



Legitimate Interests Under the GDPR and International Human Rights Law: A Proportionality Critique

Febrida Himni Ilmi¹, Johni Najwan², Akbar Kurnia Putra²

¹Doctoral Student in Law, Faculty of Law, Universitas Jambi, Jambi, Indonesia.

²Faculty of Law, Universitas Jambi, Jambi, Indonesia.

*Corresponding author : febyhimni@gmail.com

Submitted	: 19-05-2026	Accepted	: 23-09-2026
Reviewed	: 31-06-2026	Published	: 28-09-2026

Abstract

Background: The concept of legitimate interests as a basis for the lawful processing of personal data occupies a unique and vulnerable position in international data protection law. The GDPR formally adopts this concept under Article 6(1)(f); however, its operationalization raises fundamental questions regarding the adequacy of the doctrine of proportionality in protecting informational self-determination as a human right under Article 17 of the ICCPR and regional human rights instruments. **Methodology:** This article employs a normative juridical method integrating international human rights law analysis, the doctrine of proportionality, comparative legal analysis, and doctrinal analysis of judicial decisions. **Purpose:** This study critically examines whether the formal proportionality model underlying the legitimate interests framework in the GDPR can protect fundamental rights under conditions of radical informational asymmetry, surveillance capitalism, and data colonialism that characterize the global digital economy. **Findings:** The analysis shows that the GDPR proportionality model, although sophisticated, contains structural weaknesses when applied to diverse socio-economic contexts. The proposed framework consists of a mandatory three-step test, a Legitimate Interests Assessment (LIA), an anti-catch-all doctrine, and an allocation of the burden of proof based on international human rights law. **Originality/Novelty:** This article advances three arguments: first, the normative uncertainty of the GDPR legitimate interests clause challenges its adequacy as an international model; second, the transplantation of a proportionality-based balancing model without adequate institutional prerequisites risks creating accountability gaps; third, in the context of surveillance capitalism as data colonialism, a rights-first proportionality framework is required.

Keywords: legitimate interests; informational self-determination; proportionality; data colonialism; global south.

Abstrak

Latar Belakang: Konsep kepentingan yang sah sebagai dasar legitimasi pemrosesan data pribadi menempati posisi yang unik dan rentan dalam hukum perlindungan data internasional. GDPR secara formal mengadopsi konsep ini dalam Pasal 6(1)(f), namun operasionalisasinya menimbulkan pertanyaan fundamental tentang kecukupan doktrin proporsionalitas dalam melindungi penentuan-diri informasional sebagai hak asasi manusia berdasarkan Pasal 17 ICCPR dan instrumen HAM regional. **Metodologi:** Artikel ini menggunakan metode yuridis normatif yang mengintegrasikan analisis hukum HAM internasional, doktrin proporsionalitas,



perbandingan hukum, dan analisis doktrinal putusan pengadilan. **Tujuan:** Penelitian ini secara kritis mengkaji apakah model proporsionalitas formal yang mendasari kerangka kepentingan yang sah dalam GDPR dapat melindungi hak-hak fundamental dalam kondisi ketimpangan informasional radikal, kapitalisme surveilans, dan kolonialisme data yang menjadi ciri ekonomi digital global. **Temuan:** Analisis menunjukkan bahwa model proporsionalitas GDPR, meskipun canggih, mengandung kelemahan struktural ketika diterapkan pada konteks sosial-ekonomi yang beragam. Kerangka yang diusulkan terdiri atas uji tiga tahap wajib, penilaian kepentingan yang sah (LIA), doktrin anti-tangkap-semua, dan alokasi beban pembuktian yang berpijak pada hukum HAM internasional. **Orisinalitas/Keunikan:** Artikel ini mengajukan tiga argumen: pertama, ketidakpastian normatif dalam klausul kepentingan yang sah GDPR menantang kecukupannya sebagai model internasional; kedua, transplantasi model keseimbangan berbasis proporsionalitas tanpa prasyarat kelembagaan yang memadai berisiko menimbulkan kesenjangan akuntabilitas; ketiga, dalam konteks kapitalisme surveilans sebagai kolonialisme data, diperlukan kerangka proporsionalitas yang mendahulukan hak (rights-first proportionality)

Kata Kunci: kepentingan hukum yang sah; penentuan-diri informasional; proporsionalitas; kolonialisme data; global south.

