BRIDGING THE GAP: RECONCILING PRIVACY DATA PROTECTION WITH INDONESIAN COLLECTIVISM

Moch. Marsa Taufiqurrohman
Faculty of Law Universitas Padjadjaran
moch23009@mail.unpad.ac.id

Tarsisius Murwadji
Faculty of Law Universitas Padjadjaran
t.murwadji@unpad.ac.id

Helza Nova Lita
Faculty of Law Universitas Padjadjaran
helza.nova@unpad.ac.id

Abstract

This article analyzes the interplay between Indonesia's collectivist cultural values and the implementation of Law No. 27 of 2022 on Personal Data Protection (Law No. 27/2022). The Law faces significant challenges in a society where awareness of data privacy remains low. This article utilizes a socio-legal research methodology to explore the cultural factors influencing Indonesian societal attitudes and behaviors towards data privacy. The article begins by outlining the core regulatory framework of Law No. 27/2022, comparing its implementation within individualistic and collectivist contexts. It highlights the inherent tension between the Law's emphasis on individual data rights and Indonesia's deeply ingrained collectivist values, which prioritize communal harmony and open information sharing. This cultural tendency often overshadows concerns about potential security risks, hindering the Law's effective implementation. To bridge this gap, the article proposes a "hybrid" approach that integrates international data protection standards with culturally relevant strategies. This includes emphasizing the collective benefits of data protection, framing it as a shared responsibility to protect the community's well-being. Furthermore, the article stresses the

importance of public education campaigns tailored to resonate with Indonesian cultural values. By empowering individuals with knowledge and legal awareness, the article argues that Indonesia can foster a more balanced approach to data protection that respects both individual rights and collective harmony.

Keywords: Privacy Data, Socio-Legal, National Culture, Individualism, Collectivism.

Introduction

Digitalization has permeated all aspects of Indonesian society. While the rapid development of digital technologies facilitates interactions, transactions, and information sharing, it simultaneously presents challenges to digital security.[1] Public concern regarding the increasing prevalence of personal data breaches is significant, underscoring the urgent need for robust regulations to ensure the protection of personal data.[2]

A recent study on the Status of Digital Literacy in Indonesia, conducted by the Ministry of Communication and Informatics of the Republic of Indonesia and Katadata Insight Center (KIC), reveals a lack of awareness and capability among Indonesians regarding crucial personal data protection practices. The research indicates that a considerable portion of the population readily shares personal information on social media platforms, including home addresses, birth dates, and personal phone numbers. Notably, 61.3% of the 10,000 respondents included their personal phone numbers on their social media accounts, while over half (58.1%) displayed their birth dates. Furthermore, 18.2% disclosed family member names and their relationships/occupations. Alarmingly, 30.2% frequently shared their real-time location when uploading content, and an additional 16.8%

[1] Bart Custers et al., "A Comparison of Data Protection Legislation and Policies across the EU," *Computer Law & Security Review*, vol. 34, no. 2 (2018), p. 234.

[2] Sabine Trepte et al., "A Cross-Cultural Perspective on the Privacy Calculus," *Social Media Society,* vol. 3, no. 1 (2017), p.172.

did so occasionally. Additionally, 61.1% admitted to using the same password across multiple social media accounts.[3]

The study further highlights a deficiency in awareness and capability concerning other essential data protection practices. A significant 71.2% of respondents were unable to differentiate between legitimate emails and those containing spam, viruses, or malware, despite the known risk of malware distribution through spam, which can compromise device security and lead to data breaches. Moreover, a considerable proportion of respondents did not regularly utilize features designed to enhance data protection. Specifically, 62% did not habitually use applications or software to detect and remove viruses from their mobile phones or computers, 58.6% were unfamiliar with reporting abuse or misuse on social networks, and 57.1% lacked the ability to independently back up their data across multiple storage locations. [4]

The aforementioned data highlighting the low awareness of personal data protection among Indonesians prompts further investigation into the potential correlation between Indonesia's collectivist culture and this lack of awareness. There is a strong presumption that Indonesia's collectivist culture, characterized by values of togetherness and mutual cooperation ("*gotong royong*"), may influence perceptions of personal data privacy.[5]

This hypothesis aligns with the findings of Sophie Cockroft and Saphira A.C. in their paper "The Relationship between Culture and Information Privacy Policy," which elucidates the complex interplay between culture, privacy concerns, and regulation.[6] This assumption is further corroborated by Nessrine Omrani and Nicolas Soulié's research, "Culture, Privacy Conception and Privacy Concern:

---

[3] Kementerian Informasi dan Komunikasi Republik Indonesia dan Katadata Insight Center, *Status Literasi Digital di Indonesia 2022*, (Jakarta: Katadata Insight Center, 2022), p. 52.

[4] Kementerian Informasi dan Komunikasi Republik Indonesia dan Katadata Insight Center, *Status Literasi Digital di Indonesia 2022*, (Jakarta: Katadata Insight Center, 2022), p. 52.

[5] Alex B. Makulilo, "A Person Is a Person through Other Persons'-A Critical Analysis of Privacy and Culture in Africa," *Beijing L. Rev.* vol. 1, no. 7 (2016), p. 192.

[6] Sophie Cockcroft, "Culture, Law and Information Privacy," in *Proceedings of European and Mediterranean Conference on Information Systems, Polytechnic University of Valencia, Spain*, 2007, p. 18.

Evidence from Europe before PRISM," which demonstrates that hierarchical and competitive societies prioritize privacy, while those characterized by egalitarianism, cooperation, and openness to change exhibit lower levels of privacy concern.[7]

This article aims to analyze how Indonesian cultural values influence societal attitudes towards personal data privacy. The research employs a socio-legal methodology, comparing the implementation of data privacy regulations in countries with individualistic and collectivist cultures. A legal approach identifies existing legislation on personal data protection, while a sociological approach analyzes the influence of Indonesian collectivism on the implementation of Law No. 27 of 2022 on Personal Data Protection (hereinafter referred to as Law No. 27/2022). Through this methodology, this article seeks to answer two primary questions: First, how does Indonesian collectivist culture influence the implementation of personal data protection regulations? Second, how should personal data protection regulations be implemented in countries with collectivist cultures?

The Interplay of Culture and Law: How Collectivism Shapes Data Protection Practices in Indonesia

The Influence of National Culture on Personal Data Regulation Enforcement

Concerns about information privacy are not universal but are instead shaped by a confluence of factors, including demographic variations, privacy attitudes, cultural dimensions, and contextual/situational influences. As a system, Law can be evaluated from two distinct perspectives. Firstly, Law can be viewed as a system of values.[8] In this regard, the entire legal enforcement framework is grounded in a *grundnorm*, which serves as the wellspring of values. Law, therefore, acts as both a repository of values and a guiding principle

[7] *Nessrine Omrani and Nicolas Soulié, "Culture, Privacy Conception and Privacy Concern: Evidence from Europe before PRISM," 14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS), p. "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan,* 2017, p. 11.

[8] Christine ST Kansil, *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia* (Jakarta: Balai Pustaka, 1992), p. 13.

for its own enforcement. Secondly, Law exists as an integral part of society (social reality).[9] In this context, Law is inextricably intertwined with the social fabric, functioning as a subsystem within a broader network of interconnected social subsystems.[10]

Regulatory intervention aims to address individual concerns regarding the protection of personal data. However, achieving a universally ideal and unified regulatory framework for data privacy protection appears improbable. This challenge arises, in part, from the diversity of cultures and the varying perspectives on privacy they engender. Citizens' responses to data privacy protection are influenced by their respective national cultures, as suggested by Hofstede's cultural dimensions theory (initially developed during the 1960s and 1970s at IBM. Geert Hofstede's framework for cross-cultural communication posits that societal culture shapes the values of its members, subsequently impacting their behaviors.[11]

Among Hofstede's cultural dimensions, Individualism versus Collectivism holds particular relevance to data privacy. This dimension pertains to the degree of integration individuals experience within their primary groups. Individualism is characterized by a preference for loosely knit social frameworks, where individuals are expected to prioritize their own well-being and that of their immediate families. Conversely, collectivist cultures emphasize the needs and goals of the group over individual desires.[12] Cultural values and norms significantly influence how online privacy is perceived and negotiated. Therefore, understanding the interplay between cultural dimensions, particularly Individualism versus Collectivism, and data privacy perceptions is crucial for developing culturally sensitive and effective data protection regulations.[13]

---

[9] Yesmil Anwar, *Pengantar Sosiologi Hukum* (Jakarta: Grasindo, 2008), p. 19.

[10] Soerjono Soekanto, *Pokok-pokok sosiologi hukum* (Depok: Rajawali Pers, 1989), p. 12.

[11] Yao Li et al., "Cross-Cultural Privacy Prediction," *Proceedings on Privacy Enhancing Technologies*, vol. 2, no. 1 (2017), p. 113.

[12] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty," *Yale LJ* vol.113 no. 1 (2003), p. 1151.

[13] Moch Marsa Taufiqurrohman and Elisatris Gultom, "Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan Teknologi Digital dalam Bisnis Perusahaan" vol. 13, no. 2 (2003), p. 11.

Global cultural patterns can be broadly categorized into Individualistic cultures (predominantly found in Europe and North America) and Collectivist cultures (prevalent in Asia, Africa, South America, and the Pacific Rim).[14] Distinct cultural values result in divergent approaches to privacy. Individuals from individualistic cultures tend to place a higher premium on personal data protection, valuing personal autonomy and independence. Conversely, collectivist societies demonstrate greater acceptance of group and organizational intrusion into individual privacy.[15]

While these findings suggest that nations with higher individualism scores may favor less government intervention and adopt more individual-centric approaches to data privacy regulation, this does not necessarily equate to a weaker stance on data protection. Individualists, by nature, often hold strong convictions regarding privacy rights. Despite preferring limited government involvement, individuals from individualistic cultures may exhibit greater concern for the safeguarding of their personal information compared to their counterparts from collectivist backgrounds.[16]

The GLOBE study's variable of in-group collectivism, which measures the extent to which individuals prioritize group affiliation, loyalty, and cohesion within their organizations or families, provides further nuance. This emphasis on group interconnectedness within collectivist cultures can influence perceptions of data privacy, potentially leading to a greater willingness to share personal information within trusted in-groups while maintaining stricter boundaries with out-groups.[17]

The preceding arguments suggest that societies characterized by lower levels of individualism may necessitate more robust data protection regulations. High individualism scores signify loosely-knit societal ties and an expectation of self-reliance. In contrast, collectivist societies often provide individuals with enduring, cohesive group

---

[14] Geert Hofstede, "Dimensionalizing Cultures: The Hofstede Model in Context," *Online Readings in Psychology and Culture* vol. 2, no. 1 (2011), p. 8.

[15] Lior Jacob Strahilevitz, "Toward a Positive Theory of Privacy Law," *Harv. L. Rev.* vol 126, no.1 (2012), p. 201.

[16] Eden Osucha, "The Whiteness of Privacy: Race, Media, Law," *Camera Obscura: Feminism, Culture, and Media Studies,* vol. 24, no. 1 (2009), p. 67.

