Journal of Business, Management, and Social Studies
Vol. 5, No. 3, August 2025, pp. 107-115
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i3.130
Available online at www.jbms.site

Igniting the Spirit of the Personal Data Protection Law: Advancing Justice, Ethics, and Institutional Reform in Indonesia's Digital Legal Politics

Marcellius Kirana Hamonangan
Faculty of Law, Tarumanagara University, Jakarta, Indonesia

Wilma Silalahi
Faculty of Law, Tarumanagara University, Jakarta, Indonesia

ABSTRACT
Objective – This study investigates the legal and institutional challenges in implementing Law Number 27 of 2022 on Personal Data Protection (PDP Law) in Indonesia, with a particular focus on its capacity to uphold justice, ethical governance, and technological accountability in the digital age.
Methodology – This study employs a juridical-empirical approach through a comprehensive literature-based analysis. It integrates classical legal theories such as the Rechtsstaat principle and Gustav Radbruch's Trichotomy of Law, alongside modern frameworks, including Responsive Law, Living Law, the concept of the Digital Panopticon, and Behavioral Law.
Findings – This study reveals that the current PDP Law suffers from several deficiencies, notably the absence of an independent supervisory authority, the lack of explicit mechanisms for algorithmic oversight and the right to explanation, and inadequate remedies for data breach victims. These issues hinder the law's effectiveness in confronting the complexities of digital society.
Novelty – This study introduces a cross-generational theoretical framework that connects foundational legal principles with contemporary digital realities. It offers a normative and institutional pathway to reform Indonesia's data protection regime towards a more just, ethical, and human-centered legal order.
Keywords: *personal data protection, digital justice, responsive law, technological ethics, legal politics*

JEL Classification: K11, K24, O34
Article Info: Received 11 June 2025; Revised 15 June 2025; Accepted 17 June 2025
Article Correspondence: marcell.siahaan@gmail.com
Recommended Citation: Hamonangan, M. K., & Silalahi, W. (2025). Igniting the Spirit of the Personal Data Protection Law: Advancing Justice, Ethics, and Institutional Reform in Indonesia's Digital Legal Politics. Journal of Business, Management, and Social Studies, 5(3), 107-115.

I. INTRODUCTION

In today's digital society, personal data is no longer merely a collection of numbers or technical information: it represents identity, rights, and even human dignity. From transaction records and online preferences to biometric data and health histories, nearly every aspect of life is now recorded in data form. Unfortunately, this development has not always been accompanied by an adaptive legal system. Data breaches occur repeatedly, while enforcement mechanisms and protective measures remain sluggish. In Indonesia, citizen data has been openly traded on the dark web, including electoral, driver's license, and health insurance databases (Kompas, 2023).

As a response, Law Number 27 of 2022 on Personal Data Protection (UU PDP) was enacted as a foundational step in reforming national privacy law. This law governs principles of data processing, the rights of data subjects, the obligations of controllers, and stipulates administrative and criminal sanctions. However, as a relatively new legal instrument, the PDP Law still leaves many institutional and normative gaps: the absence of an independent supervisory authority, the lack of a tiered classification of violations, and the underdeveloped integration of technological ethics in its operational framework.

The problem is not merely technical, but conceptual. Has the state truly fulfilled its role in safeguarding its citizens in the digital realm? Is the law sufficient as mere written text, without being socialized and internalized as part of legal culture? As Eugen Ehrlich once asserted, "the law of the living" often plays a greater role in shaping social order than the law written in books (Ehrlich, 1936). In this context, the PDP Law has yet to ignite the spirit of the law: it has not yet fostered awareness, trust, or institutional effectiveness.

On the other hand, Philip Selznick's concept of responsive law argues that good law should not only be prescriptive, but must also be capable of addressing real social problems (Selznick, 1969). Thus, the challenge for Indonesia's PDP Law today is not simply to serve as a legal guide, but to function as a transformative instrument that is ethical, inclusive, and applicable to the complexities of the digital age.