A. Introduction

Personal data has become the constitutive resource of twenty-first-century digital capitalism. Zuboff identifies the systematic extraction and commodification of behavioural data as the defining feature of what she terms surveillance capitalism a logic of accumulation that translates human experience into behavioural prediction products traded on platforms invisible to the individuals whose data drives them. Couldry and Mejias extend this analysis to its global dimension, characterising the relationship between platform corporations and data subjects as a new form of data colonialism: the structural appropriation of the human lifeworld for capital accumulation, mediated by digital infrastructure rather than territorial occupation.¹ Couldry and Mejias extend this analysis to its global dimension, characterizing the relationship between platform corporations and data subjects in the developing world as a new form of data colonialism: the structural appropriation of the human lifeworld for capital accumulation, mediated by digital infrastructure rather than territorial occupation.²

The legal concept of legitimate interest as a basis for personal data processing sits at the precise point of collision between these economic imperatives and the fundamental rights of individuals. Properly constructed, it may enable proportionate data use for socially valuable purposes; improperly constructed, it becomes an instrument of asymmetrical digital power. Indonesia's Personal Data Protection Law (PDP Law), enacted as Law Number 27 of 2022, formally adopts legitimate interest as a lawful processing basis in Article 20(f).³ The provision is normatively denuded: it contains no

¹ Aharon Barak, *Proportionality: Constitutional Rights and Their Limitations*, 1st ed., Cambridge Studies in Constitutional Law (Cambridge, U.K.; New York: Cambridge University Press, 2012), 32, <https://doi.org/10.1017/CBO9781139035293>.

² Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Culture and Economic Life (Stanford, California: Stanford University Press, 2019), 1–35, <https://doi.org/10.1515/9781503609754>.

³ Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP Law), Pasal 20 huruf (f). For doctrinal analysis of the six legal bases, see Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)* (Sinar Grafika, 2023), 112–35.

definition, no mandatory testing mechanism, no allocated burden of proof, and no substantive operationalization of the data subject's right to object. What Article 20(f) provides, in effect, is an uncircumscribed grant of discretion to data controllers a legislative choice whose constitutional and practical consequences this article examines critically.

This article employs a normative juridical method. The methodological framework consists of four interconnected components. Examination of Article 17 of the ICCPR, General Comments by the UN Human Rights Committee, and regional human rights instruments (ECHR Article 8, ACHR Article 11, African Charter Article 4) to establish the positive obligation of states to protect informational self-determination as a human right, Systematic analysis of the GDPR Article 6(1)(f), including secondary sources such as WP29 Opinion 06/2014 and EDPB Guidelines 06/2020, compared with other international and regional data protection frameworks and Examination of *ratio decidendi* from CJEU decisions (Google Spain, Planet49, Schrems II), EDPB decisions, and international human rights jurisprudence relevant to informational privacy and proportionality.

This article advances three claims that together constitute a new legal-theoretical intervention in international data protection scholarship. First, the normative indeterminacy of the GDPR's legitimate interest clause despite its three-part test and supervisory infrastructure challenges its adequacy as an international model for protecting informational self-determination as a human right. Second, the transplantation of the GDPR's proportionality-based balancing model into diverse legal systems without the institutional preconditions that give the European model its effectiveness will produce what this article terms an *accountability gap*: formal compliance with the outer structure of legitimate interest doctrine combined with systematic substantive deficiency in its protection of data subjects' rights. Third, the bare balancing model implicit in most legitimate interest frameworks including, to an extent, the GDPR's is theoretically insufficient in conditions of radical informational inequality: what international human rights law demands is not a neutral balancing test but a rights-first proportionality framework that begins from a presumption in favour of informational self-determination derived from binding international legal obligations.⁴

These arguments are developed through a normative juridical methodology that integrates international human rights law analysis, proportionality doctrine, comparative law, and doctrinal analysis of judicial decisions. The article deliberately positions the GDPR not as an unassailable model but as a test case for broader propositions about whether liberal proportionality models can deliver adequate protection of fundamental rights in the conditions of structural inequality, regulatory asymmetry, and platform dependency that characterise the global digital economy. The research is prescriptive rather than empirical: it formulates normative parameters for legitimate interest doctrine derived from international human rights law. All legal materials are analysed using deductive logical reasoning from international legal norms to operational principles for data protection governance.

⁴ Barak, *Proportionality*.

B. Discussion

1. *Informational Self-Determination as a Constitutional Right*

The doctrinal foundation of this article's normative framework is the concept of informational self-determination as a constitutionally protected fundamental right. The concept traces its modern lineage to the German Federal Constitutional Court's landmark *Volkszählung* decision of 1983, which recognized the right of every individual to determine, in principle, the disclosure and use of their personal data. That judgment established a constitutional principle of lasting global significance: that informational autonomy is a precondition for the exercise of all other fundamental rights, and that the state must provide a regulatory framework capable of protecting it against both public and private power.⁵ At the international level, Article 17 of the ICCPR provides the explicit foundation for this right, guaranteeing that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. The UN Human Rights Committee's General Comment No. 16 (1988) and subsequent jurisprudence have elaborated that this right extends to informational privacy, including the collection, storage, use, and dissemination of personal data. Regional human rights instruments Article 8 of the ECHR, Article 11 of the ACHR, and Article 4 of the African Charter on Human and Peoples' Rights provide analogous protections.⁶