[17] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty," *Yale LJ* vol.113 no. 1 (2003), p. 1151.

affiliations throughout their lives, offering support and security in exchange for unwavering loyalty.[18]

However, the interplay between individualism and data protection preferences is not without complexities. On the one hand, the strong social connections inherent in collectivist cultures can serve as a "cushion" or safety net for individuals facing adversity. This sense of collective security might, in turn, lead to a diminished emphasis on formal data protection mechanisms.[19]

Conversely, Bellman proposes an alternative theory, suggesting that such societies may exhibit less concern for personal data protection and demonstrate reduced motivation to seek government intervention in this domain. They posit that societies with low individualism and high collectivism tend to accept a greater degree of intrusion into individual privacy by groups, including the government.[20] This "intrusion theory" finds support in the work of Milberg, who observed similar patterns of acceptance towards group intrusion in collectivist contexts. Therefore, while a strong correlation exists between cultural values and data protection preferences, further research is needed to fully disentangle the complex interplay between individualism, collectivism, perceived social support, and attitudes towards government intervention in the realm of data privacy.

Awareness of data privacy is intrinsically linked to the effectiveness of data protection measures. Concerns regarding information privacy are not universal but are instead shaped by a confluence of factors, including demographic variations, privacy attitudes, cultural dimensions, and contextual/situational influences.[21] Consequently, the implementation of data privacy regulations designed to safeguard privacy rights is significantly influenced by a nation's cultural fabric. As posited by Hofstede's cultural dimensions theory,

---

[18] Samantha Barbas, "The Sidis Case and the Origins of Modern Privacy Law," *Colum. JL & Arts*, vol. 36, no. 1 (2012), p. 21.

[19] Uta Kohl, "The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy," *International & Comparative Law Quarterly*, vol. 72, no. 3 (2023), p. 737.

[20] Sophie Cockcroft and Saphira Rekker, "The Relationship between Culture and Information Privacy Policy," *Electronic Markets,* vol. 26, no. 1 (2016), p. 55.

[21] Moch Marsa Taufiqurrohman and Elisatris Gultom, "Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan Teknologi Digital dalam Bisnis Perusahaan," *Humani (Hukum dan Masyarakat Madani)*, vol. 13, no. 2 (2023), p. 311.

citizens' responses to data privacy are shaped by their respective national cultures.[22] Geert Hofstede's theory of cross-cultural communication highlights the profound influence of societal culture on the values of its members and how these values, in turn, shape their behaviors.

Privacy criteria certainly differ between nations and countries, shaped fundamentally by their unique philosophical foundations and constitutional frameworks. In Indonesia, collectivism is not merely a cultural tendency observable in daily social interactions, but is deeply rooted in the nation's foundational philosophy—Pancasila—and enshrined in the 1945 Constitution of the Republic of Indonesia. Understanding Indonesian collectivism requires examining its philosophical underpinnings, particularly through the lens of what Notonagoro termed the *causa materialis* of Pancasila, which refers to the material or substantive foundation from which Indonesia's state philosophy emerged.

According to Notonagoro's philosophical framework, Pancasila serves as the *causa materialis* of Indonesian law, meaning that the Indonesian people themselves, along with their culture, traditions, and religious values, constitute the material foundation from which Pancasila was formulated.[23] This concept is crucial for understanding how Indonesian collectivism manifests in legal frameworks, including contemporary data protection regulations. Notonagoro argues that the *causa materialis* of Pancasila originates from three primary sources: first, the customs and traditions (*adat-istiadat*) of Indonesian society, which encompass social, economic, and political structures; second, the diverse cultures (*kebudayaan*) that have developed across the archipelago over centuries; and third, the religious values (*agama-agama*) that permeate Indonesian society and acknowledge the unity of God.[24] These three elements are not separate but interwoven, forming the substantive basis upon which Pancasila was constructed and continues to guide Indonesian legal development.

---

[22] Geert Hofstede, "Dimensionalizing Cultures: The Hofstede Model in Context," *Online Readings in Psychology and Culture* vol. 2, no. 1 (2011), p. 8.
[23] Miska Amien, "Causa Materialis Pancasila Menurut Notonagoro," *Jurnal Filsafat* 16, no. 1 (2006): 18–26.
[24] Sukamto Notonagoro, *Pancasila Secara Ilmiah Populer* (Pantjuran Tudjuh, 1975).

The customs and traditions that form part of Pancasila's *causa materialis* are characterized by values of *gotong royong* (mutual cooperation), communal decision-making through *musyawarah mufakat* (deliberation to reach consensus), and collective responsibility for community welfare. These values, developed through centuries of agrarian society and village-based governance systems, prioritize group harmony and collective interests over individual autonomy. The cultural dimension reflects Indonesia's extraordinary diversity, with hundreds of ethnic groups sharing common values despite linguistic and regional differences. This cultural plurality is unified by shared principles of respect for elders, communal land ownership traditions, and collective resource management. The religious foundation acknowledges that Indonesian society's moral and ethical framework is inseparable from religious values, as reflected in the first principle of Pancasila—*Ketuhanan Yang Maha Esa* (Belief in the One Supreme God)—which emphasizes community welfare, social responsibility, and collective moral obligations rooted in religious teachings.

The relationship between law and cultural values, as articulated by Notonagoro and further developed by Sudjito, can be understood through the concept of *causa materialis*. Law must represent the cultural values characteristic of the nation, serving as both a reflection and reinforcement of those values.[25] Sudjito's work on the Pancasila legal system elaborates how each of the five principles (*sila*) embodies collectivist values that influence legal interpretation and implementation. The first principle, *Ketuhanan Yang Maha Esa*, establishes that individual rights, including privacy, are not absolute but must be exercised within the framework of religious and moral responsibility to the community. The second principle, *Kemanusiaan yang Adil dan Beradab* (Just and Civilized Humanity), emphasizes human dignity within a social context, where individual rights are balanced with obligations to respect and protect the dignity of others in the community. The third principle, *Persatuan Indonesia* (Unity of Indonesia), prioritizes national unity and social cohesion, which can sometimes require individuals to subordinate personal interests for the collective good. The fourth principle, *Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan Perwakilan* (Democracy

[25] Pembukaan Undang-Undang Dasar Notonagoro, "Dalam Pancasila Dasar Falsafah Negara," *Cetakan Ketujuh, Jakarta: Bina Aksara*, 1988.

Led by Wisdom through Deliberation/Representation), emphasizes collective decision-making and consensus-building, reflecting a preference for communal rather than individualistic approaches to governance. The fifth principle, *Keadilan Sosial bagi Seluruh Rakyat Indonesia* (Social Justice for All Indonesian People), explicitly prioritizes collective welfare and equitable distribution of resources, reinforcing the notion that individual rights must serve broader social justice goals.[26]

Based on the Pancasila philosophy and constitutional framework, Indonesian collectivism can be characterized by several distinct criteria that differentiate it from collectivism in other cultural contexts. First, there is a primacy of communal harmony, where individual actions, including data sharing practices, are evaluated based on their contribution to social cohesion and communal well-being rather than solely on individual benefit or harm. Second, privacy is understood not as an absolute individual right but as a relational concept that must be balanced with obligations to family, community, and state, reflecting what might be termed a "relational privacy" framework. Third, within trusted social circles (*in-groups*), open information sharing is valued as a sign of social solidarity and mutual trust, creating cultural expectations that may conflict with strict data protection principles. Fourth, data protection is viewed as a shared responsibility rather than solely an individual concern, aligning with the *gotong royong* principle that emphasizes collective action for common benefit. Fifth, there is an acceptance of hierarchical respect, where sharing information with legitimate authorities and institutions is seen as appropriate, reflecting the hierarchical nature of Indonesian social structures rooted in traditional governance systems.

Article 33 of the 1945 Constitution exemplifies this collectivist orientation, stating that the earth, water, and natural resources contained therein shall be controlled by the State and utilized for the greatest welfare of the people, and those branches of production which are important for the State and which affect the life of most people shall be controlled by the State. This constitutional provision reflects the broader principle that resources—including, by extension, data—that impact collective welfare should be subject to communal

[26] R. Karlina Lubis, "Pancasila: Paradigma Ilmu Hukum Indonesia," *Conference: Kongres Pancasila VI, Ambon*, 2014.

considerations and state oversight rather than purely individual control. This philosophical and constitutional foundation creates a unique context for implementing Law No. 27/2022 on Personal Data Protection. The law must navigate the inherent tension between international data protection standards, which are predominantly based on individualistic conceptions of privacy rights emphasizing personal autonomy and control, and Indonesia's deeply embedded collectivist values rooted in Pancasila that prioritize communal harmony and collective welfare. Understanding this *causa materialis* is essential for developing culturally appropriate implementation strategies that respect both individual data rights as recognized in international human rights frameworks and collective cultural values that form the foundation of Indonesian society and the legal system.

Practical Implications: Data Protection Implementation within Indonesia's Collectivist Framework

Indonesian society is characterized by strong collectivist values, where group interests often supersede individual ones. This cultural orientation permeates various facets of life, including the implementation of legal frameworks. Collectivism in Indonesia manifests in a deep-rooted emphasis on togetherness, *gotong royong*, and a propensity for sharing.[27] This focus on collective well-being and sharing can, however, lead to a diminished emphasis on individual privacy concerns, potentially resulting in less stringent codification of data protection elements within Indonesian Law. One plausible explanation for this apparent anomaly is that the right to privacy, as understood in individualistic societies, may not hold the same fundamental status within a collectivist cultural context.[28] Therefore, Indonesia's collectivist cultural orientation significantly influences

[27] Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), p. 171.

[28] Munir Fuady, Teori-Teori dalam Sosiologi Hukum (Jakarta: Kencana, 2015), p. 23.

perspectives on data privacy, shaping the attitudes of both the general populace and regulatory bodies.[29]

Indonesia's deeply ingrained communal culture significantly shapes perspectives on data privacy, influencing the attitudes of both the general populace and regulatory authorities. Justus M. van der Kroef, in his seminal article "Collectivism in Indonesian Society," posits that Indonesia exhibits a fundamentally collectivist ethos. This assertion finds implicit support in Article 33 of the 1945 Constitution of the Republic of Indonesia, which stipulates, in essence, that Water, land, and natural resources should be managed through a spirit of *gotong royong*. Economic sectors impacting the welfare of the majority should be collectively owned and regulated. Branches of the economy affecting the lives of most citizens should be subject to communal ownership. This constitutional emphasis on collective ownership and cooperative management underscores the deeply rooted collectivist values that permeate Indonesian society, potentially influencing perceptions of data privacy and shaping regulatory approaches to data protection.[30] This cultural predisposition towards collectivism helps explain the observed tendencies, reflecting the affinity of Indonesian leaders for traditional patterns of collective organization and decision-making.

This cultural proclivity is further corroborated by observing the predilection of Indonesian leaders for traditional communal patterns, particularly those reminiscent of the cooperative social structures found in agrarian societies. This collective tendency emerged as a response to colonial capitalism and the prevailing social order of the time. As Made Suwitra argues, Indonesia's communal culture stems from the noble values embedded in the nation's foundational philosophy, characterized as religio-communal.[31] This philosophy prioritizes the interests of the community over individual concerns, shaping the relationship between individuals and society at large.

---

[29] Moch Marsa Taufiqurrohman, "Adopting Osman Warning in Indonesia: An Effort to Protect Potential Victims of Crime Target," *Jurnal Hukum Dan Peradilan* vol. 11, no. 3 (2022), p. 22.

[30] Justus M. Van Der Kroef, "Collectivism in Indonesian society," *Social Research* vol. 52, no.1 (1953), p. 193.

[31] Hiroshi Miyashita, "The Evolving Concept of Data Privacy in Japanese Law," *International Data Privacy Law* vol. 1, no. 4 (2011), p. 229.