Through a juridical-empirical approach based on literature studies, this study critically explores how the ideal institutional framework for supervising personal data protection can be formulated within the Indonesian legal system to ensure the effective enforcement of privacy rights in an increasingly digital society. It also examines the extent to which the concept of substantive justice can be implemented within the PDP Law, particularly in providing fair and proportional remedies for individuals harmed by data breaches. Equally important, this discussion aims to understand how principles of technological ethics such as algorithmic transparency, digital non-discrimination, and the right to explanation, all of which can be integrated into data protection practices rooted in constitutional safeguards and human dignity. Accordingly, this study does not merely offer normative reflection but aspires to contribute substantively to the development of Indonesia's digital legal politics in a way that upholds human dignity and strengthens the broader culture of law.

II. LITERATURE REVIEW

The Right to Privacy and Personal Data: From Constitutional Norms to Digital Realities

The right to privacy has long been recognized as an integral part of human rights, and in Indonesia, it is protected under Article 28G(1) and Article 28I(1) of the 1945 Constitution. In the digital age, the notion of privacy extends beyond physical space into cyberspace, making personal data the new medium for expressing autonomy, freedom, and dignity. Warren and Brandeis (1890), in their seminal work, famously defined privacy as "the right to be let alone," a form of individual control against unwanted social intrusion. This idea has evolved into the modern legal framework of data protection, most notably embodied in instruments such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Indonesia's enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) represents a legal milestone aimed at aligning domestic regulation with global standards. However, as Abdullah (2019) notes, the law's normative formulation still falls short in ensuring substantive justice, particularly in cases of mass data breaches and the misuse of personal data by digital platforms. This highlights the urgency of strengthening both ethical principles and institutional safeguards to ensure that data protection goes beyond mere legal formalism and becomes embedded in public consciousness and practice.

Theoretical Framework: Responsive, Living, and Just Law

This study draws on both classical and modern legal theories to guide its analysis. From a classical perspective, Friedrich Julius Stahl's Rechtsstaat theory asserts that a just legal state must ensure the protection of individual rights, particularly in power asymmetries between individuals and dominant institutions, including digital corporations. Similarly, Immanuel Kant emphasizes law as a means of preserving human moral autonomy, with data control as a critical extension of individual freedom (Kant, 1797). In the context of personal data protection, Kant's concept of moral autonomy affirms that individuals are not merely objects of data processing, but must be regarded as subjects entitled to determine how their data is used, based on the principle of autonomous will. This implies the necessity of a right to explanation and direct control over AI systems, particularly in automated decision-making contexts.

Gustav Radbruch's theory of legal trichotomy offers a normative compass for evaluating law through three lenses: justice, legal certainty, and utility. In the context of the PDP Law, these elements must be balanced. Without substantive justice for victims of data breaches, the law risks becoming merely administrative; without institutional certainty, its implementation is vulnerable; and without perceived utility, it risks losing its legitimacy (Radbruch, 1950).

From a modern perspective, Philip Selznick's concept of responsive law views law as a social institution that must respond to real-world problems, adapt to societal needs, and rejects the notion of law as a static set of rule (Selznick, 1969). In an era where technology advances faster than legislation, legal responsiveness becomes essential. Also in practice, mechanisms such as algorithmic audits and oversight can only become effective if accompanied by legal institutional reform and proactive systems for reporting violations.

Likewise, Eugen Ehrlich's living law theory reminds us that social norms often carry more influence than formal laws. In the context of digital Indonesia, the weak culture of reporting data breaches and the low level of user participation in consent mechanisms indicate that the PDP Law has yet to evolve into a "living law" and must therefore be internalized as part of Indonesia's legal culture, not just as a formal statute (Ehrlich, 1936).

Michel Foucault's theory of the digital panopticon adds a critical lens by illustrating how data has become not only an administrative asset but a tool of invisible surveillance and control. Without robust regulation, data processing reinforces the dominant position of corporations and the state in monitoring and manipulating behavior (Foucault, 1975). This makes algorithmic transparency and data accountability essential for ensuring justice in digital governance.

Lastly, behavioral law and economics, articulated by Cass Sunstein and Richard Thaler, shows that individuals often make irrational or uninformed choices when consenting to data processing. Hence, legal frameworks must be designed not merely to provide options but to protect people from exploitative consent structures (Sunstein & Thaler, 2008). This underpins the need for stricter consent standards and public digital literacy as part of a broader legal culture reform.