This international human rights framing has decisive implications for the design of legitimate interest doctrine. A legal provision that confers unchecked discretion on data controllers to define the content of legitimate interest without objective normative parameters derived from international human rights law does not fulfil states' positive obligations under the ICCPR. As Westin's foundational account of privacy establishes, the capacity to control information about oneself is not a commodity preference to be traded against commercial interests in a market-style balancing exercise; it is a constitutive dimension of human dignity and political autonomy. Nissenbaum's theory of contextual integrity further sharpens this point: personal data flows are normatively appropriate when they match the norms of the context from which the data originates, and the legitimacy of data processing cannot be reduced to a simple cost-benefit calculus.⁷

In Indonesia, Articles 28G(1) and 28H(4) of the 1945 Constitution provide the explicit constitutional foundation for this right, guaranteeing protection of personal identity, dignity, and the right to have personal property under one's own control. Read together, and in the light of Indonesia's ratification of the International Covenant on Civil and Political Rights (ICCPR) under Article 17, these provisions impose on the state a positive

⁵ Indonesian 1945 Constitution Article 28G(1) and Article 28H(4); Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008), 171–185.

⁶ United Nations Human Rights Committee, *General Comment No. 16 (1988): Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, General Comment (New York: United Nations, 1988), 1–10, <https://www.refworld.org/docid/453883f922.html>; see also Rudi Natamiharja et al., "Patient Rights During the Covid-19 Pandemic: The Dilemma between Data Privacy and Transparency in Indonesia," *The Age of Human Rights Journal*, no. 19 (December 2022): 121–36, <https://doi.org/10.17561/tahrj.v19.7004>.

⁷ Couldry and Mejias, *The Costs of Connection*, 521–38.

obligation not merely to refrain from violating informational autonomy, but actively to protect it against interference by private data controllers.⁸

This constitutional framing has decisive implications for the design of legitimate interest doctrine. A legislative provision that confers unchecked discretion on data controllers to define the content of “legitimate interest” without objective normative parameters does not fulfil this positive obligation: it delegates the definition of constitutional rights protection to the very parties whose economic interests are structurally opposed to it. As Westin’s foundational account of privacy establishes, the capacity to control information about oneself is not a commodity preference to be traded against commercial interests in a market-style balancing exercise; it is a constitutive dimension of human dignity and political autonomy.⁹ Nissenbaum’s theory of contextual integrity further sharpens this point: personal data flows are normatively appropriate when they match the norms of the context from which the data originates, and the legitimacy of data processing cannot be reduced to a simple cost-benefit calculus. The commodification of personal data under surveillance capitalism directly threatens informational self-determination in a way that generic balancing models are ill-equipped to address. When Zuboff demonstrates that digital platforms extract behavioural data not primarily as a byproduct of service provision but as the primary product, the raw material for predictive behavioral modification, she reveals the structural inadequacy of a legal framework that asks only whether the controller’s interest “overrides” the data subject’s rights. Where data extraction is the business model, every processing activity generates a “legitimate” business interest to be weighed against individual privacy; the balancing test becomes an asymmetric exercise that systematically produces outcomes favorable to the powerful party.¹⁰

2. Proportionality Doctrine and Its Critical Limits in the Data Context

Proportionality, as developed by Alexy through the sequential application of the sub-principles of legitimate aim, necessity, and balancing in the strict sense, represents the most sophisticated available instrument for adjudicating conflicts between rights and competing social interests.¹¹ Barak’s development of the rationality requirement and his account of proportionality *stricto sensu* as a benefits-versus-costs analysis that must never be formally neutral because constitutional rights carry presumptive priority provide the normative architecture for the framework proposed in this article.¹² But

⁸ Rudy Rudy et al., “Implementation of Civil Rights against Vulnerable Groups in the Legal and Constitutional System in Indonesia,” *Hasanuddin Law Review* 8, no. 3 (February 2023): 299, <https://doi.org/10.20956/halrev.v8i3.4229>.

⁹ Alan Furman Westin, *Privacy and Freedom*, New edition (New York: IG Publishing, 2015), 7–40; Helen Nissenbaum, “Privacy in Context: Technology, Policy, and the Integrity of Social Life,” in *Privacy in Context* (Stanford University Press, 2009), 67–100.

¹⁰ Nadezhda Purtova, “The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law,” *Law, Innovation and Technology* 10, no. 1 (January 2018): 40–81, <https://doi.org/10.1080/17579961.2018.1452176>; Luciano Floridi, “Open Data, Data Protection, and Group Privacy,” *Philosophy & Technology* 27, no. 1 (March 2014): 1–3, <https://doi.org/10.1007/s13347-014-0157-8>.

¹¹ Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press, 2002), 66–69; Barak, *Proportionality*, 131–370.