Jurnal Hukum dan Peradilan Vol. 14, no. 3 (2025), pp. 549-598
ISSN: 2303-3274 (p), 2528-1100 (e)
DOI: https://doi.org/10.25216/jhp.14.3.2025. *549-598*

Empirical evidence from recent years further reinforces Indonesia's classification as a collectivist society while revealing critical gaps in data protection awareness. To substantiate this assertion and assess current data protection awareness, this article analyzes recent empirical data from multiple authoritative sources, employing a socio-legal methodology that examines both cultural orientation indicators and digital literacy metrics related to data protection. This comparative analysis provides a contemporary understanding of how Indonesian collectivism intersects with data privacy awareness in the digital age.

Indonesia's position as a collectivist society is confirmed by its consistently low score on Hofstede's Individualism dimension. According to Hofstede Insights, Indonesia scores 14 on the Individualism index (on a scale of 0-100, where higher scores indicate greater individualism), placing it among the most collectivist societies globally.[32] This score has remained stable over decades, indicating that collectivist values are deeply entrenched and resistant to change despite rapid digitalization and increased exposure to global cultural influences. This cultural stability has significant implications for data protection implementation, as it suggests that behavioral change cannot rely solely on legal mandates but must engage with existing cultural frameworks that prioritize collective over individual interests.

Table 1. Indonesia's Digital Literacy and Data Protection Indicators (2021-2022 & 2024)

Indicator	2021	2022	2024	Source
Digital Literacy Index (National, scale 1-5)	3.49	3.54	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center
Digital Safety Sub-Index (scale 1-5)	3.10	3.49	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center
Digital Culture Sub-Index (scale 1-5)	3.90	N/A	N/A	Kementerian Komunikasi dan

[32] Geert Hofstede et al., *Cultures et Organisations: Nos Programmations Mentales* (Pearson Education France, 2010).

				Informatika & Katadata Insight Center
Digital Skills and Literacy Score (scale 0-100)	N/A	N/A	58.25	Tech for Good Institute
Two-Factor Authentication Usage (%)	N/A	N/A	36.4%	Tech for Good Institute
Refrain from Uploading Sensitive Data (%)	N/A	N/A	64.8%	Tech for Good Institute
Personal Phone Number on Social Media (%)	N/A	61.3%	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center
Birth Date Displayed on Social Media (%)	N/A	58.1%	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center
Password Reuse Across Platforms (%)	N/A	61.1%	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center
Unable to Identify Spam/Malware (%)	N/A	71.2%	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center
Frequently Share Real-Time Location (%)	N/A	30.2%	N/A	Kementerian Komunikasi dan Informatika & Katadata Insight Center

Sources: Kementerian Komunikasi dan Informatika Republik Indonesia and Katadata Insight Center, Status Literasi Digital di Indonesia 2021-2022 and Tech for Good Institute 2024.

Regarding digital literacy and data protection awareness, the Indonesian Ministry of Communication and Informatics (Kominfo), in collaboration with Katadata Insight Center, has conducted annual surveys measuring the Digital Literacy Index. The 2021 survey established a baseline score of 3.49 (on a scale of 1-5, where higher scores indicate greater digital literacy), categorized as "moderate"

level.[33] The 2022 survey showed modest improvement to 3.54, indicating gradual progress in digital competency across the Indonesian population.[34] These measurements utilize four pillars: Digital Skills (*Kecakapan Digital*), Digital Ethics (*Etika Digital*), Digital Safety (*Keamanan Digital*), and Digital Culture (*Budaya Digital*), based on the framework outlined in the 2020-2024 Digital Literacy Roadmap developed by the Ministry of Communication and Informatics.

Significantly, across both measurement years, the Digital Safety pillar—which specifically measures data protection awareness, understanding of cyber security threats, and practices for safeguarding personal information—consistently performs as the lowest-scoring pillar. In 2021, Digital Safety scored 3.10, the lowest among all four pillars, while Digital Culture scored highest at 3.90.[35] In 2022, Digital Safety improved slightly to 3.49 but remained the weakest area.[36] This persistent gap suggests that while Indonesians are becoming more digitally capable in terms of technical skills and are developing digital cultural practices, awareness of data security and privacy protection lags significantly behind other digital competencies. More recent data from 2024 indicates continued challenges, with a study by the Tech for Good Institute reporting that Indonesia's digital skills and literacy score stood at 58.25 out of 100, with only 36.4 percent of Indonesian respondents using two-factor authentication, a basic security measure for protecting online accounts, and only 64.8 percent refraining from uploading sensitive personal data on social media platforms.[37]

The 2022 Digital Literacy survey data reveal alarming patterns of data sharing behavior that reflect collectivist cultural norms intersecting with insufficient awareness of data protection risks. The survey found that 61.3 percent of the 10,000 respondents included their personal phone numbers on their social media accounts, while 58.1 percent displayed their birth dates publicly, and 18.2 percent

[33] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI," accessed November 4, 2025, https://data.komdigi.go.id/opendata/dataset/indeks-literasi-digital-indonesia.
[34] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI."
[35] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI."
[36] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI."
[37] "Strengthening Indonesia's Personal Data Protection Framework," *Tech For Good Institute*, March 21, 2025, https://techforgoodinstitute.org/blog/country-spotlights/strengthening-indonesias-personal-data-protection-framework/.

disclosed family member names along with their relationships and occupations.[38] Furthermore, 30.2 percent of respondents frequently shared their real-time location when uploading content, with an additional 16.8 percent doing so occasionally, creating significant risks for physical security and stalking. In terms of password security practices, 61.1 percent admitted to using the same password across multiple social media accounts, a practice that dramatically increases vulnerability to credential stuffing attacks and account compromise.[39] Additionally, 71.2 percent of respondents were unable to differentiate between legitimate emails and those containing spam, viruses, or malware, despite the well-documented risk of malware distribution through phishing emails that can compromise device security and lead to data breaches.[40] These behaviors can be interpreted through a socio-legal lens as manifestations of collectivist values: the willingness to share personal information reflects cultural norms of openness and trust within perceived *in-groups* (social media networks), while the lack of security consciousness reflects insufficient awareness of digital threats and limited understanding of data protection as an individual responsibility.

To contextualize Indonesia's situation within the broader Asian region, a comparative analysis of collectivism and data protection frameworks across selected Asian countries provides valuable insights. Japan, with an Individualism score of 46 on Hofstede's index, enacted its Act on the Protection of Personal Information (APPI) in 2003, with substantial amendments in 2017 and 2020 to strengthen data protection provisions.[41] Despite being more individualistic than Indonesia, Japan demonstrates moderate public awareness of data protection, influenced by its collectivist emphasis on group harmony (*wa*) and historical rice farming culture that necessitated collective decision-making. Singapore, scoring 20 on the Individualism index, enacted its Personal Data Protection Act (PDPA) in 2012 and has achieved high public awareness through comprehensive government-led digital literacy programs and strict enforcement

[38] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI."
[39] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI."
[40] "Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI."
[41] "Data Protection Laws of the World," accessed November 4, 2025, https://www.dlapiperdataprotection.com/.

mechanisms.[42] Malaysia, with an Individualism score of 26, enacted its Personal Data Protection Act in 2010, demonstrating moderate awareness levels influenced by Islamic values emphasizing community welfare and a multi-ethnic society requiring careful balancing of group interests.[43] South Korea, scoring 18 on the Individualism index, enacted its Personal Information Protection Act (PIPA) in 2011 and has achieved high public awareness through rapid digital adoption, high technological literacy, and strong government investment in cybersecurity education.[44]

This comparative analysis reveals a crucial insight: while all these Asian countries exhibit collectivist cultural orientations (Individualism scores below 50), their data protection awareness levels vary significantly. Singapore and South Korea, despite low Individualism scores comparable to or lower than Indonesia's, demonstrate high public awareness of data protection. This suggests that collectivism itself is not an insurmountable barrier to effective data protection; rather, the key differentiating factors include the length of time since law enactment (countries with longer-standing frameworks show higher awareness through sustained education efforts), government investment in digital literacy and cyber security education programs, integration of data protection into national digital transformation strategies, and cultural adaptation of data protection messaging to resonate with local values rather than simply transplanting Western individualistic frameworks.

Table 2. Comparative Analysis of Collectivism and Data Protection Frameworks in Selected Asian Countries

Country	Hofstede Individualism Score	Data Protection Law	Public Awareness Level	Key Cultural Characteristics

[42] "Personal Data Protection Commission Singapore | PDPC," accessed November 4, 2025, https://www.pdpc.gov.sg/.
[43] *Jabatan Perlindungan Data Peribadi (PDP), Malaysia*, July 4, 2024, https://www.pdp.gov.my/ppdpv1/.
[44] "Data Protection Laws of the World."

Indonesia	14	Law No. 27/2022 on Personal Data Protection	Low-Moderate	Strong collectivism rooted in Pancasila; *gotong royong* culture; relational privacy concept
Japan	46	Act on Protection of Personal Information (APPI)	Moderate	Collectivism based on group harmony (wa); historical rice farming culture; indirect communication patterns
Singapore	20	Personal Data Protection Act (PDPA)	High	Collectivism with strong state governance; high digital literacy; comprehensive education programs
Malaysia	26	Personal Data Protection Act (PDPA)	Moderate	Collectivism influenced by Islamic values; multi-ethnic society; communal welfare emphasis
South Korea	18	Personal Information Protection Act (PIPA)	High	Collectivism with rapid digital adoption; high technological literacy; strong cyber security culture
Indonesia	14	Law No. 27/2022	Low-Moderate	Strong collectivism

	on Personal Data Protection	rooted in Pancasila; *gotong royong* culture; relational privacy concept

Sources: Hofstede, Geert, Gert Jan Hofstede, and Michael Minkov. Cultures and Organizations: Software of the Mind. 3rd ed. New York: McGraw-Hill, 2010 and DLA Piper: Data Protection Laws of the World 2025.

The data reveals what can be termed an "awareness gap"—the disconnect between legal frameworks such as Law No. 27/2022 and public understanding and behavior regarding data protection. This gap is particularly pronounced in Indonesia due to several factors: the recent enactment of Law No. 27/2022 in October 2022, with full implementation required by October 2024, means that public education efforts are still in early stages; cultural dissonance exists between the law's emphasis on individual consent and control, derived from European GDPR principles, and collectivist norms of communal information sharing and trust-based data exchange; and limited public education campaigns have not yet achieved sufficient scale or cultural resonance, as evidenced by the modest improvement in Digital Safety scores between 2021 and 2022 and persistent risky behaviors. The distinction between sensitive and non-sensitive data remains poorly understood among the Indonesian public, as evidenced by the high rates of personal information sharing on social media platforms. This lack of awareness is particularly concerning given that data categorization in Indonesia is determined by the country's specific socio-cultural context, including considerations of race, ethnicity, religion, and other identifiers that carry particular significance in Indonesia's diverse society and have historically been sources of social tension.

This socio-legal analysis of recent empirical data demonstrates that Indonesia faces a dual challenge: maintaining its collectivist cultural identity rooted in Pancasila while implementing data protection standards that originated in individualistic legal traditions emphasizing personal autonomy. The data suggests that successful implementation of Law No. 27/2022 requires a multi-faceted approach: first, recognizing that awareness building is a multi-year

process, as comparative data from Singapore and South Korea shows that countries with decade-old data protection frameworks demonstrate higher awareness; second, developing culturally adapted education programs that resonate with Pancasila values and collectivist norms rather than generic data protection education based on Western individualistic assumptions; and third, leveraging collectivism as an asset by framing data protection as a collective responsibility (*gotong royong* for digital safety) that protects community welfare rather than solely as an individual right that may seem foreign or selfish in a collectivist context.