Previous Research: Gaps and Opportunities

Several previous studies have addressed the urgency of data protection in Indonesia. Rahman (2022) emphasized the need for harmonized sectoral regulations and the establishment of an independent data protection authority. Kurniawati (2021) highlighted the ethical dimensions of data governance, which remain underrepresented in national policy discourse. Fadli (2020) focused on the legal remedies for victims of data breaches, which he found to be inadequate. Yet, few studies have comprehensively integrated both classical and modern legal theories in addressing personal data protection as part of digital legal politics and efforts to foster a responsive legal culture.

This review affirms that personal data protection is not merely a normative legal issue: it is inherently political, ethical, and institutional. As such, it demands an approach that goes beyond.

III. METHODOLOGY

Type and Approach of Research

This research employs a juridical-empirical approach, with a balanced composition of 50% literature-based analysis and empirical contextual reflection on the implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law). This combined approach was chosen because the issue of personal data protection involves not only normative legal aspects, but also institutional dynamics, public legal awareness, and ethical responses to technological disruption.

The juridical approach is used to examine and interpret the substance of positive legal norms, namely the PDP Law, the 1945 Constitution of the Republic of Indonesia, and other relevant regulations. In parallel, the empirical approach is applied indirectly through literature-based observation of case studies, judicial decisions, and verified news reports, aimed at capturing the actual conditions of legal enforcement and public perception of personal data governance in Indonesia.

Types of Sources of Data

The research utilizes three categories of data: (1) Primary data, which includes legislative sources such as Law No. 27 of 2022, the 1945 Constitution, and judicial decisions (e.g., Supreme Court Decision No. 615 K/Pdt/2021) and foundational legal texts from both classical and contemporary legal thinkers, such as works by Gustav Radbruch, Philip Selznick, Eugen Ehrlich, Cass Sunstein, and Michel Foucault; (2) Secondary data, comprising national academic journals indexed in SINTA (minimum rank 4), including Jurnal Legislasi Indonesia (Rahman, 2022), Jurnal Komunikasi Hukum (Kurniawati, 2021), Jurnal Hukum dan Pembangunan (Fadli, 2020), and Jurnal Konstitusi (Abdullah, 2019); and (3) Tertiary data, which includes credible media publications that reflect factual situations and public discourse, such as articles from Kompas, Tempo, Katadata, and The Conversation Indonesia.

All sources used in this study have been verified, publicly accessible through active official links, and deemed reliable and free of misinformation.

Data Collection and Analysis Technique

Data was collected using a literature review method, involving systematic analysis of legal sources and academic references. This also included the identification of contextual information drawn from verified news articles, court documentation, and reports from non-governmental sources focusing on personal data issues.

The collected data was then analyzed qualitatively using a normative and critical-theoretical approach. Legal norms were evaluated in light of social realities, and examined through the lenses of classical legal theory (such as Rechtsstaat and the Radbruch formula) and modern legal perspectives (such as Responsive Law, Living Law, the Digital Panopticon, and Behavioral Law). The result of this analysis was then structured to propose actionable legal-political recommendations that are both contextual and forward-looking.

IV. RESULTS AND DISCUSSION

Institutional Reform and the Challenge of Enforcing Data Protection

One of the most fundamental weaknesses in the implementation of Indonesia's Personal Data Protection Law (PDP Law) lies in the absence of an independent supervisory authority as mandated by the legislation. The lack of such a body creates a vacuum in oversight, audit, and administrative sanction mechanisms for data controllers. Article 58(1) of the PDP Law clearly envisions a regulatory institution with the authority to supervise, resolve disputes, and act as a public-accessible accountability hub.

From the perspective of Rechtsstaat theory, a true rule of law must guarantee the protection of citizens' rights through credible and independent institutions (Stahl in Radbruch, 1950). In line with this, responsive law insists that legal structures must respond to real social conditions, in this case, the widespread and unchecked data breaches occurring across digital platforms and public agencies (Selznick, 1969). When law enforcement remains fragmented, sectoral, and lacks a central authority, public trust inevitably deteriorates.

The urgency of establishing an independent supervisory authority is also supported by an official brief from the Indonesian House of Representatives (DPR RI), which argues that effective data protection cannot rely solely on passive and sectoral administrative mechanisms (2021).

Rahman (2022) emphasizes that a data protection authority must not be merely an administrative function embedded within a technical ministry. Rather, it must be a morally legitimate institution, with budgetary independence and public accountability. Without such characteristics, the law risks becoming a powerless symbol lacking the authority to safeguard personal data rights.