¹² Mattias Kumm, *Political Liberalism and the Structure of Rights: On the Place and Limits of the Proportionality Requirement*, 2007; in George Pavlakos and Robert Alexy, eds., *Law, Rights and Discourse: The Legal Philosophy of Robert Alexy* (Oxford ; Portland, Or: Hart Pub, 2007), 131–66; Kai Möller, *The Global Model of Constitutional Rights* (Oxford University Press, 2012).

proportionality doctrine applied to legitimate interest assessment carries a fundamental tension that must be confronted rather than assumed away: it presupposes a relatively equal institutional contest between the party asserting a rights restriction and the party invoking fundamental rights protection. In the data economy, this presupposition fails.

The critical literature on proportionality doctrine identifies a structural limitation that is acute in the data context. Kumm observes that proportionality review, applied without adequate attention to power differentials, risks becoming a legitimating mechanism for rights restrictions rather than a constraint on them: the formalization of the balancing stage can produce the appearance of rational adjudication while concealing substantive bias in favor of the party with superior resources, information, and institutional access. In legitimate interest assessments conducted by data controllers about their own processing activities, this structural bias is not a contingent risk but a systematic feature: the party whose interests are to be weighed against those of the data subject is also the party conducting the assessment, documenting the outcome, and - in the absence of mandatory supervisory review - bearing no externally verifiable accountability for its conclusions. This is precisely the problem that mandatory normative parameters, documented LIA requirements, and constitutionally grounded burden allocation are designed to correct.

This article therefore proposes not the abandonment of proportionality doctrine but its constitutional recalibration: a rights-first proportionality model in which the balancing stage begins not from a neutral position but from a constitutional presumption in favour of informational self-determination, which data controllers must affirmatively rebut through documented, externally reviewable evidence. This recalibration reflects the theoretical insight, shared by Barak and the more critical strand of constitutional rights scholarship represented by Möller (2012), that the point of proportionality review is not to produce balance but to protect rights. Article 20(f) of the PDP Law - which authorizes personal data processing for the "fulfilment of other legitimate interests" - exhibits the defining features of what Fuller (1964) identified as a failure of legality: a rule so indeterminate that it provides no genuine guidance to those it purports to govern.¹³ Fuller's inner morality of law includes the requirement of clarity (*lex certa*) as a precondition for law's claim to authority: rules that do not enable their subjects to predict what conduct is legally required or permitted cannot function as law in any normatively meaningful sense. Article 20(f) fails this test comprehensively. A data controller confronted with the provision cannot determine, from its text, which interests qualify as "legitimate," how the necessity of processing is to be assessed, or what standard governs the weighing of its interests against those of data subjects. Regulatory indeterminacy of this magnitude is not a neutral condition; it systematically benefits the institutionally stronger party.

Four specific normative deficiencies compound the open-ended structure of Article 20(f). First, the provision contains no definition of "legitimate interest," leaving entirely to data controllers the identification of interests that qualify a structural invitation to self-serving interpretation. Second, no testing mechanism exists: unlike the GDPR's mandatory three-part test, the PDP Law provides no operational standard against which the validity of a legitimate interest claim can be independently assessed. Third, the burden of proof is unallocated: neither the PDP Law nor its implementing regulations

¹³ H. L. A. Hart, *The Concept of Law* (Oxford University Press, 1961), 79–99; Lon L. Fuller, *The Morality of Law* (Yale University Press, 1964), 39–94 (on the *lex certa* requirement as a foundational element of legality).

expressly require data controllers to document their reliance on legitimate interest before processing commences, which means that accountability is structurally deferred until a violation has already occurred. Fourth, the right to object is not operationalized: Article 9's general acknowledgment of data subject rights is not elaborated into a specific, accessible, and cost-free right to object to processing based on legitimate interest.¹⁴

The normative deficiencies of Article 20(f) constitute more than a drafting imperfection: they generate a structural constitutional risk. Under Articles 28G(1) and 28H(4) of the 1945 Constitution, the Indonesian state bears a positive constitutional obligation to protect informational self-determination as a component of human dignity and personal autonomy. That positive obligation is not discharged by the formal enactment of a personal data protection statute: it requires that the statute's substantive provisions be adequate to the task of genuine protection. A provision that delegates the definition of its own normative content to data controllers - who possess structurally superior institutional, informational, and economic resources - does not protect informational self-determination; it subordinates it to the discretion of those who benefit most from its absence.

