Oktarina Sarare et al., "National Arrangements Regarding Free Trade Between Indonesia And China," *Progressive Law Review* 6, no. 01 (2024): 86–96.

compliance requirements are proportionate and practical. The regulations should establish minimum technical standards applicable to all MSMEs, such as the mandatory implementation of a simple privacy policy and a basic data consent mechanism, while also introducing stricter standards for MSMEs that process sensitive data. Additionally, the regulatory framework must impose government obligations to provide proactive legal assistance and capacity-building programs for MSMEs. Local governments should be required to establish data protection support units within regional Communication and Information Office offices and Cooperative Agencies, ensuring that MSMEs receive adequate guidance and support. A multi-sectoral coordination framework must also be mandated, integrating standardized supervision procedures (SOPs) to ensure effective oversight while avoiding excessive regulatory burdens. Moreover, specific incentives should be introduced for MSMEs that comply with data protection standards, reinforcing a compliance-driven rather than purely punitive approach. By integrating legal enforcement with structured support mechanisms, the Hybrid Model would not only ensure compliance through sanctions but also provide MSMEs with the necessary tools and incentives to adopt data protection measures effectively and proportionally. This approach fosters a sustainable data protection culture, ensuring that MSMEs are both capable and willing to meet their legal obligations.

Conclusion

A hybrid model of personal data protection for MSMEs in Indonesia must combine the active role of the government in regulation with the utilization of AI-driven compliance technologies to ensure effective and efficient adherence to data protection obligations. Comparative studies with China demonstrate that a strict top-down approach can improve business compliance; however, a more adaptive model is necessary for Indonesian MSMEs, considering their limited resources and varying levels of digital literacy.

Therefore, the recommended personal data protection model consists of three main components: (1) Flexible yet binding regulations, accompanied by clear implementation guidelines tailored for MSMEs;

(2) Integration of automation-based technologies within data management systems to enhance security and compliance; and (3) Educational programs and incentives for MSMEs to encourage the implementation of data protection policies without hindering their business growth. Through this approach, consumer personal data protection in Indonesia can be strengthened more inclusively and sustainably, aligned with the development of the global digital economy.

References

Adhyputra, Muhammad Fadel, Thoriq Ahmadi, and Mohammad Rifqi. "Analisis Komparatif Rancangan Lppdp Indonesia Dengan Otoritas Pelindungan Data Singapura Dalam Penegakan Hukum Pelanggaran Data Pribadi: The Notion Of Personal Data Protection By Indonesia's LPPDP: A Comparative Study With The Singapore Personal Data Protection." *Jurnal Nomokrasi* 2, no. 2 (2024): 56–74.

Afdhali, Dino Rizka, and Taufiqurrohman Syahuri. "Idealitas Penegakkan Hukum Ditinjau Dari Perspektif Teori Tujuan Hukum." *Collegium Studiosum Journal* 6, no. 2 (2023): 555–61 DOI: https://doi.org/10.56301/csj.v6i2.1078.

Afriyanto, Renaldy, Ainur Gufron, Ahmad Syauqi Bawashir, and Rahmad Ready Kurniawan. "Eksistensi Asas Kepastian Hukum, Kemanfaatan Hukum Dan Keadilan Hukum Sebagai Tujuan Hukum Di Indonesia Dalam Perspektif Para Filsuf." *Unizar Law Review* 7, no. 2 (2024): 203–11 DOI: 10.36679/ulr.v7i2.80.

Al-Fatih, Sholahuddin. *Perkembangan Metode Penelitian Hukum Di Indonesia*. UMMPress, 2023.

AllahRakha, Naeem. "Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's World." *Lex Scientia Law Review* 8, no. 1 (2024): 405–32 DOI: https://doi.org/10.15294/lslr.v8i1.2081.

Amory, Jeffriansyah Dwi Sahputra, Muhtar Mudo, and J Rhena. "Transformasi Ekonomi Digital Dan Evolusi Pola Konsumsi: Tinjauan Literatur Tentang Perubahan Perilaku Belanja Di Era Internet." *Jurnal Minfo Polgan* 14, no. 1 (2025): 28–37 DOI: 10.33395/jmp.v14i1.14608.

Arbani, Muhammad. "Aspek Hukum Perlindungan Umkm Dalam Penjualan Di E-Commerce: Tantangan Dan Solusi Di Era Digital." *Jurnal Syntax Admiration* 6, no. 2 (2025): 1166–75 DOI: 10.46799/jsa.v6i2.2115.

Astuti, Endah Fuji, Achmad Nizar Hidayanto, Sabila Nurwardani, and Ailsa Zayyan Salsabila. "Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001: 2013." *International Journal of Safety & Security Engineering* 14, no. 5 (2024) DOI: 10.18280/ijsse.140523.

Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431–55 DOI: https://doi.org/10.14710/jphi.v6i3.%p.

Balafif, Sabri. "Penyesuaian Model Ketahanan Siber Umkm Di Indonesia Dengan Nist Cybersecurity Framework." *Jurnal Informatika: Jurnal Pengembangan IT (JPIT)* 8, no. 291 (2023) DOI: https://doi.org/10.30591/jpit.v8i3.5662.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33 DOI: https://doi.org/10.14710/gk.2020.7504.

Bouraffa, Tayssir, and Kai-Lung Hui. "Regulating Information and Network Security: Review and Challenges." *ACM Computing Surveys* 57, no. 5 (2025): 1–38 DOI: 10.1145/3711124.

Calzada, Igor. "Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL)." *Smart Cities* 5, no. 3 (2022): 1129–50 DOI: 10.3390/smartcities5030057.

Chen, Pinghua, Minye Rao, Syed Ali Raza, Xiaohui Zhan, and Xin Zhao. "The Impact of Sudden Public Events and Fiscal Policy Relief on the Financing Constraints of Small and Medium Enterprises: A Quasi-Natural Experiment during COVID-19." *Venture Capital* 26, no. 1 (2024): 31–46 DOI: 10.1080/13691066.2023.2178348.

Creemers, Rogier. "China's Emerging Data Protection Framework." *Journal of Cybersecurity* 8, no. 1 (2022): tyac011 DOI: 10.1093/cybsec/tyac011.

Cui, Juan, Jing Du, Ning Zhang, and Zhanming Liang. "National Patient Satisfaction Survey as a Predictor for Quality of Care and Quality Improvement–Experience and Practice." *Patient Preference and Adherence*, 2025, 193–206 DOI: 10.2147/PPA.S496684.

Das, Badhan Chandra, M Hadi Amini, and Yanzhao Wu. "Security and Privacy Challenges of Large Language Models: A Survey." *ACM Computing Surveys* 57, no. 6 (2025): 1–39 DOI: 10.1145/3712001.

Determann, Lothar, Zhenyu Jay Ruan, Tingting Gao, and Jonathan Tam. "China's Draft Personal Information Protection Law." *Journal of Data Protection & Privacy* 4, no. 3 (2021): 235–59.

Disemadi, Hari Sutra, Lu Sudirman, Junimart Girsang, and Arwa Meida Aninda. "Perlindungan Data Pribadi Di Era Digital: Mengapa Kita Perlu Peduli?" *Sang Sewagati Journal* 1, no. 2 (2023): 66–90 DOI: https://doi.org/10.37253/sasenal.v1i2.8579.

Harahap, Nita Maharani. "Resiko Kejahatan Teknologi Informasi Dan Komunikasi Cyber Crime Dan Analisi Inovasi Pencegahan Resiko Cyber Crime Di Indonesia." *Jurnal Teknologi Dan Manajemen Sistem Industri* 3, no. 1 (2024): 52–59 DOI: 10.56071/jtmsi.v3i1.483.

Harinath, Depavath, Madhu Bandi, Archana Patil, M R Murthy, and A V S Raju. "Enhanced Data Security and Privacy in IoT Devices Using Blockchain Technology and Quantum Cryptography." *Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793)* 34, no. 6 (2024) DOI: 20.14118.jsee.2024.V34I6.1706.

Huang, Daoli. *Research on the Rule of Law of China's Cybersecurity*. Springer, 2022.

Jasmine, Alifia, Benny Djaja, and Maman Sudirman. "Tanggung Jawab Notaris Dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 5, no. 1 (2024) DOI: 10.38035/jihhp.v5i1.3204.

Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, and Anil Kumar Sinha. "Digital Economy to Improve the Culture of Industry 4.0: A Study on Features, Implementation and Challenges." *Green Technologies and Sustainability*, 2024, 100083 DOI:

https://doi.org/10.1016/j.grets.2024.100083.

Jin, Yulu, and Yu Wang. "Balancing Smart City Development and Personal Data Protection: A Regulatory Framework." *International Review of Economics & Finance*, 2025, 104022 DOI: https://doi.org/10.1016/j.iref.2025.104022.

Junaidi, Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil. "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspectives of Progressive Legal Theory." *Journal of Law and Legal Reform* 5, no. 2 (2024) DOI: https://doi.org/10.15294/jllr.vol5i2.3437.

Katiandagho, Vicky, Diana Darmayanti Putong, and Isye Junita Melo. "Undang–Undang Perlindungan Data Pribadi Memperkuat Undang–Undang Perbankan Dalam Menjaga Rahasia Data Nasabah Dan Untuk Melindungi Data Pribadi Masyarakat Indonesia." *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 1 (2023): 106–14 DOI: 10.55809/tora.v9i1.212.