Indonesia's collectivist culture, while rooted in noble values of community and shared responsibility, can pose challenges to data privacy protection. [45] The tendency towards open information sharing within trusted circles, while fostering strong social bonds, may inadvertently increase the risk of data breaches and misuse. [46] Law No. 27/2022, enacted in October 2022, designates personal data protection as a fundamental human right. This Law mandates that all personal data processing must align with the legitimate interests of the data collector and prohibits misuse for any other purpose. Law No. 27/2022 is intended to raise public awareness regarding the importance of data privacy, safeguard individuals from data breaches and misuse, and mitigate cybersecurity risks. Therefore, it is imperative to enhance public understanding of privacy provisions and empower individuals with practical strategies to minimize their risk of personal data breaches.[47]

Fundamentally, Law No. 27/2022 stipulates that the processing of personal data by a Data Controller, including processing by a Data Processor on behalf of the Controller, is permissible only with the explicit consent of the Data Subject. Furthermore, Law No. 27/2022 mandates that Data Controllers must establish a legitimate basis for all

---

[45] Alexandre Veronese et al., *The Concept of Personal Data Protection Culture from European Union Documents: A "Brussels Effect" in Latin America?*, Universidade do Minho. Escola de Direito (ED), 2023, http://repositorium.uminho.pt/handle/1822/88911.

[46] Sandra Seubert and Carlos Becker, "The Culture Industry Revisited: Sociophilosophical Reflections on 'Privacy' in the Digital Age," *Philosophy & Social Criticism* vol. 45, no. 8 (2019), p. 930.

[47] Sinta Dewi Rosadi, *Pembahasan UU Perlindungan Data Pribadi (UU RI No. 27 Tahun 2022)*, (Jakarta: Sinar Grafika, 2023), p. 24.

personal data processing activities.[48] Regarding the processing of personal data based on recorded consent from the data subject,[49] the Data Controller is obligated to provide clear and comprehensive information regarding: Legality of Processing The legal basis for processing the personal data; Purpose of Processing: The specific, legitimate purpose(s) for which the data is being processed; Data Categories and Relevance: The types of personal data to be processed and their relevance to the stated purpose; Retention Period: The duration for which the personal data will be stored and the criteria for determining this period; Data Processing Details: Specifics regarding the methods and scope of data processing activities; and Data Subject Rights: A clear explanation of the rights afforded to the Data Subject under Law No. 27/2022, including the right to access, rectification, erasure, and objection to processing.[50] Furthermore, the processing of personal data belonging to individuals with disabilities requires explicit consent from the data subject themselves and/or their legal guardians.[51] The Data Controller is obligated to cease processing personal data in the event that the Data Subject withdraws their consent for such processing.[52]

Law No. 27/2022 does not establish additional specific provisions beyond the overarching principle that personal data processing is permissible only with the informed consent of the Data Subject. The prohibitions outlined in Law No. 27/2022 are primarily confined to Chapter XIII (Prohibitions in the Use of Personal Data), which encompasses: Prohibits obtaining or collecting personal data that does not belong to the collector for personal gain or to benefit others, potentially causing harm to the Data Subject;[53] Prohibits disclosing personal data that does not belong to the discloser; Prohibits using personal data that does not belong to the user.

[48] Article 20 paragraph (2) letter a Law Number 27 of 2022 on Personal Data Protection.

[49] Article 22 paragraph (1) Law Number 27 of 2022 on Personal Data Protection.

[50] Article 21 paragraph (1) Law Number 27 of 2022 on Personal Data Protection.

[51] Article 26 paragraph (3) Law Number 27 of 2022 on Personal Data Protection.

[52] Article 40 Law Number 27 of 2022 on Personal Data Protection.

[53] Article 65 Law Number 27 of 2022 on Personal Data Protection.

Prohibits creating false personal data or falsifying existing data for personal gain or to benefit others, potentially causing harm to individuals;[54] Chapter XIV (Criminal Provisions) outlines the penalties associated with these prohibitions: penalties for violations of Article 65 paragraph (1) Law No. 27/2022; penalties for violations of Article 65 paragraph (2) Law No. 27/2022; and penalties for violations of Article 65 paragraph (3) Law No. 27/2022.

Law No. 27/2022 also establishes penalties for individuals who misuse personal data, underscoring the seriousness of data protection. Consequently, public awareness regarding the risks associated with disclosing personal information in the public domain must be heightened to mitigate potential misuse. Personal data, due to its sensitive nature, can have significant implications for individuals if mishandled.

However, it is important to acknowledge that collectivist cultures, like that of Indonesia, often place less emphasis on the individual right to privacy compared to individualistic societies. This cultural nuance can present challenges in implementing data protection frameworks that prioritize individual consent and control over personal information.[55] This situation may result in a lack of awareness among the public regarding their rights to personal data protection and a limited understanding of privacy concepts as defined by Law No. 27/2022. In a collectivist culture, sharing information about oneself and others is often perceived as a sign of familiarity. This tendency may lead to the habitual sharing of personal data without due consideration for the associated legal ramifications or security risks.[56]

Within collectivist societies, the understanding of privacy may diverge from the principles enshrined in Law No. 27/2022. Privacy, rather than being viewed as an inherent individual right requiring stringent protection, may be perceived differently. This difference in

[54] Article 66 Law Number 27 of 2022 on Personal Data Protection.

[55] Jolanda Jetten, Tom Postmes, dan Brendan J. McAuliffe, "'We're *All* Individuals': Group Norms of Individualism and Collectivism, Levels of Identification and Identity Threat," *European Journal of Social Psychology,* vol. 32, no. 2 (2002), p. 189.

[56] Adele Da Veiga, "An information privacy culture instrument to measure consumer privacy expectations and confidence," *Information & Computer Security*, vol. 26, no. 3 (2018), p. 64.

perception can diminish the perceived urgency for robust personal data protection measures. Furthermore, individuals within collectivist societies may not be fully cognizant of their rights pertaining to the control and management of their personal information. This lack of awareness can, in turn, lead to diminished public demand for the implementation and enforcement of comprehensive data protection safeguards.[57] A cultural emphasis on information sharing within communities may pose challenges to the enforcement of stringent limitations on the collection, processing, and dissemination of personal data as mandated by Law No. 27/2022.

Effective enforcement of Law No. 27/2022 necessitates a strong societal understanding of privacy rights and a commitment to compliance with data protection regulations. However, within collectivist cultures, such enforcement can be challenging due to potentially divergent perceptions of privacy and a correspondingly lower prioritization of personal data protection. Existing social norms and traditions may run contrary to the provisions of Law No. 27/2022. For instance, customary practices of sharing information regarding marriages, births, or deaths within a community may not align with the principles of strict personal data management as outlined in the Law.

Furthermore, the effectiveness of Law No. 27/2022, which fundamentally hinges on the principle of informed consent and user control over personal data processing, may be hampered in its implementation. Data subjects, encompassing Indonesian society with its collectivist ethos, may readily provide consent, particularly if their immediate needs or interests are met. The ingrained cultural tendency towards information sharing within Indonesian society further complicates the application of stringent data protection measures.[58] Collectivist cultural norms that encourage the free exchange of information may conflict with data privacy principles, which mandate limitations on data access and dissemination.

---

[57] Reza Ghaiumy Anaraky, Yao Li, dan Bart Knijnenburg, "Difficulties of Measuring Culture in Privacy Studies," *Proceedings of the ACM on Human-Computer Interaction,* vol. 5, no. 2 (2021), p. 26.

[58] Dodi Wirawan Irawanto, "An analysis of national culture and leadership practices in Indonesia," *Journal of Diversity Management (JDM)* vol. 4, no. 2 (2009), p. 41.

Furthermore, Article 63 of Law No. 27/2022 underscores the crucial role of public participation, both direct and indirect, in ensuring effective personal data protection. Therefore, public awareness, understanding, cultural norms, and established practices significantly influence the successful implementation of Law No. 27/2022.

Despite the legal framework provided by Law No. 27/2022, which explicitly mandates public engagement in data protection (Article 63), empirical evidence suggests that only a segment of the Indonesian population demonstrates readiness for its implementation. This finding underscores the urgent need for proactive measures to enhance public awareness and understanding of data privacy principles, coupled with the cultivation of responsible data handling practices. Specifically, individuals should exercise restraint in sharing personal information on digital platforms and social media, while adopting robust digital security measures to minimize the risk of data breaches.

The Cross-cultural comparisons such as with Japan, offer valuable insights into the interplay of collectivism and data protection. As De George posits, cultural values significantly influence the perception and interpretation of privacy. Different societies hold varying views on the definition of privacy, its significance, and the extent to which it warrants legal protection.[59]

Scholarly research indicates that Japanese society demonstrates a comparatively lower sensitivity towards privacy rights. The absence of a direct linguistic equivalent to the English word "privacy" further underscores this point.[60] The adopted term "*puraibashi*," while commonly used, often lacks a nuanced understanding among the general populace.[61] Consequently, privacy in Japan is often perceived as an imported concept, with some arguing that its subjective nature

[59] Yohko Orito and Kiyoshi Murata, "Privacy Protection in Japan: Cultural Influence on the Universal Value," *Electronic proceedings of Ethicomp* vol. 5, no.1 (2005), p. 9.

[60] Miyashita, "The Evolving Concept of Data Privacy in Japanese Law." *International Data Privacy Law* vol. 1, no. 4 (2011), p. 229.

[61] Yohko Orito and Kiyoshi Murata, "Privacy Protection in Japan: Cultural Influence on the Universal Value," *Electronic proceedings of Ethicomp* vol. 5, no.1 (2005), p. 9.

could potentially enable individuals to arbitrarily reject legitimate interactions or requests for information.

The conceptualization of privacy in Japan is deeply intertwined with its socio-cultural and historical context. It is argued that Japan's historical reliance on rice farming, which necessitates collective decision-making, has contributed to a societal emphasis on group harmony over individual needs. Japanese society places significant emphasis on group cohesion and believes that character development is best achieved through collaborative endeavors. Consequently, placing undue emphasis on individual rights, such as privacy, can be perceived as disruptive or indicative of distrust.[62] This cultural context is further reflected in communication patterns characterized by indirectness and an emphasis on interpreting unspoken cues (*tatemae* and *hon'ne*). Asserting privacy rights within such a framework can be misconstrued as a lack of cooperation or an inability to navigate social expectations effectively.[63]

The concept of group collectivism, which measures the extent to which individuals prioritize group membership and loyalty, provides a valuable lens for understanding societal attitudes towards data privacy. Societies with high group collectivism, such as Singapore, Malaysia, and Japan, often prioritize familial and social ties over individual rights. This emphasis on group cohesion can lead to a decreased emphasis on codifying stringent data protection measures.[64]

The apparent lack of comprehensive data protection frameworks in such societies can be attributed, in part, to the fact that privacy, as understood from an individualistic perspective, is not necessarily a foundational principle. This is further evidenced by the observation that societies with high group collectivism tend to lack stringent regulations governing the cross-border transfer of personal

---

[62] Miyashita, "The Evolving Concept of Data Privacy in Japanese Law." *International Data Privacy Law* vol. 1, no. 4 (2011), p. 229.

[63] *Nessrine Omrani and Nicolas Soulié, "Culture, Privacy Conception and Privacy Concern: Evidence from Europe before PRISM," 14th Asia-Pacific Regional Conference of the International Telecommunications Society (ITS), p. "Mapping ICT into Transformation for the Next Information Society", Kyoto, Japan,* 2017, p. 11.