This constitutional analysis generates a critical implication for the design of normative parameters. It is not sufficient to propose a balancing framework that treats the interests of data controllers and data subjects as formally commensurate: the constitutional order requires a framework that acknowledges the asymmetric weight of fundamental rights in the balancing exercise. The argument for a rights-first proportionality model is therefore not merely a policy preference; it is a constitutional inference from the state's positive obligation to protect human dignity against the predatory dynamics of surveillance capitalism. The urgency of this constitutional and doctrinal problem is illustrated by the regulatory environment in which the PDP Law's deficiencies operate. Table 1, compiled from official government documentation, records the pattern of personal data violations reported in Indonesia's e-commerce sector. It is reproduced here not as an empirical finding but as contextual evidence of the conditions under which the absence of normative parameters for legitimate interest produces real-world harm to fundamental rights.¹⁵

Table 1. Documented Personal Data Violations in Indonesian E-Commerce (2018-2024): Contextual Regulatory Background¹⁶

No.	Year	Nature of Reported Violation	Number of Cases Recorded
1	2018	Misuse of consumer data by e-commerce platforms	1,857
2	2019	Leakage of marketplace user account data	2,349

¹⁴ Bayu Sujadmiko et al., "The Concept of E-Voting Mechanism Based on Law of General Election and Information Security," *Jambe Law Journal* 3, no. 1 (November 2020): 19–36, <https://doi.org/10.22437/jlj.3.1.19-36>.

¹⁵ Ministry of Communication and Informatics of the Republic of Indonesia., *Report on Data Breach Incidents and Failures in Electronic System Protection for 2024* (Ministry of Communication and Informatics of the Republic of Indonesia, 2025), 29–33.

¹⁶ Ministry of Communication and Informatics of the Republic of Indonesia., 29–33.

No.	Year	Nature of Reported Violation	Number of Cases Recorded
3	2020	Use of data for advertising purposes without consent	3,256
4	2021	Leakage of consumer transaction and identity data	4,789
5	2022	Personal data violations on digital trading platforms	5,234
6	2023	Illegal access and distribution of consumer data	5,890
7	2024	Electronic system protection failures (data breach)	6,417

Source: Ministry of Communication and Information Technology, Republic of Indonesia (2025, pp. 29-33).¹⁷

The categories of violation recorded in Table 1 - particularly the large-scale use of consumer data for commercial advertising without consent, and the unauthorized distribution of personal data - represent precisely the processing activities most readily defensible under an untested legitimate interest clause.¹⁸ The doctrinal point is not that these violations are caused by the normative deficiency of Article 20(f), but that the provision's indeterminacy removes the legal standard against which the lawfulness of such activities could be assessed, and thereby creates conditions in which data controllers face no operative normative constraint on invoking legitimate interest as a universal justification for commercially motivated processing.

C. Comparative Analysis: The GDPR Model and the Risks of Transplantation

The GDPR's treatment of legitimate interest under Article 6(1)(f) represents the most developed normative framework for the concept currently available in positive law. Its architecture - an explicit balancing test requirement, detailed interpretive authority through the WP29 Opinion 06/2014 and EDPB Guidelines 06/2020, a developed supervisory enforcement infrastructure, and a body of CJEU jurisprudence that has progressively circumscribed the concept's scope - provides a genuine model for rights-protective legitimate interest governance. Table 2 maps the twelve key regulatory dimensions of that architecture against Indonesia's PDP Law.

Table 1. GDPR Legitimate Interest Framework: Regulatory Dimensions

Regulatory Dimension	GDPR Provision / Source	Key Content
Legal Basis	Art. 6(1)(f)	Explicit balancing test; Recitals 47-49 provide context

¹⁷ Ministry of Communication and Informatics of the Republic of Indonesia., 29–33.

¹⁸ Retno Kusniati, "Free, Prior, and Informed Consent Principles as Indigenous Peoples' Right: Soft Law or Hard Law?," *Jambe Law Journal* 7, no. 1 (July 2024): 169–93, <https://doi.org/10.22437/home.v7i1.350>.

Regulatory Dimension	GDPR Provision / Source	Key Content
Normative Definition	Recital 47, WP29 Opinion 06/2014	Operationalised through guidelines
Testing Mechanism	EDPB Guidelines 06/2020	Mandatory three-part test
LIA Documentation	Art. 5(2) accountability	Required before processing
Burden of Proof	CJEU jurisprudence	On data controller
Right to Object	Art. 21	Specific, mandatory notification
Supervisory Authority	Art. 51-59	Independent DPAs + EDPB
Risk-Based Approach	Art. 35	Mandatory DPIA for high-risk processing
Judicial Development	CJEU case law	Google Spain (2014), Planet49 (2019), Schrems II (2020)
Exclusionary Categories	EDPB Guidelines	Excludes processing where another basis available

Table 2. Comparative Normative Matrix: Indonesian PDP Law vs. GDPR

Regulatory Dimension	PDP Law Indonesia (UU No. 27/2022)	GDPR (Regulation EU 2016/679)
Legal Basis	Art. 20(f): open-ended clause; no definition or constraint	Art. 6(1)(f): explicit balancing test; Recitals 47-49 provide context and limitations
Normative Definition	Absent; entirely delegated to controllers	Operationalized through Recital 47, WP29 Opinion 06/2014, and EDPB Guidelines 06/2020
Testing Mechanism	None	Mandatory three-part test: Purpose → Necessity → Balancing
LIA Documentation	None required	Required before processing; part of accountability obligation under Art. 5(2)