Substantive Justice and the Power Imbalance of Data Subjects

The second issue lies in the lack of effective and proportional redress mechanisms for victims of data breaches. In practice, many individuals affected by data leaks, such as those involved in illegal lending, identity theft, or national ID leaks have no clear access to legal remedies, either material or immaterial.

Gustav Radbruch's trichotomy of law underscores the balance between justice, legal certainty, and utility. While the PDP Law prescribes administrative and criminal sanctions, it does not provide clear and accessible pathways for individuals to claim damages. In fact, in Supreme Court Decision No. 615 K/Pdt/2021, a personal data breach lawsuit was dismissed due to the plaintiff's inability to prove direct harm, setting an evidentiary burden that is arguably too high for ordinary data subjects (Radbruch, 1950).

Fadli (2020) argues that this indicates the absence of substantive justice for affected citizens. The PDP Law should be supplemented with mechanisms for class action suits, legal aid for victims, and the establishment of a data breach fund accessible to groups. Without this, the law merely preserves structural inequality between powerful data processors (e.g., corporations and platforms) and vulnerable individual users.

Also, there is a report from Indonesia's National Law Development Agency (BPHN) notes that violations in the marketplace sector are often driven by poor consumer literacy and the lack of compliance by platforms with core data protection principles. This finding reinforces the urgency of strengthening enforcement through a digital ethics framework (Priliasari, 2022).

Technological Ethics and the Challenge of Automation: Toward Algorithmic Oversight

In the era of artificial intelligence and automated data systems, critical decisions such as legal, financial, and social are increasingly made by opaque algorithms. Unfortunately, Indonesia's PDP Law does not explicitly recognize the right to explanation or the right to object to automated decision-making.

Philosophically, control over one's personal data is not merely a question of administrative regulation but it touches the core of human autonomy. Immanuel Kant (1797) asserts that the law must safeguard individual freedom as a manifestation of rational moral agency. Similar with Warren and Brandeis, they introduced the concept of privacy as "the right to be let alone," a notion that has become the normative foundation for data protection in the modern legal era (Warren & Brandeis, 1890).

From a behavioral law perspective, individuals often consent to data processing without fully understanding the consequences, simply following platform-driven defaults (Sunstein & Thaler, 2008). Worse still, as Foucault describes in his theory of the digital panopticon, algorithmic systems create a silent form of surveillance where individuals are constantly monitored without knowing who watches or how (Foucault, 1975).

Giovanni De Gregorio (2021) argues that the digital era requires an expansion of constitutional protections into the realm of cyberspace: a framework known as digital constitutionalism. In the context of the PDP Law, such a framework is not yet fully reflected, particularly in the areas of algorithmic accountability and the right to explanation. Solove (2008) further classifies privacy violations into categories such as information processing and dissemination, which highlights how Indonesia's PDP Law still lacks detailed protection on profiling and data inference.

Kurniawati (2021) warns that without an ethical framework embedded in regulation, data processing may be weaponized for discrimination and exclusion especially in credit scoring, insurance eligibility, or AI-based recruitment. Hence, integrating technological ethics into legal norms becomes essential: including algorithmic audit requirements, the obligation to disclose decision logic, and the legal right for users to challenge automated outcomes.

These findings collectively show that personal data protection cannot rely solely on formal legal articles. It requires a living institutional soul, a substantive sense of justice, and embedded ethical principles in the design of digital law. Without these pillars, the law will remain a static artifact detached from the evolving social realities it is meant to protect.

Comparative Institutional Models: Lessons from the EU and United States

To strengthen institutional design, Indonesia could draw valuable lessons from comparative models. The European Union's General Data Protection Regulation (GDPR) mandates that each member state establish an independent Data Protection Authority (DPA) empowered to monitor and enforce compliance. These DPAs are coordinated under the European Data Protection Board (EDPB), which facilitates consistency and cooperation across jurisdictions. In Article 22 of the GDPR explicitly prohibits decisions based solely on automated processing, including profiling, that produce legal effects concerning a data subject or significantly affect them, except under strict conditions. This serves as a key normative safeguard against algorithmic harms. Unfortunately, Indonesia's PDP Law lacks an equivalent provision, despite the growing prevalence of automation in sectors such as digital finance, employment, and social governance. The GDPR also outlines a clear framework for cross-border cases, complaint mechanisms, and binding decisions, offering a model of accountability that Indonesia has yet to match. In contrast, the United States applies a sectoral model, where agencies like the Federal Trade Commission (FTC) oversee data privacy within consumer protection and trade practices. While the U.S. lacks a federal omnibus privacy law, its strong enforcement actions and case-by-case remedies highlight how institutional authority can still be assertive in protecting user rights. Indonesia's PDP implementation could benefit from combining the structured independence of the EU model with the pragmatic enforcement approach of the U.S.