Kessler, Florian, Jost Blöchl, and Yahui Mao. "Data Collection, Use, and Security: Developments in China." In *Standardization Strategies in China and India: Industrial Policy and Geopolitics and Implications for Europe*, 231–62. Springer, 2025.

Khan, Sameer Ullah, Inam Ullah Shah, Khansa Shah, and Muhammad Jawed Iqbal. "The Role of China-Pakistan Relations in the Global Tech Competition, Especially in Areas like 5G, AI, and Cybersecurity." *Review of Education, Administration & Law* 8, no. 1 (2025): 73–85 DOI: 10.47067/real.v8i1.404.

King, Thomas C, Nikita Aggarwal, Mariarosaria Taddeo, and Luciano Floridi. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science and Engineering Ethics* 26 (2020): 89–120 DOI: 10.1007/s11948-018-00081-0.

Liang, Lin, and Yan Li. "How Does Government Support Promote Digital Economy Development in China? The Mediating Role of Regional Innovation Ecosystem Resilience." *Technological Forecasting and Social Change* 188 (2023): 122328 DOI: 10.1016/j.techfore.2023.122328.

Lin, Xi. "A Model of Big Data-Based Governance: China's National

Government Big Data Platform and an Analysis of Its Governance Competence." *Chinese Political Science Review*, 2025, 1–40 DOI: 10.1007/s41111-025-00279-1.

Luntungan, Benjamin Lemta, and Andhika Arthawijaya. "Legal Analysis of Law No. 27 of 2022 Concerning Personal Data Protection (Decision No. 597/Pid. Sus/2021/Pn. Jkt. Pst)." *Formosa Journal of Sustainable Research* 4, no. 3 (2025): 553–60 DOI: https://doi.org/10.55927/fjsr.v4i3.136.

Mardiana Parihin, Nela. "Urgensi Perlindungan Data Pribadi Dalam Perpektif Hak Asasi Manusia." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 5, no. 1 (2023): 16–23 DOI: https://doi.org/10.52005/rechten.v5i1.108.

Meng, Zhen, and Lu Wang. "Personal Data Trusts in China: A Balance between Data Sharing and Privacy Protection." *Trusts & Trustees* 31, no. 1 (2025): 15–23 DOI: 10.1093/tandt/ttae089.

Napitupulu, Christian, Itsqon Wafi Fauzan Nasution, William Girsang, and Lokot Muda Harahap. "Peranan Ekonomi Digital Dalam Pertumbuhan Ekonomi Di Indonesia." *Jurnal Penelitian Ilmiah Multidisipliner* 1, no. 03 (2025): 138–45.

Nento, Henro Prayitno, Melki T Tunggati, Irwan Polidu, Octaviani Suryaningsih Masaguni, Karlin Z Mamu, Sri Olawati Suaib, and Sri Wahyuni S Moha. "Peningkatan Literasi Hukum Dalam Pengelolaan Keuangan: Strategi Edukasi Bagi UMKM Modern Di Kecamatan Dungingi." *Abdimas Awang Long* 8, no. 1 (2025): 137–50 DOI: https://doi.org/10.56301/awal.v8i1.

Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi. "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity." *Computer Law & Security Review* 55 (2024): 106066 DOI: https://doi.org/10.1016/j.clsr.2024.106066.

Pardosi, ROAG, and Yuliana Primawardani. "Perlindungan Hak Pengguna Layanan Pinjaman Online Dalam Perspektif Hak Asasi Manusia (Protection of the Rights of Online Loan Customers from a Human Rights Perspective)." *Jurnal Ham* 11, no. 3 (2020): 353–67 DOI: 10.30641/ham.2020.11.353-368.

Pernot-Leplay, Emmanuel. "China's Approach to Data Privacy Law: A Third Way between the US and the EU?" *Penn St. JL & Int'l Aff.*

8 (2020): 49.

Pramita, Cindy, Sudarmiatin Sudarmiatin, and Ludi Wishnu Wardhana. "Consumer Satisfaction with Non-Halal Culinary MSMEs at PIK through a Chinese-Themed Atmosphere and Stakeholder Involvement." *Journal of Management and Social Sciences* 3, no. 1 (2025): 1–8 DOI: https://doi.org/10.59031/jmsc.v3i1.516.

Prayuti, Yuyut. "Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik e-Commerce Dan Perlindungan Data Konsumen Di Indonesia." *Jurnal Interpretasi Hukum* 5, no. 1 (2024): 903–13 DOI: https://doi.org/10.22225/juinhum.5.1.8482.903-913.