[64] Orla Lynskey, "The 'Europeanisation of Data Protection Law," *Cambridge Yearbook of European Legal Studies* vol. 19, no. 1 (2017), p. 252.

data, often accompanied by a lack of robust enforcement mechanisms.[65]

Comparative Analysis: Data Protection in Individualist Societies

Numerous factors contribute to individual concerns regarding online privacy, including personal experiences, privacy awareness, personality traits, demographic variations, and cultural background, as highlighted by Smith. An individual's personal disposition, particularly their level of social consciousness, can significantly influence their privacy concerns. Dinev and Hart posit that individuals with heightened social consciousness tend to be more attuned to privacy-related issues and their societal implications.[66]

Furthermore, cultural background emerges as a crucial factor shaping privacy concerns. While the impact of culture on privacy has been widely acknowledged, empirical research directly addressing this relationship remains limited. Hofstede defines national culture as the "collective programming of the mind" that distinguishes members of one nation from another. This collective programming influences individual behavior through culturally ingrained values that prioritize certain actions while discouraging others. Given that culture profoundly shapes human thought and behavior, it naturally extends to influence individuals' perceptions and expectations regarding privacy.[67]

Hofstede's cultural dimensions and privacy concerns contain Individualism (IND), Power Distance (PDI), Uncertainty Avoidance (UAI), and Masculinity (MAS). The individualism (IND) dimension reflects the degree to which individuals prioritize their own needs and autonomy over those of the group. Individuals in highly individualistic cultures (high IND) tend to be more privacy-conscious, placing a higher value on personal boundaries and autonomy in managing

[65] Neil Richards and Woodrow Hartzog, "Taking Trust Seriously in Privacy Law," *Stan. Tech. L. Rev.* vol. 19, no. 1 (2015), p. 431.

[66] Abdel-Fattah E. Darwish and Günter L. Huber, "Individualism vs Collectivism in Different Cultures: A Cross-Cultural Study," *Intercultural Education* vol. 14, no. 1 (2003), p. 47.

[67] Richards and Hartzog, "Taking Trust Seriously in Privacy Law." *Stan. Tech. L. Rev.* vol. 19, no. 1 (2015), p. 431.

personal information.[68] The power Distance (PDI) dimension measures the extent to which less powerful members of society accept and expect unequal power distribution. Individuals in high PDI cultures may be more likely to accept intrusions into their privacy by those in positions of authority. The Uncertainty Avoidance (UAI) dimension reflects a society's tolerance for ambiguity and uncertainty. Higher UAI scores correlate with increased anxiety, stress, and a greater need for security. Consequently, individuals in high UAI cultures may exhibit greater privacy concerns due to heightened sensitivity to potential risks associated with information disclosure.[69] The Masculinity (MAS) dimension reflects the extent to which a society prioritizes achievement, assertiveness, and material success. High MAS cultures often place a higher value on economic gains, potentially leading individuals to prioritize the potential benefits of sharing personal information over privacy concerns. [70]

Bellman conducted a global survey of 534 internet users across 38 countries, employing three distinct analytical approaches to examine the influence of cultural values on privacy concerns. Their findings suggest that cultural values significantly impact consumer attitudes towards privacy. Similarly, a study analyzing data from 1,261 internet users across five cities (Bangalore, Seoul, Singapore, Sydney, and New York) found that nationality and cultural background, as measured by Hofstede's dimensions, influence online privacy concerns.[71] Specifically, individuals from individualistic cultures exhibited greater concern for online privacy compared to their counterparts from collectivist cultures. Miltgen and Guillard, through a qualitative survey of seven European Union member states, further

[68] Serge Gutwirth, Ronald Leenes, and Paul De Hert, eds., *Reforming European Data Protection Law*, vol. 20, Law, Governance and Technology Series (Dordrecht: Springer Netherlands, 2015), p. 37.

[69] John M. Roberts and Thomas Gregor, "Privacy: A Cultural View," in *Privacy and Personality* (Oxfordshire: Routledge, 2017), p. 199.

[70] Serge Gutwirth, Ronald Leenes, and Paul De Hert, eds., *Reforming European Data Protection Law*, vol. 20, Law, Governance and Technology Series (Dordrecht: Springer Netherlands, 2015), p. 37.

[71] Lilian Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective," *Eur. Data Prot. L. Rev.* vol. 2, no. 1 (2016), p. 28.

corroborated the finding that individuals from collectivist cultures tend to express lower levels of privacy concern.[72]

While the right to privacy has gained global recognition, particularly in light of the rapid evolution of the information society, Japan presents a unique case study. Despite the increasing emphasis on personal data protection in many developed nations, Japan demonstrates a comparatively lower level of sensitivity towards privacy concerns. This can be attributed, in part, to the country's distinct cultural and social environment.[73]

As previously discussed, Japan's collectivist culture, rooted in historical practices that prioritize group harmony and interdependence, significantly shapes societal attitudes towards privacy. Within this context, asserting individual privacy rights can be perceived as disruptive or indicative of distrust within social and professional relationships. The concept of privacy itself is relatively new to Japan, with the adopted term "*puraibashi*" lacking a deeply ingrained cultural understanding.[74] This further contributes to the perception of privacy as a foreign concept, potentially less deserving of protection compared to traditional values like group harmony and social cohesion.

Understanding the interplay between culture and privacy concerns is crucial in our increasingly interconnected world. While the right to privacy has gained global recognition, its interpretation and application vary significantly across cultures. Collectivist societies, such as Japan, present a unique set of challenges and considerations for data protection efforts. Recognizing and addressing these cultural nuances is essential for developing effective and culturally sensitive

[72] Yohko Orito and Kiyoshi Murata, "Privacy Protection in Japan: Cultural Influence on the Universal Value," *Electronic proceedings of Ethicomp* vol. 5, no.1 (2005), p. 9.

[73] Paul De Hert and Serge Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power," *Privacy and the Criminal Law*, Intersentia Antwerp/Oxford, 2006, 61–104.

[74] Subhajit Basu, "Privacy Protection: A Tale of Two Cultures," *Masaryk University Journal of Law and Technology* 6, no. 1 (2012), p. 1–34.

privacy frameworks that balance individual rights with societal values.[75]

Individualism is defined as a preference for a loosely-knit social framework. In individualistic cultures, individuals are expected to prioritize their own well-being and that of their immediate family. Consequently, individuals within such cultures tend to demonstrate heightened concern for online privacy.[76] Countries characterized by individualistic cultures generally hold strong convictions, value personal autonomy, and place a high premium on the right to privacy.[77] Within the context of individualistic cultures, where values such as self-reliance, privacy, and individual rights are paramount, the implementation of data protection regulations is highly relevant and often encounters greater societal acceptance. Individualistic cultures, prevalent in many Western societies, are frequently underpinned by principles of liberal democracy, which champion the notion of individuals having inherent rights to control their personal information.[78]

National cultures that place a high value on privacy tend to possess more developed infrastructures to support the implementation of data protection regulations. This includes robust information security technologies and effective data management systems. Furthermore, individualistic cultures often have legal systems founded on the principle of individual rights, including the right to privacy. This provides a strong legal foundation for data protection regulations and facilitates their seamless integration into existing legal frameworks.[79]

---

[75] Yohko Orito and Kiyoshi Murata, "Privacy Protection in Japan: Cultural Influence on the Universal Value," *Electronic proceedings of Ethicomp,* vol. 5, no.1 (2005), p. 9.

[76] I. Reay et al., "Privacy Policies and National Culture on the Internet," *Information Systems Frontiers,* vol. 15, no. 2 (2013), p. 279.

[77] Sophie Cockcroft dan Saphira Rekker, "The Relationship between Culture and Information Privacy Policy," *Electronic Markets,* vol. 26, no. 1 (2016), p. 55.

[78] Rowena Cullen, "Culture, identity and information privacy in the age of digital government," *Online Information Review* vol. 33, no. 3 (2009), p. 21.

[79] Saskia Witteborn, "Data privacy and displacement: A cultural approach," *Journal of Refugee Studies* vol. 34, no. 2 (2021), p. 22.

Reconciling Data Protection with Indonesian Collectivism: Negotiating Effective Implementation

Grounding Data Protection Education in Pancasila: The Reciprocal Relationship between Law and Ideology

The implementation of Law No. 27/2022 on Personal Data Protection cannot be divorced from Indonesia's foundational ideology—Pancasila. The relationship between law and ideology is fundamentally reciprocal and mutually constitutive, a principle that has profound implications for legal education and public awareness campaigns related to data protection. Understanding this reciprocal relationship is essential for developing effective strategies to bridge the gap between legal frameworks and societal practices in Indonesia's collectivist context.

The reciprocal relationship between law and ideology has been extensively analyzed in legal theory, particularly within critical legal studies and Marxist legal scholarship. Hugh Collins, in his seminal work *Marxism and Law*, articulates that law is not merely an ideology supported by institutionalized social forces, but also an institutionalized social force that is articulated in and reinforced by ideology.[80] In other words, ideology determines legal products—shaping what laws are created, how they are interpreted, and what values they prioritize—and legal products, in turn, strengthen the prevailing ideology by legitimizing certain values, normalizing particular social arrangements, and providing institutional mechanisms for ideology's reproduction. This bidirectional relationship means that law both reflects and shapes the ideological commitments of a society, creating a reinforcing cycle where legal institutions embody ideological principles while simultaneously working to entrench those principles more deeply in social consciousness.

Applied to the Indonesian context, this reciprocal relationship between law and ideology manifests in the connection between Pancasila and the legal system. Pancasila serves as both the philosophical foundation (*grundnorm* in Hans Kelsen's terminology) and the ideological framework for Indonesia's legal system, as explicitly recognized in the 1945 Constitution. As Sudjito argues, Pancasila is not merely a political concept or abstract philosophy but a

[80] Hugh Collins, *Marxism and Law* (Oxford University Press, 1984).

comprehensive worldview (*Weltanschauung*) that shapes how Indonesians understand rights, responsibilities, and the proper relationship between individuals and society.[81] Therefore, legal education regarding Law No. 27/2022 must be explicitly grounded in Pancasila's five principles to achieve cultural resonance and genuine behavioral change rather than mere superficial compliance driven by fear of penalties.

If legal education is conducted without grounding in Pancasila ideology, it risks creating cognitive dissonance among the Indonesian public, who may perceive data protection principles as foreign impositions that conflict with their deeply held cultural values of openness, trust, and communal information sharing. This perception can lead to resistance, non-compliance, or merely performative adherence to legal requirements without internalization of data protection values. Conversely, when legal education is explicitly framed within Pancasila ideology, demonstrating how data protection principles align with and support Indonesia's foundational values, it gains legitimacy and cultural resonance. This approach transforms data protection from a foreign legal transplant into an authentic expression of Indonesia's own ideological commitments, facilitating genuine behavioral change and fostering a sense of ownership over data protection norms.

The first principle of Pancasila, *Ketuhanan Yang Maha Esa* (Belief in the One Supreme God), provides a foundation for understanding data protection as a moral and ethical responsibility rooted in religious values. Legal education should emphasize that all major religions practiced in Indonesia—Islam, Christianity, Catholicism, Hinduism, Buddhism, and Confucianism—teach principles of honesty, trustworthiness (*amanah* in Islamic terminology), and respect for others' dignity and privacy. Misusing personal data, whether through unauthorized access, exploitation for commercial gain, or disclosure without consent, violates these fundamental religious principles. Educational campaigns can frame data protection as *amanah*, emphasizing that when individuals entrust us with their personal information, we have a religious and moral obligation to protect it as a sacred trust. This framing resonates deeply in Indonesian society, where religious identity is central to personal and communal life, and

[81] Lubis, "Pancasila."

religious teachings are widely accepted as legitimate sources of moral guidance. Furthermore, respect for human dignity, a principle emphasized across all religious traditions, requires protecting individuals from data exploitation and misuse that can harm their reputation, economic interests, or personal safety. Religious teachings apply equally to online and offline behavior, meaning that ethical conduct in digital spaces is not optional but is a religious obligation for believers.