Regulatory Dimension	PDP Law Indonesia (UU No. 27/2022)	GDPR (Regulation EU 2016/679)
Burden of Proof	Unallocated	On data controller: must demonstrate interest does not override data subject's rights
Right to Object	Art. 9: general; not operationalized for legitimate interest	Art. 21: specific, mandatory notification, and absolute in some contexts
Regulatory Guidelines	None; supervisory authority not yet operational	Binding EDPB Guidelines and WP29 Opinions; subject to CJEU review
Risk-Based Approach	Absent	Mandatory DPIA under Art. 35 for high-risk processing; risk-calibrated framework
Judicial Development	Negligible; courts default to tort law	Extensive: Google Spain (2014), Planet49 (2019), Schrems II (2020), Meta Ireland (2023)
Implementing Regulations	Government Regulations not yet addressing LI parameters	Integrated framework of Recitals, EDPB Guidelines, and national DPA decisions
Exclusionary Categories	None	EDPB: excludes processing where another basis applies; large-scale profiling restricted
Supervisory Authority	Mandated but not yet constituted or operational	Independent DPA per Member State; EDPB as supranational coordinator

Source: Authors' normative analysis.¹⁹

Yet even within the GDPR framework, the concept of legitimate interest retains an internal tension that the scholarly literature has been frank in acknowledging. Zafir-Fortuna (2021) observes that the three-part test, despite its sophistication, leaves significant room for self-serving interpretation in the necessity and balancing stages, particularly in the absence of strong ex-ante supervisory review.²⁰ Kuner and de Hert and

¹⁹ Authors' analysis based on Law Number 27 of 2022 on Personal Data Protection (2022), <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>; Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217)* (Brussels: European Commission, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf; European Data Protection Board, *Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR* (Brussels: European Data Protection Board, 2020), https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en.

²⁰ Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer International Publishing, 2017), <https://doi.org/10.1007/978-3-319-57959-7>; see also Orla Lynskey, *The Foundations of EU Data Protection Law*, Oxford Studies in European Law (Oxford, GB: Oxford University Press,

Papakonstantinou have both noted the risk of legitimate interest becoming the provision through which the GDPR's otherwise robust framework is progressively hollowed out, as data controllers invoke it as a residual basis for processing activities that cannot survive consent or contractual necessity analysis.²¹ These internal tensions are multiplied many times over in a transplantation context.

The scholarly literature on legal transplantation consistently demonstrates that the effectiveness of a legal rule depends critically on the institutional, political, and social context into which it is transplanted. Greenleaf and Ryngaert and Taylor have charted the global influence of the GDPR as a regulatory model, but both note that its effectiveness outside Europe depends on the presence of institutional preconditions that are not universally available.²² For the legitimate interest doctrine specifically, four institutional preconditions are necessary for the three-part test to function as a genuine rights protection mechanism rather than a formal compliance ritual: (a) an independent, adequately resourced supervisory authority with genuine enforcement powers; (b) a developed body of administrative law capable of subjecting supervisory decisions to judicial review; (c) a civil society and data rights community capable of providing the countervailing pressure that drives rights-protective enforcement; and (d) a judiciary with the doctrinal familiarity to engage in substantive proportionality review of legitimate interest assessments.

Indonesia currently lacks all four. The PDPA mandated by Chapter IX of the PDP Law has not yet been constituted. Administrative law review of data protection decisions remains embryonic. The civil society infrastructure for data rights advocacy, while growing, cannot match the institutional resources of major digital platform operators.²³ And Indonesian courts, as the Mahkamah Agung's default to general tort doctrine in the 2018 e-commerce case illustrates, have not yet developed a proportionality-based jurisprudence adequate to legitimate interest review. In this institutional environment, the adoption of the GDPR's balancing model without the normative parameters proposed in this article would produce precisely the accountability gap that this article identifies: data controllers invoking legitimate interest would face no operative constraint, while data subjects would nominally possess rights whose exercise is, in practice, inaccessible.

The argument that Indonesia requires a localized rather than directly transplanted legitimate interest doctrine is not an argument for lower standards of protection. It is an argument that the normative parameters appropriate to Indonesia's constitutional context, institutional capacity, and socioeconomic conditions must be more structural, more presumptive in favour of rights, and more demanding in their documentation

2015); Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217)*.

²¹ Christopher Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," *Bloomberg BNA Privacy and Security Law Report* (2012) February 6, no. 12 (2012): 1–11; Paul De Hert and Vagelis Papakonstantinou, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals," *Computer Law & Security Review* 28, no. 2 (April 2012): 130–42, <https://doi.org/10.1016/j.clsr.2012.01.011>.