Putra, Purwanto. "Menyelamatkan Dan Potensi Penyelamatan Ekonomi Pasca Covid-19:: Adopsi Kebijakan Literasi Digital Untuk Sektor UMKM." *IKOMIK: Jurnal Ilmu Komunikasi Dan Informasi* 2, no. 1 (2022): 21–28 DOI: 10.33830/ikomik.v2i1.2430.

Rahman, Faiz. "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia." *Jurnal Legislasi Indonesia* 18, no. 1 (2021): 81–102 DOI: 10.54629/jli.v18i1.736.

Sahril, Iran, and Dhody A R Widjaja Atmadja. "Perlindungan Data Pribadi Konsumen, Dokumen Dan Tanda Tangan Elektronik Yang Dipergunakan Oleh Pihak Ketiga Dalam Transaksi E-Commerce." *CENDEKIA: Jurnal Penelitian Dan Pengkajian Ilmiah* 2, no. 2 (2025): 173–89 DOI: https://doi.org/10.62335/cendekia.v2i2.897.

Sarare, Oktarina, Rahmat Amin, Akhmad Saripudin, and Artha Dana Pangesti. "National Arrangements Regarding Free Trade Between Indonesia And China." *Progressive Law Review* 6, no. 01 (2024): 86–96 DOI: https://doi.org/10.36448/plr.v6i01.155.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lessons Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 95–109 DOI: 10.18196/iclr.2219.

Silviani, Ninne Zahara, Rina Shahriyani Shahrullah, Vanessa Riarta Atmaja, and Park Ji Hyun. "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South

Korea." *Jurnal Hukum Dan Peradilan* 12, no. 3 (2023): 517–46 DOI: https://doi.org/10.25216/jhp.12.3.2023.517-546.

Sinaga, Blassyus Bevry, and Raia Putri Noer Azzura. "Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan Di Era Society 5.0." *Padjadjaran Law Review* 12, no. 1 (2024): 71–82 DOI: 10.56895/plr.v12i1.1651.

Sudarwanto, Al Sentot, and Dona Budi Budi Kharisma. "Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong and Malaysia." *Journal of Financial Crime* 29, no. 4 (2022): 1443–57 DOI: 10.1108/JFC-09-2021-0193.

Suparto, Susilowati, Deviana Yuanitasari, Sonny Dewi Judiasih, and Yamudin Salaeh. "Consumer Protection of Girls from Cybercrime in a Gender Perspective." *Journal of Law and Legal Reform* 5, no. 4 (2024): 2045–70 DOI: https://doi.org/10.15294/jllr.v5i4.11899.

Suryanto, Dasep, and Slamet Riyanto. "Implementasi Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Dalam Industri Ritel Tinjauan Terhadap Kepatuhan Dan Dampaknya Pada Konsumen." *VERITAS* 10, no. 1 (2024): 121–35 DOI: https://doi.org/10.34005/veritas.v10i1.3711.

Syailendra, Moody Rizqy, and Inayah Fasawwa Putri. "Tinjauan Hukum Mengenai Perlindungan UMKM Serta Efektivitas Permendag No. 31 Tahun 2023 Terhadap Social Commerce Tiktok Shop." *INNOVATIVE: Journal of Social Science Research* 3, no. 6 (2023): 5087–5100.

Tampi, Jelvica Meiceline. "Tinjauan Yuridis Terhadap Pelanggaran Privasi Berdasarkan UU No 27 Tahun 2022 Tentang Perlindungan Data Pribadi (Studi Kasus Tokopedia)." *LEX ADMINISTRATUM* 13, no. 1 (2025).

Tan, David. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 8, no. 8 (2021): 2463–78 DOI : 10.31604/jips.v8i8.2021.2463-2478.

Utomo, Setiyo, and Deny Slamet Pribadi. "Kebijakan Hukum Persaingan Usaha Terhadap Usaha Mikro, Kecil Dan Menengah Di Era Digital." *Zaaken: Journal of Civil and Business Law* 5, no.

2 (2024): 307–17 DOI: https://doi.org/10.22437/zaaken.v5i2.33133.

Yanamala, Anil Kumar Yadav, Srikanth Suryadevara, and Venkata Dinesh Reddy Kalli. "Balancing Innovation and Privacy: The Intersection of Data Protection and Artificial Intelligence." *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence* 15, no. 1 (2024): 1–43.

Zainuddin, Muhammad, and Aisyah Dinda Karina. "Penggunaan Metode Yuridis Normatif Dalam Membuktikan Kebenaran Pada Penelitian Hukum." *Smart Law Journal* 2, no. 2 (2023): 114–23 https://journal.unkaha.com/index.php/slj/article/view/26/12.

This page is intentionally left blank

Acknowledgment

None.

Funding Information

None.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.