The second principle, *Kemanusiaan yang Adil dan Beradab* (Just and Civilized Humanity), emphasizes that human dignity must be protected in a just and civilized manner, providing another foundation for data protection education. Legal education should articulate that data protection is fundamentally a human rights issue, as personal data protection is an extension of the fundamental right to human dignity recognized in international human rights instruments and the Indonesian Constitution. Justice requires equal protection, meaning that all Indonesians, regardless of their digital literacy level, socioeconomic status, or geographic location, deserve equal protection of their personal data from exploitation and misuse. A civilized society, as envisioned in this principle, respects boundaries, including digital boundaries and privacy, and does not tolerate exploitation of vulnerable individuals or communities through data misuse. This framing connects data protection to Indonesia's aspirations for a just and civilized society, making it part of the nation's broader development goals rather than a narrow technical legal requirement.

The third principle, *Persatuan Indonesia* (Unity of Indonesia), provides a powerful framework for emphasizing the collective dimensions of data protection rather than framing it solely as an individualistic concern. Legal education should emphasize that protecting Indonesian citizens' data strengthens national digital sovereignty in an era where data has become a strategic resource and foreign entities increasingly seek access to Indonesian data for commercial and potentially strategic purposes. Data breaches affecting individuals can undermine trust and social cohesion, threatening national unity when citizens lose confidence in digital systems and institutions. The principle of *gotong royong*, deeply embedded in Indonesian culture and explicitly referenced in the Constitution, can be applied to digital safety: just as communities traditionally cooperate

for physical security, mutual aid, and infrastructure development, they must now cooperate for digital security and collective data protection. This framing transforms data protection from an individual responsibility that may seem selfish or contrary to collectivist values into a collective responsibility that strengthens community bonds and national unity.

The fourth principle, *Kerakyatan yang Dipimpin oleh Hikmat Kebijaksanaan dalam Permusyawaratan/Perwakilan* (Democracy Led by Wisdom through Deliberation/Representation), emphasizes collective decision-making and informed participation, which can be connected to the concept of informed consent in data protection. Legal education should emphasize that just as citizens have the right to informed participation in governance through democratic processes, they have the right to informed consent regarding how their personal data is collected, used, and shared. Democratic values require that data controllers be transparent about data use, providing clear and accessible information rather than hiding practices in lengthy, incomprehensible terms of service agreements, and be accountable for violations through effective oversight mechanisms and meaningful penalties. Empowerment through knowledge is central to democratic participation, meaning that legal education itself is a democratic right that enables citizens to exercise their data protection rights effectively and participate meaningfully in the digital economy and digital governance.

The fifth principle, *Keadilan Sosial bagi Seluruh Rakyat Indonesia* (Social Justice for All Indonesian People), explicitly prioritizes collective welfare and equitable distribution of resources, providing a framework for addressing digital inequality and data exploitation. Legal education should emphasize that social justice requires protecting vulnerable populations from data exploitation, including children, elderly individuals with limited digital literacy, rural communities with limited access to information about data protection, and economically disadvantaged groups who may be coerced into sharing data for access to essential services. Addressing digital inequality means ensuring that legal education reaches marginalized communities, providing equitable access to data protection knowledge and resources regardless of socioeconomic status or geographic location. Fair distribution of digital benefits requires that the

advantages of digitalization—including access to services, economic opportunities, and information—are shared equitably, and that data protection ensures individuals are not exploited or excluded from these benefits due to data misuse or lack of awareness.

This Pancasila-based framework for legal education operationalizes the reciprocal relationship between law and ideology. On one hand, Pancasila ideology shapes how Law No. 27/2022 is understood, interpreted, and implemented, providing cultural legitimacy and moral authority for data protection requirements. On the other hand, legal education about Law No. 27/2022, when explicitly grounded in Pancasila principles, reinforces and strengthens public commitment to Pancasila values, demonstrating their continued relevance in the digital age and their capacity to guide Indonesia through contemporary challenges. This creates a reinforcing cycle where ideology shapes legal understanding, legal education reinforces ideology, and behavioral change becomes culturally congruent rather than imposed from outside.

Table 3. The Reciprocal Relationship Between Pancasila Ideology and Data Protection Law

Pancasila Principle	How Ideology Shapes Data Protection Law	How Data Protection Law Reinforces Ideology	Educational Approach
Ketuhanan Yang Maha Esa (Belief in the One Supreme God)	Religious values of amanah (trustworthiness) and respect for human dignity provide a moral foundation for data protection obligations	Implementing data protection demonstrates that religious values apply to digital spaces, reinforcing religious ethics in modern contexts	Frame data protection as a religious and moral obligation; engage religious leaders in education campaigns
Kemanusiaan	Human dignity	Enforcing data	Emphasize

yang Adil dan Beradab (Just and Civilized Humanity)	requires protection from data exploitation; justice demands equal protection regardless of digital literacy	protection rights demonstrates a commitment to human dignity and justice in the digital age	data protection as a human rights issue; highlight justice dimensions of equal protection
Persatuan Indonesia (Unity of Indonesia)	National unity requires collective digital security; data sovereignty strengthens national independence	Collective data protection efforts strengthen social cohesion and trust in digital systems	Frame data protection as *gotong royong* for digital safety; emphasize collective benefits
Kerakyatan (Democracy through Deliberation)	Democratic participation requires informed consent; transparency and accountability are democratic values	Data protection rights empower democratic participation in digital governance and economy	Connect informed consent to democratic participation; emphasize transparency and accountability
Keadilan Sosial (Social Justice for All)	Social justice requires protecting vulnerable populations from data exploitation; equitable access to data protection knowledge	Implementing equitable data protection reduces digital inequality and ensures fair distribution of digital benefits	Address digital inequality; ensure education reaches marginalized communities; prevent exploitation

Source: Author's analysis based on Pancasila philosophy and Law No. 27/2022 on Personal Data Protection.

The operationalization of Pancasila-based legal education requires concrete strategies that translate these philosophical principles into practical educational programs. Curriculum development must be explicitly rooted in Pancasila, with educational materials referencing Pancasila principles using language and examples that resonate with Indonesian cultural values rather than simply translating Western data protection materials. Religious leaders should be engaged as educators to communicate data protection principles through religious frameworks, leveraging their moral authority and trusted position in communities. Cultural narratives, including Indonesian folklore, proverbs (*pepatah*), and cultural stories, should be used to illustrate data protection concepts in culturally familiar terms. Pancasila-based case studies should be developed showing how data protection aligns with each Pancasila principle, making abstract legal concepts concrete and culturally relevant.

Rather than emphasizing individual rights in isolation, which may seem selfish or contrary to collectivist values, education should frame data protection as a collective responsibility aligned with *gotong royong*. Messaging should emphasize that "protecting your data protects our community," highlighting how individual data security contributes to collective digital safety and community well-being. Community-based education should be conducted through existing community structures such as *RT/RW* (neighborhood associations), religious organizations, community centers, and traditional governance structures, leveraging existing social networks and trusted community leaders. Peer education models should train community leaders to educate their peers, recognizing that information from trusted community members is more persuasive than messages from distant government authorities.

Formal education systems should integrate data protection within Pancasila education (*Pendidikan Pancasila*), which is already a required subject at all educational levels in Indonesia. Curriculum integration should include data protection modules in Pancasila and Civic Education (*PPKn*) courses, showing students how data protection embodies Pancasila values. Teacher training programs

should equip teachers to articulate the connection between Pancasila values and data protection, ensuring they can answer students' questions and address cultural concerns. Youth engagement initiatives should develop youth-friendly materials that connect Pancasila values to digital citizenship, recognizing that young Indonesians are both the most digitally active population and the future guardians of Indonesian values.

Public awareness campaigns should explicitly demonstrate how Law No. 27/2022 embodies Pancasila values rather than presenting it as a technical legal requirement or foreign imposition. Campaign slogans should connect data protection to Pancasila, such as "*Melindungi Data Pribadi, Mewujudkan Keadilan Sosial*" (Protecting Personal Data, Realizing Social Justice) or "*Gotong Royong Digital untuk Indonesia yang Aman*" (Digital Mutual Cooperation for a Secure Indonesia). Visual symbolism should use Pancasila symbols, including the Garuda Pancasila and representations of the five principles, in educational materials to create visual associations between data protection and national identity. A national narrative should frame data protection as part of Indonesia's national development aligned with Pancasila, connecting it to broader goals of digital sovereignty, economic development, and social justice.

By grounding legal education in Pancasila ideology, Indonesia can create a reinforcing cycle where ideology shapes legal understanding, providing the cultural framework through which Law No. 27/2022 is understood and accepted; legal education reinforces ideology, with teaching about data protection through Pancasila strengthening public commitment to Pancasila values and demonstrating their continued relevance; and behavioral change becomes culturally congruent, as data protection is seen as an expression of Pancasila values rather than external imposition, making compliance a matter of cultural identity and moral obligation rather than mere legal requirement. This approach addresses the fundamental challenge of implementing data protection in a collectivist society by transforming potential cultural conflict into cultural alignment, where protecting personal data becomes an authentic expression of Indonesian values rather than an adoption of foreign individualistic principles.

Prioritizing Legal Education and Legal Awareness

Sage and Woodlock contend that legal sector reforms often falter due to a failure to adequately account for the "cultural embeddedness" of target nations, which frequently exhibit diverse non-state and customary legal norms. This underscores the importance of cultural considerations in legal reform initiatives and gives rise to the concept of legal pluralism. This perspective posits that the shortcomings of many legal reforms stem from a failure on the part of donor institutions to recognize and accommodate the plurality of legal orders within recipient countries. Kyed argues that the approach of donor institutions towards legal pluralism is often characterized by "ambiguities and ideological baggage," wherein customary Law is granted recognition only insofar as it aligns with Western legal principles.[82]

To address the practical challenges inherent in legal pluralism projects, Kyed proposes the concept of "hybrid political orders." This framework emphasizes that legal and security institutions are not merely pluralistic in nature but also exist in a state of constant overlap, mutual influence, and ongoing transformation. This explanation for overlapping legal orders, particularly relevant in the context of developing nations, is attributed to the nature of the state itself. However, Kyed's analysis stops short of providing a definitive answer as to why certain countries are characterized by the presence of diverse and overlapping legal systems.[83]

Indonesian society, with its collectivist cultural orientation, is considered by some to be particularly vulnerable in the realm of data privacy due to a relatively low level of awareness and a lack of proactive measures to safeguard personal information.[84] This vulnerability is deeply intertwined with the nation's cultural background, a crucial aspect often overlooked in the development and implementation of data protection regulations. Despite the

[82] Garfield Benjamin, "Privacy as a Cultural Phenomenon," *Journal of Media Critiques* vol. 3, no. 10 (2017), p. 55.

[83] Ruth Gavison, "Privacy and the Limits of Law," *The Yale Law Journal* vol. 89, no. 3 (1980), p. 421.

[84] Lee A. Bygrave, "Privacy and Data Protection in an International Perspective," *Scandinavian Studies in Law,* vol. 56, no. 8 (2010), p. 165.

demonstrable influence of cultural factors on privacy mechanisms, Indonesia's regulatory framework has yet to fully incorporate these considerations.[85]

In alignment with Article 63 of Law No. 27/2022, public participation is paramount for the effective implementation of data protection regulations. Education and awareness-raising initiatives are essential for fostering a culture of data privacy, particularly during the critical implementation phase. Integrating data protection and privacy principles into educational curricula at all levels, starting from an early age, is crucial for instilling a strong foundation of understanding.