²² Cedric Ryngaert and Mistale Taylor, "The GDPR as Global Data Protection Regulation?," *AJIL Unbound* 114 (2020): 5–9, <https://doi.org/10.1017/aju.2019.80>; G. Greenleaf, "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108," *International Data Privacy Law* 2, no. 2 (May 2012): 68–92, <https://doi.org/10.1093/idpl/ips006>.

²³ Andi Agus Salim et al., "Protecting Critical National Infrastructure Against Cyber Operations Under International Humanitarian Law: Lessons for Southeast Asia," *International Law Discourse in Southeast Asia* 5, no. 1 (July 2026): 296–329, <https://doi.org/10.15294/ildisea.v5i1.42796>.

requirements than the GDPR model - precisely because the institutional mechanisms that compensate for the GDPR model's remaining ambiguities are absent. Specifically, three modifications to the GDPR template are constitutionally and institutionally justified:

1. Constitutional presumption of primacy: In the Indonesian constitutional framework, informational self-determination under Articles 28G and 28H is not merely one interest among many. The PDP Law's implementing regulations should codify an explicit presumption that the data subject's right to informational self-determination takes constitutional priority in the balancing stage, and that this presumption can only be rebutted by documented, specific, and independently verifiable evidence that the controller's interest is compelling;
2. Mandatory prior review for high-risk processing: Given the absence of an operational supervisory authority, the normative framework must build in structural accountability mechanisms that do not depend on supervisory capacity. For high-risk processing activities invoking legitimate interest, a mandatory prior review mechanism - analogous to the DPIA under the GDPR but adapted to Indonesia's institutional context - should be required, with publication of LIA conclusions to enable civil society scrutiny.
3. Strict anti-catchall enforcement: The GDPR's anti-catchall principle, which is enforced through EDPB guidance and supervisory decisions, must in Indonesia be codified as a positive statutory obligation. Given the absence of a functioning supervisory authority, the statutory text itself must exclude any invocation of legitimate interest where consent or a more specific legal basis is available.

In a normative-juridical study, analysis of judicial decisions serves a doctrinal rather than evidentiary function: the *ratio decidendi* of courts adjudicating legitimate interest cases reveals the legal principles that have acquired juridical recognition, and which any normative parameters framework must reflect and advance. Table 3 presents the doctrinal analysis of five decisions from EU and Indonesian jurisdictions:

Table 3. Judicial Analysis: Ratio Decidendi in Legitimate Interest Cases

Case	Forum & Year	Legal Question	Ratio Decidendi	Doctrinal Implication
Google Spain SL v. AEPD (C-131/12)	CJEU, 2014	Does LI of a search engine operator override the right to erasure?	Fundamental rights of data subjects in principle take precedence over the economic interest of the controller. Balancing is mandatory and contextual. LI is not an absolute defence.	Establishes constitutional priority of fundamental rights in balancing. Normative parameters must build in the same presumption.

Case	Forum & Year	Legal Question	Ratio Decidendi	Doctrinal Implication
Planet49 GmbH v. Bundesverband (C-673/17)	CJEU, 2019	Can LI substitute for consent in marketing contexts?	LI cannot circumvent the consent requirement. Processing for direct marketing requires a specific and affirmative legal basis. Pre-ticked boxes are invalid.	Doctrinal foundation for the anti-substitution principle. Residual character of LI is non-negotiable.
Data Protection Commissioner v. Facebook Ireland (Schrems II, C-311/18)	CJEU, 2020	Does the Privacy Shield guarantee adequacy for LI-based cross-border transfers?	Necessity and proportionality must be satisfied in substance, not form. National security claims are not immune from proportionality review. Transfer instruments must guarantee genuine protection.	Proportionality is a substantive, not formal, requirement. Parameters must resist compliance theatre.
Meta Platforms Ireland v. DPC & EDPB (2023)	DPC Ireland & EDPB	Can systematic cross-border transfers be justified on LI grounds?	LI cannot justify systematic, repeated transfers that violate fundamental rights. LIA required per processing operation. EUR 1.2B fine.	Non-delegable burden of proof; concrete, operation-specific LIA required. Abstract invocation of business necessity is insufficient.
Supreme Court RI, No. 1441 K/Pdt/2018	Mahkamah Agung RI, 2018	Is use of consumer data without a lawful basis an unlawful act?	Use of personal data without lawful basis is an unlawful act (PMH) under Art. 1365 Civil Code. Controller bears burden of proving lawfulness. Material and immaterial damages awarded.	In the absence of normative parameters, Indonesian courts default to general tort law, producing less rights-protective and less certain outcomes.