Critical Reflections and Adaptive Pathways for Indonesia

While lessons from the EU and U.S. provide clear regulatory blueprints, Indonesia's legal, political, and cultural context demands a carefully tailored approach. This section proposes a hybrid institutional framework and outlines key legal-political considerations for ensuring the PDP Law evolves into an effective instrument of digital rights protection.

Indonesia's PDP Law (Law No. 27/2022) currently mandates the formation of a supervisory authority, but as of writing, such an institution remains unformed. The law does not yet provide sufficient details on the independence, structure, or enforcement powers of this body and then raising concerns about its future effectiveness.

Indonesia could adopt a hybrid model by embedding the institutional independence and cross-sector coordination found in the EU's DPA system; ensuring strong enforcement mandates modeled after the FTC's ability to intervene quickly and impose deterrent penalties; and mandating annual transparency reports, public disclosure of enforcement actions, and mechanisms for handling cross-border complaints, especially as Indonesia increasingly integrates with the global digital economy.

More fundamentally, Indonesia must recognize that institutional design cannot be detached from normative commitments to human rights, legal certainty, and procedural fairness. As Selznick (1969) reminds us through his theory of responsive law, institutions must be not only structurally sound but also morally alert and socially attuned.

Ultimately, borrowing selectively from international models while tailoring them to local legal culture and digital realities may yield the most resilient and legitimate data protection framework for Indonesia.

V. CONCLUSION

The enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law) marks a significant milestone in Indonesia's journey toward safeguarding digital rights. However, in both substance and institutional design, the law still requires serious enhancement to meet the growing complexity of digital society. This study identifies five key areas that must be addressed to truly ignite the "spirit" of personal data protection in Indonesia.

First, from an institutional standpoint, the absence of an independent data protection authority has created a vacuum in legal enforcement. The PDP Law requires a supervisory body that is equipped with regulatory, investigative, and dispute resolution powers, grounded in public legitimacy and institutional autonomy.

Second, from the perspective of substantive justice, the lack of effective redress mechanisms for victims of data breaches shows the law's inability to protect data subjects fairly. The high burden of proof and absence of collective remedies have left many individuals vulnerable and without access to meaningful justice, as many victims are neglected in legal processes.

Third, from the standpoint of technological ethics, the law currently lacks explicit provisions and remains silent on issues such as algorithmic oversight and the right to explanation, the two core components of human rights protection in the age of artificial intelligence. This normative gap is especially dangerous in an age of automation, where opaque data-driven decisions increasingly impact people's rights and opportunities.

Fourth, international models such as the EU's GDPR and the U.S. FTC system offer valuable institutional benchmarks. The former provides a structured and independent supervisory framework, while the latter emphasizes assertive enforcement, even without a comprehensive federal law. Both systems highlight the importance of institutional clarity, coordination, and public accountability.

Journal of Business, Management, and Social Studies
Vol. 5, No. 3, August 2025, pp. 107-115
e-ISSN 2798-6209
DOI: https://doi.org/10.53748/jbms.v5i3.130
Available online at www.jbms.site

Fifth, and most critically, institutional reform in Indonesia must be rooted in normative values and adapted to local digital realities. As Selznick's theory of responsive law reminds us, institutions must not only be legally sound but also socially attuned and morally alert to the context in which they operate.

Taken together, these findings suggest that the PDP Law must not be treated merely as an administrative regulation. Instead, it should be understood as part of Indonesia's broader legal-political transformation toward a digital legal system that is responsive, just, fosters public trust in digital governance, and is grounded in human dignity.

Recommendations

Based on the above conclusions, this study offers the following recommendations:

(a) Establish an Independent and Inclusive Data Protection Authority, through either revision of the PDP Law or strong executive regulation, to ensure that enforcement is not limited to a technical ministry and also aimed to be a dedicated, autonomous and accountable public body.