Indonesia's collectivist culture, characterized by communal values, openness, and information sharing, presents unique considerations for implementing data protection regulations. The principles of *gotong royong* and social trust are deeply ingrained in Indonesian society. Therefore, implementing Law No. 27/2022 requires a nuanced approach that respects and leverages these existing cultural values.

Rather than prioritizing immediate and stringent enforcement, the initial focus should be on comprehensive and sustained public education and legal awareness campaigns.[86] This approach aligns with the essence of collectivism itself – fostering shared understanding and collective action towards a common goal, which in this case is the protection of personal data.[87]

Introducing Law No. 27/2022 necessitates a carefully considered approach to avoid misinterpretations among the public, who may perceive it as a restriction on their ingrained cultural practices of information sharing. Effective education can bridge this gap and cultivate a positive perception of data privacy principles.

Public education campaigns should emphasize that data protection, within the context of collectivist values, is not solely an individual right but a shared responsibility to create a secure and trustworthy digital environment for all. By highlighting the collective

---

[85] Soedjono Dirdjosisworo, *Sosiologi Hukum: Studi Tentang Perubahan Hukum Dan Sosial* (Jakarta: Raja Grafindo, 1996), p. 27.

[86] Alex Boniface Makulilo, "Privacy and Data Protection in Africa: A State of the Art," *International Data Privacy Law* vol. 2, no. 3 (2012), p. 163.

[87] Leonardo Horn Iwaya et al., "Organisational Privacy Culture and Climate: A Scoping Review," *IEEE Access* vol. 10, no. 1 (2022), p. 739.

benefits of data protection, education can bridge the gap between individual rights and communal values.[88]

Essential elements of an effective educational strategy contain five strategies. First, accessible language and relatable content. Educational materials should utilize clear, concise language tailored for the general public, incorporating relatable examples, illustrations, and culturally relevant narratives. Second, multi-platform dissemination. Information dissemination should leverage diverse and accessible platforms, including social media, digital channels, traditional media (television, radio, print), and community engagement initiatives. Third, collaborative partnerships. Successful implementation hinges on robust collaboration among government agencies, civil society organizations, academia, the private sector, and influential community figures. Fourth, early intervention and curriculum integration. Integrating data protection principles into formal education curricula across all levels will empower future generations with essential knowledge and skills, ensuring the long-term sustainability of a privacy-conscious society. Fifth, continuous evaluation and adaptation. Ongoing evaluation and adaptation of educational programs are essential to ensure relevance, effectiveness, and responsiveness to evolving societal needs and technological advancements.[89]

Indonesia's collectivist spirit, exemplified by *gotong royong*, presents a unique opportunity to foster a collective movement for data protection. Educational initiatives should emphasize five steps. First, demystifying Law No. 27/2022. Explaining the core principles of the Law in clear and accessible language, outlining the rights and responsibilities of data subjects, and elucidating the legal consequences for violations. Second, fostering data literacy. Enhancing public understanding of personal data types, potential risks associated with unauthorized access or misuse, and practical measures individuals can take to safeguard their own data and respect the data of others. Third, cultivating ethical data-sharing practices. Establishing clear ethical guidelines for sharing information in the digital age, emphasizing the importance of informed consent, transparency, and accountability.

---

[88] William A. Galston, "Limits of Privacy: Culture, Law, and Public Office," *Geo. Wash. L. Rev.* vol. 67, no.1 (1998), p. 1197.

[89] Janice Richardson, *Law and the Philosophy of Privacy* (Oxfordshire: Routledge, 2015), p. 98.

Implementing Law No. 27/2022 is a gradual process that requires a long-term vision and sustained commitment. Prioritizing education over immediate enforcement is crucial for fostering genuine and sustainable compliance, driven not by fear of penalties but by a collective understanding of the value of data privacy. Through sustained and culturally sensitive education, respect for data privacy can become deeply ingrained in Indonesia's social fabric, reflecting the nation's values of mutual respect, responsibility, and collective well-being.

Effective implementation necessitates widespread dissemination of information regarding the implementing regulations of Law No. 27/2022, along with practical guidance on enhancing personal data security. Public awareness campaigns should equip individuals with the knowledge and tools to protect their data effectively. Furthermore, it is crucial to empower citizens by enhancing their understanding of their rights under Law No. 27/2022. This includes the right to provide informed consent for data processing, access their personal data, request data rectification or deletion, and receive timely notifications regarding any data breaches that may impact their privacy. Finally, ensuring accountability for data handlers and processors is essential for building public trust in the data protection framework.[90] Clear mechanisms for reporting violations, seeking redress, and enforcing penalties against those who violate data protection regulations will contribute to the Law's effectiveness and foster a culture of compliance.[91]

Navigating Cultural Expectations: A Hybrid Approach to Data Privacy in Indonesia

From a sociological standpoint, the formulation of data protection regulations stems from the need to safeguard individual rights within the context of increasingly sophisticated data collection, processing, management, and dissemination practices. Robust privacy protections foster public trust, encouraging individuals to share

[90] Darwish, Abdel-Fattah E., and Günter L. Huber. "Individualism vs collectivism in different cultures: a cross-cultural study." *Intercultural education* vo.l 14, no. 1 (2003): p. 47.

[91] Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (New York: Cornell University Press, 1997), p. 89.

personal data for broader societal benefits without fear of misuse or infringement upon their rights.[92] This balance between individual and collective interests, the latter often represented by the state, is crucial for fostering a fair and equitable digital society. Effective data protection regulations are, therefore, essential for promoting order and progress within the evolving information landscape.

Some argue that Indonesian society, with its collectivist cultural orientation, places less emphasis on privacy as an inherent value. However, a closer examination reveals that Indonesian society does indeed value privacy, albeit manifested through different cultural expressions. Traditional values emphasizing respect for individual boundaries and discouraging actions that disrupt social harmony underscore the inherent, albeit culturally nuanced, recognition of privacy as a social good. This perspective is further corroborated by survey data indicating public awareness of and support for robust privacy and data protection measures.

The lack of adequate awareness and safeguards surrounding data privacy in Indonesia has created opportunities for violations and misuse of personal information.[93] The rampant buying and selling of citizen data for targeted marketing purposes is a pressing concern. This practice spans various sectors, from consumer goods to financial services, highlighting the widespread commodification of personal data.[94] The rise of social media has further amplified these risks, with the buying and selling of accounts and followers becoming increasingly common. Similarly, location-based messaging services, often operating without explicit user consent, exemplify how technological advancements can facilitate privacy violations.[95]

While Indonesia's Law No. 27/2022 draws inspiration from the European Union's General Data Protection Regulation (GDPR), it is essential to recognize that direct transplantation of a legal framework developed within a different cultural context may not be entirely

[92] Rowena Cullen, "Culture, Identity and Information Privacy in the Age of Digital Government," *Online Information Review,* vol. 33, no. 3 (2009), p. 405–21.

[93] Custers et al., "A Comparison of Data Protection Legislation and Policies across the EU." Computer Law & Security Review, vol. 34, no. 2 (2018), p. 234.

[94] Marco De Boni and Martyn Prigmore, "Cultural Aspects of Internet Privacy," *Retrieved May* vol. 13, no. 2 (2002), p. 2013.

[95] Cullen, "Culture, Identity and Information Privacy in the Age of Digital Government," *Online Information Review* vol. 33, no. 3 (2009), p. 405.

suitable. The European Union's emphasis on data protection, deeply rooted in its history and legal traditions, stands in contrast to Indonesia's evolving data privacy landscape. Therefore, a more nuanced "hybrid" approach is necessary, one that harmonizes international best practices with Indonesia's collectivist values and cultural norms. This approach can effectively bridge the cultural and knowledge gap regarding privacy among Indonesian citizens while fostering a more privacy-conscious society.

A successful data protection framework for Indonesia must be robust, enforceable, and culturally resonant. A hybrid approach, blending international standards with local context, is crucial for developing a framework that garners widespread acceptance and adherence. There are two key strategies for implementing a hybrid framework.[96] First, is community participation. Actively involving communities in the policy-making process is essential for ensuring that the resulting framework reflects their collective values and needs. This participatory approach should encompass. Second, culturally tailored education. Developing educational initiatives that resonate with local communities, taking into account collectivist values and utilizing culturally appropriate communication channels. Third, inclusive dialogue. Facilitating meaningful dialogue between the government, the private sector, academia, civil society organizations, and cultural experts to foster consensus and address potential concerns. Fourth, international collaboration. Engaging with international institutions and learning from best practices in other countries, particularly those with similar cultural contexts, to ensure alignment with global standards while preserving national interests. Fifth, flexibility and contextualization. Developing a regulatory framework that allows for flexibility without compromising on core data protection principles is crucial.[97]

The strategies above can be achieved through three steps. First, a principles-based approach. Adopting a principles-based approach

[96] Faye Fangfei Wang, "Culture and Trust in Privacy Information Protection," *International Review of Law, Computers & Technology* vol. 24, no. 2 (2010), p. 143.

[97] Makulilo, Alex B. "A Person Is a Person through Other Persons"-A Critical Analysis of Privacy and Culture in Africa." *Beijing L. Rev.* vol. 7, no. 3 (2016), p 192.

that allows for interpretation and adaptation to specific contexts, ensuring the framework remains relevant and responsive to evolving societal needs and technological advancements. Second, respect for existing norms. Recognizing and respecting existing social norms and cultural practices, such as *gotong royong*, while establishing clear boundaries to prevent these norms from being exploited to undermine data privacy. Third, context-specific exemptions. Considering carefully crafted exemptions for specific social and cultural practices, such as the use of personal data for religious or customary purposes, provided these exemptions do not compromise fundamental data protection principles or individual rights.

By embracing a hybrid approach that prioritizes community participation, flexibility, and international collaboration, Indonesia can develop a data protection framework that effectively safeguards individual privacy while respecting and upholding the nation's cherished collectivist values.[98] This culturally sensitive approach will pave the way for a more secure, trustworthy, and inclusive digital future for all Indonesians.

Conclusion

The concepts of privacy and data protection are highly regarded and deeply ingrained within individualistic cultures. Individuals in these societies tend to possess a heightened awareness of their privacy rights, including the right to control their personal information. However, Indonesia's collectivist culture, which prioritizes communal harmony, *gotong royong*, and information sharing, presents unique challenges for effectively implementing data protection regulations, such as Law No. 27/2022. The deeply ingrained practice of information sharing within Indonesian communities can lead to a lower perceived urgency for stringent data protection measures. Existing social norms often do not align with the principles of strict personal data management. While Law No. 27/2022 mandates informed consent for data processing, the lack of widespread awareness and a deep understanding of privacy rights and data security can result in individuals granting consent without fully considering the potential risks.

[98] Trepte, Sabine, et al. "A cross-cultural perspective on the privacy calculus." *Social Media Society,* vol. 3, no. 1 (2017), p. 205.

To effectively implement data protection regulations within Indonesia's collectivist context, a multi-pronged approach is necessary. Prioritizing education and public legal awareness campaigns is paramount. Enhancing public understanding through culturally relevant educational initiatives and targeted public campaigns is essential for fostering a culture of data privacy. Furthermore, a hybrid regulatory framework that harmonizes international data protection standards with Indonesia's unique cultural values is essential. This framework should prioritize active community participation in the policy-making process to ensure that the resulting regulations resonate with local values and address community concerns. Additionally, the framework should incorporate flexibility to accommodate existing social and business practices while upholding core data protection principles. This may involve carefully crafted exemptions for specific cultural practices, provided these exemptions do not undermine fundamental privacy rights. By respecting existing cultural norms while clearly delineating boundaries to prevent the exploitation of these norms in a way that undermines data privacy, Indonesia can foster a digital environment that effectively safeguards individual privacy while honoring its unique cultural values.

Acknowledgments

The author wishes to express their deepest gratitude to Yesmil Anwar, S.H., M.Si., and Dr. Dadang Epi Sukarsa, S.H., M.H., lecturers of the Sociology of Law course within the Project-Based Master's Program at the Faculty of Law, Padjadjaran University. Their invaluable guidance, insightful critiques, and unwavering support throughout the research and writing process have been instrumental in shaping this article. Furthermore, the author extends sincere appreciation to their esteemed colleagues in the Project-Based Master's Program at the Faculty of Law, Padjadjaran University. Their insightful feedback, collaborative spirit, and engaging discussions during the article's development have significantly enriched its quality and depth. The author feels privileged to be part of such a vibrant and intellectually stimulating academic community.

Bibliography

Amien, Miska. "Causa Materialis Pancasila Menurut Notonagoro." *Jurnal Filsafat*, vol. 16, no. 1 (2006): 18–26.

Anwar, Yesmil. *Pengantar Sosiologi Hukum*. Grasindo, 2008.

Barbas, Samantha. "The Sidis Case and the Origins of Modern Privacy Law." *Colum. JL & Arts* 36 (2012): 21.

Basu, Subhajit. "Privacy Protection: A Tale of Two Cultures." *Masaryk University Journal of Law and Technology*, vol. 6, no. 1 (2012): 1–34.

Benjamin, Garfield. "Privacy as a Cultural Phenomenon." *Journal of Media Critiques*, vol. 3, no. 10 (2017): 55–74.

Bygrave, Lee A. "Privacy and Data Protection in an International Perspective." *Scandinavian Studies in Law*, vol. 56, no. 8 (2010): 165–200.

Cockcroft, Sophie. "Culture, Law and Information Privacy." *Proceedings of European and Mediterranean Conference on Information Systems, Polytechnic University of Valencia, Spain*, 2007.

Cockcroft, Sophie, and Saphira Rekker. "The Relationship between Culture and Information Privacy Policy." *Electronic Markets*, vol. 26, no. 1 (2016): 55–72. https://doi.org/10.1007/s12525-015-0195-9.

Collins, Hugh. *Marxism and Law*. Oxford University Press, 1984.

Cullen, Rowena. "Culture, Identity and Information Privacy in the Age of Digital Government." *Online Information Review*, vol. 33, no. 3 (2009): 405–21.

Cullen, Rowena. "Culture, Identity and Information Privacy in the Age of Digital Government." *Online Information Review*, vol. 33, no. 3 (2009): 405–21.

Custers, Bart, Francien Dechesne, Alan M. Sears, Tommaso Tani, and Simone Van der Hof. "A Comparison of Data Protection Legislation and Policies across the EU." *Computer Law & Security Review*, vol. 34, no. 2 (2018): 234–43.

Da Veiga, Adele. "An Information Privacy Culture Instrument to Measure Consumer Privacy Expectations and Confidence." *Information & Computer Security*, vol. 26, no. 3 (2018): 338–64.

Darwish, Abdel-Fattah E., and Günter L. Huber. "Individualism vs Collectivism in Different Cultures: A Cross-Cultural Study."

Intercultural Education, vol. 14, no. 1 (2003): 47–56. https://doi.org/10.1080/1467598032000044647.

"Data Protection Laws of the World." Accessed November 4, 2025. https://www.dlapiperdataprotection.com/.

De Boni, Marco, and Martyn Prigmore. "Cultural Aspects of Internet Privacy." *Retrieved May* 13 (2002): 2013.

De Hert, Paul, and Serge Gutwirth. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power." *Privacy and the Criminal Law*, Intersentia Antwerp/Oxford, 2006, 61–104.

DeCew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, 1997.

Dirdjosisworo, Soedjono. *Sosiologi Hukum: Studi Tentang Perubahan Hukum Dan Sosial*. Raja Grafindo Persada, 1996.

Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." *Eur. Data Prot. L. Rev.* 2 (2016): 28.

Fuady, Munir. *Teori-Teori Dalam Sosiologi Hukum*. Kencana, 2013.

Galston, William A. "Limits of Privacy: Culture, Law, and Public Office." *Geo. Wash. L. Rev.* 67 (1998): 1197.

Gavison, Ruth. "Privacy and the Limits of Law." *The Yale Law Journal* , vol. 89, no. 3 (1980): 421–71.

Ghaiumy Anaraky, Reza, Yao Li, and Bart Knijnenburg. "Difficulties of Measuring Culture in Privacy Studies." *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2 (2021): 1–26. https://doi.org/10.1145/3479522.

Gutwirth, Serge, Ronald Leenes, and Paul De Hert, eds. *Reforming European Data Protection Law*. Vol. 20. Law, Governance and Technology Series. Springer Netherlands, 2015. https://doi.org/10.1007/978-94-017-9385-8.

Hofstede, Geert. "Dimensionalizing Cultures: The Hofstede Model in Context." *Online Readings in Psychology and Culture*, vol. 2, no. 1 (2011): 8.

Hofstede, Geert, Gert Jan Hofstede, and Michael Minkov. *Cultures et Organisations: Nos Programmations Mentales*. Pearson Education France, 2010..

"Indeks Literasi Digital Indonesia Tahun 2021-2022 - Satu Data KOMDIGI." Accessed November 4, 2025.

https://data.komdigi.go.id/opendata/dataset/indeks-literasi-digital-indonesia.

Irawanto, Dodi Wirawan. "An Analysis of National Culture and Leadership Practices in Indonesia." *Journal of Diversity Management (JDM)*, vol. 4, no. 2 (2009): 41–48.

Iwaya, Leonardo Horn, Gabriel Horn Iwaya, Simone Fischer-Hübner, and Andrea Valeria Steil. "Organisational Privacy Culture and Climate: A Scoping Review." *IEEE Access* 10 (2022): 73907–30.

Jabatan Perlindungan Data Peribadi (PDP), Malaysia. July 4, 2024. https://www.pdp.gov.my/ppdpv1/.

Jetten, Jolanda, Tom Postmes, and Brendan J. McAuliffe. "'We're *All* Individuals': Group Norms of Individualism and Collectivism, Levels of Identification and Identity Threat." *European Journal of Social Psychology*, vol. 32, no. 2 (2002): 189–207. https://doi.org/10.1002/ejsp.65.

Kansil, Christine ST. *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia*. Balai Pustaka, 1992.

Kohl, Uta. "The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy." *International & Comparative Law Quarterly*, vol. 72, no. 3 (2023): 737–69.

Li, Yao, Alfred Kobsa, Bart P. Knijnenburg, and M-H. Carolyn Nguyen. "Cross-Cultural Privacy Prediction." *Proceedings on Privacy Enhancing Technologies*, vol. 1 no. 2 (2017): 113–32. https://doi.org/10.1515/popets-2017-0019.

Lubis, R. Karlina. "Pancasila: Paradigma Ilmu Hukum Indonesia." *Conference: Kongres Pancasila VI, Ambon*, 2014.

Lynskey, Orla. "The 'Europeanisation'of Data Protection Law." *Cambridge Yearbook of European Legal Studies* 19 (2017): 252–86.

Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford University Press, 2015.

Makulilo, Alex B. "' A Person Is a Person through Other Persons'-A Critical Analysis of Privacy and Culture in Africa." *Beijing L. Rev.* 7 (2016): 192.

Makulilo, Alex Boniface. "Privacy and Data Protection in Africa: A State of the Art." *International Data Privacy Law*, vol. 2, no. 3 (2012): 163–78.

Miyashita, Hiroshi. "The Evolving Concept of Data Privacy in Japanese Law." *International Data Privacy Law*, vol. 1, no. 4 (2011): 229–38.

Notonagoro, Pembukaan Undang-Undang Dasar. "Dalam Pancasila Dasar Falsafah Negara." *Cetakan Ketujuh, Jakarta: Bina Aksara*, 1988.

Notonagoro, Sukamto. *Pancasila Secara Ilmiah Populer*. Pantjuran Tudjuh, 1975.

Omrani, Nessrine, and Nicolas Soulié. *Culture, Privacy Conception and Privacy Concern: Evidence from Europe before PRISM*. n.d.

Orito, Yohko, and Kiyoshi Murata. *Privacy Protection in Japan: Cultural Influence on the Universal Value*. n.d.

Osucha, Eden. "The Whiteness of Privacy: Race, Media, Law." *Camera Obscura: Feminism, Culture, and Media Studies*, vol. 24, no. 1 (2009): 67–107.

"Personal Data Protection Commission Singapore | PDPC." Accessed November 4, 2025. https://www.pdpc.gov.sg/.

Reay, I., P. Beatty, S. Dick, and J. Miller. "Privacy Policies and National Culture on the Internet." *Information Systems Frontiers* 15, no. 2 (2013): 279–92. https://doi.org/10.1007/s10796-011-9336-7.

Richards, Neil, and Woodrow Hartzog. "Taking Trust Seriously in Privacy Law." *Stan. Tech. L. Rev.* 19 (2015): 431.

Richardson, Janice. *Law and the Philosophy of Privacy*. Routledge, 2015.

Roberts, John M., and Thomas Gregor. "Privacy: A Cultural View." In *Privacy and Personality*. Routledge, 2017.

Seubert, Sandra, and Carlos Becker. "The Culture Industry Revisited: Sociophilosophical Reflections on 'Privacy' in the Digital Age." *Philosophy & Social Criticism* 45, no. 8 (2019): 930–47. https://doi.org/10.1177/0191453719849719.

Soekanto, Soerjono. "Pokok-Pokok Sosiologi Hukum." *Rajawali Pers*, 1989.

Strahilevitz, Lior Jacob. "Toward a Positive Theory of Privacy Law." *Harv. L. Rev.* 126 (2012): 2010.

"Strengthening Indonesia's Personal Data Protection Framework." *Tech For Good Institute*, March 21, 2025.

Taufiqurrohman, Moch Marsa, and Elisatris Gultom. Corporate Digital Responsibility: Tanggung Jawab Etis Penggunaan

Teknologi Digital dalam Bisnis Perusahaan. *Humani*: Hukum dan Masyarakat Madani, vol. 13, no. 2 (2023).

Trepte, Sabine, Leonard Reinecke, Nicole B. Ellison, Oliver Quiring, Mike Z. Yao, and Marc Ziegele. "A Cross-Cultural Perspective on the Privacy Calculus." *Social Media + Society* 3, no. 1 (2017): 205630511668803. https://doi.org/10.1177/2056305116688035.

Van Der Kroef, Justus M. "Collectivism in Indonesian Society." *Social Research*, JSTOR, 1953, 193–209.

Veronese, Alexandre, Alessandra Silveira, Rebecca Lemos Igreja, Amanda Nunes Lopes Espiñeira Lemos, and Thiago Guimarães Moraes. *The Concept of Personal Data Protection Culture from European Union Documents: A "Brussels Effect" in Latin America?* Universidade do Minho. Escola de Direito (ED), 2023. http://repositorium.uminho.pt/handle/1822/88911.

Wang, Faye Fangfei. "Culture and Trust in Privacy Information Protection." *International Review of Law, Computers & Technology*, vol. 24, no. 2 (2010): 143–44. https://doi.org/10.1080/13600861003748193.

Whitman, James Q. "The Two Western Cultures of Privacy: Dignity versus Liberty." *Yale LJ* 113 (2003): 1151.

Witteborn, Saskia. "Data Privacy and Displacement: A Cultural Approach." *Journal of Refugee Studies*, vol. 34, no. 2 (2021): 2291–307.