(b) Strengthen Redress Mechanisms for Victims, by introducing provisions for class actions, legal aid in data breach cases, and the creation of a data breach compensation fund to ensure proportional restitution for affected individuals and groups.

(c) Integrate Technological Ethics into Legal Norms, including requirements for algorithmic audits, the right to explanation, and safeguards against automated decision-making bias and discrimination.

(d) Promote Digital Legal Literacy and a Culture of Law, by initiating public education campaigns and ensuring community participation in data protection policymaking platforms, to foster a living and sustainable legal culture and also reflects the values and needs of Indonesian society.

(e) Mandate Institutional Reviews and Transparency Reporting, including periodic evaluation of the supervisory body, publication of audit results, and open reporting of enforcement outcomes, to ensure democratic accountability and continuous adaptation.

These strategic actons are essential not only to ensure the PDP Law's practical effectiveness, but also with these reforms, the PDP Law can evolve beyond its current textual limitations to become a transformative legal instrument that advances digital justice for all Indonesian citizens rooted in constitutional justice, public accountability, and the ethical use of technology.

REFERENCES

Bygrave, L. A. (2014). Data Privacy Law: An International Perspective. Oxford University Press. https://global.oup.com/academic/product/data-privacy-law-9780199675555

De Gregorio, G. (2020). The rise of digital constitutionalism in the European Union. International Journal of Constitutional Law, 14(1), 41–70.

DPR RI (2021). Urgency of establishing a personal data protection framework. Info Singkat P3DI DPR RI. https://berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XIII-11-I-P3DI-Juni-2021-195.pdf

Ehrlich, E. (1936). Fundamental Principles of the Sociology of Law. Harvard University Press.

Foucault, M. (1975). Discipline and Punish: The Birth of the Prison. Pantheon Books.

Katadata.co.id (2023). Public trapped in data breach, 6 big banks profit. https://katadata.co.id/berita/nasional/64c8912d859d0/top-stories-publik-terjepit-kebocoran-data-pribadi-laba-6-bank-besar

Kant, I. (1797). The Metaphysics of Morals (Modern Edition). Cambridge University Press.

Kompas.com (2024, September 20). NPWP data breach raises concerns over government preparedness. https://nasional.kompas.com/read/2024/09/20/11370801/data-npwp-bocor-kesiapan-pemerintah-kelola-data-pribadi-dipertanyakan

Kompas.com (2024, September 20). Public institutions seem immune to law despite data breaches, experts say. https://nasional.kompas.com/read/2024/09/20/14565761/pengamat-kritik-instansi-pemerintah-alami-kebocoran-data-seolah-kebal-hukum

Kompas.com (2024, September 25). What role should a data protection authority play in the future? https://nasional.kompas.com/read/2024/09/25/05300001/menilik-peran-lembaga-pdp-dalam-mencegah-kebocoran-data-di-masa-depan

Lesmana, T. (2021). The urgency of the personal data protection law in ensuring data security as a fulfillment of privacy rights. JASS: Journal of Administrative and Social Science, 4(12), 3601–3605.

Priliasari, E. (2022). Legal Protection of Consumer Personal Data in E-Commerce According to Laws dan Regulations in Indonesia. Jurnal RechtsVinding, 12(2), 261–279.

Rahman, F. (2021). The legal framework for personal data protection in the implementation of electronic-based government systems in Indonesia. Jurnal Legislasi Indonesia, 18(1), 81–102.

Republic of Indonesia (1945). The 1945 Constitution of the Republic of Indonesia. State Secretariat. https://peraturan.bphn.go.id

Republic of Indonesia (2022). Law Number 27 of 2022 on Personal Data Protection. JDIH Ministry of Law and Human Rights. https://peraturan.go.id/id/uu-no-27-tahun-2022

Selznick, P. (1969). Law, Society, and Industrial Justice. Russell Sage Foundation.

Solove, D. J. (2008). Understanding Privacy. Harvard University Press.

Stahl, F. J. (n.d.). The Doctrine of Law and State (Translated ed.). (Printed source).

Sunstein, C. R., & Thaler, R. H. (2008). Nudge: Improving Decisions about Health, Wealth, and Happiness. Yale University Press.

Supreme Court of Indonesia (2021). Decision No. 615 K/Pdt/2021. https://putusan3.mahkamahagung.go.id

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.