Three doctrinal principles emerge with consistency across the decisions analyzed in Table 3, and each has direct implications for the design of normative parameters. First, courts treat the burden of proof as non-delegably allocated to the data controller: the party seeking to override data subjects' rights through a legitimate interest claim bears the full evidentiary obligation of demonstrating that the three conditions of the balancing test are satisfied. Second, the balancing exercise is substantive and contextual: courts refuse to accept abstract assertions of business necessity and require the specific processing activity to be assessed against the specific rights impact on the specific data subjects affected. Third, legitimate interest is treated as a strictly residual legal basis, not a general licence for commercially motivated processing: courts foreclose its use wherever a more appropriate legal basis exists. These principles are not merely the products of European judicial culture; they reflect the constitutional logic of proportionality doctrine applied to informational rights, and they provide the doctrinal foundation from which the normative parameters framework is constructed.²⁴

D. Comparative Analysis with International Human Rights Law

When assessed against international human rights law standards, the GDPR's legitimate interest framework reveals both convergences and gaps. The UN Human Rights Committee's General Comment No. 16 requires that any interference with privacy must be provided by law, pursue a legitimate aim, and be proportionate. The European Court of Human Rights' jurisprudence under Article 8 ECHR has elaborated a similar three-part test in cases such as *S. and Marper v. the United Kingdom* (2008) and *Big Brother Watch v. the United Kingdom* (2021). However, several gaps remain:

Human Rights Requirement	GDPR Implementation	Identified Gap
Law must be accessible and precise	GDPR Article 6(1)(f) with guidelines	Normative indeterminacy remains
Legitimate aim must be specific	Recital 47 provides examples	Catch-all risk persists
Necessity requires least intrusive means	Three-part test includes necessity	Self-interpretation by controller
Proportionality stricto sensu	Balancing test	No presumption in favour of rights
Effective remedy	Article 79	Dependent on judicial access

²⁴ Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD), Case C-131/12 (2014); Bundesverband Der Verbraucherzentralen Und Verbraucherverbände v. Planet49 GmbH (October 1, 2019), <https://curia.europa.eu/juris/liste.jsf?num=C-673/17>; Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (Schrems II) (July 16, 2020), <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>; European Data Protection Board, *Binding Decision 01/2023 on the Dispute Submitted by the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Facebook)* (European Data Protection Board, 2023), https://www.edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en.

Sources: Author's analysis based on ICCPR General Comment No. 16 and ECHR jurisprudence

E. The Normative Parameters Framework: A Rights-First Proportionality Model

The foundational design choice of the normative parameters framework proposed in this article is the rejection of a formally neutral balancing model in favour of a rights-first proportionality architecture. The constitutional logic of this choice flows directly from the positive obligation analysis developed in Section III: where the state has a constitutional obligation to protect informational self-determination, and where the structural conditions of the digital economy systematically advantage data controllers in any formally neutral balancing exercise, a balanced framework that treats commercial and constitutional interests as commensurate does not fulfil that obligation. The framework therefore begins from an explicit constitutional presumption that informational self-determination takes priority in the balancing stage, and places on data controllers the full burden of rebutting that presumption through documented, specific, and independently reviewable evidence.²⁵

This constitutional framing does not render legitimate interest inaccessible to data controllers with genuine and proportionate processing needs. It ensures that only such controllers - those who can demonstrate that their interests are specific, that their processing is strictly necessary, and that the rights impact is justified by the benefit produced - can lawfully rely on the basis. The framework is rights-protective without being rights-absolute; it channels legitimate interest to its proper scope rather than eliminating it. The three-part test operationalizes the rights-first proportionality architecture through a mandatory sequential assessment. Each stage carries a distinct doctrinal rationale grounded in the constitutional logic of proportionality: **Step 1 - Purpose Test:** The data controller must identify a specific, lawful, and non-pretextual processing purpose that is independently reviewable by the supervisory authority or a court. The constitutional rationale is Alexy's *legitimate aim* sub-principle: any restriction on a constitutional right must pursue an objective that is itself constitutionally permissible. Vague purposes, purposes that amount to restating a general commercial interest, or purposes that could equally well be served by seeking consent, do not satisfy this requirement. The stage operationalizes Fuller's *lex certa* requirement at the level of individual processing justifications: the purpose must be stated with sufficient precision to enable external evaluation.

Step 2 - Necessity Test: The data controller must demonstrate that the processing is the least privacy-intrusive means reasonably available for achieving the identified purpose. The constitutional rationale is the necessity sub-principle: rights restrictions must be minimized to what is strictly required. This requires the controller to document: (a) that no less intrusive alternative is available; (b) that data categories are limited to what is strictly necessary; and (c) that retention periods are minimized. The stage implements Barak's rationality requirement - the existence of a rational connection between means and purpose - and ensures that data minimization is a structural feature of legitimate

²⁵ European Data Protection Board (EDPB), *Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR*; See Also EDPB *Recommendations on Legitimate Interests* (EDPB, 2020), 30–40; Art. 5(2) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), L119 Official Journal of the European Union 1 (2016), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>; see also Barak, *Proportionality*, 233–70.

interest processing rather than an optional practice. **Step 3 - Balancing Test:** The constitutional presumption in favour of informational self-determination operates at this stage. The data controller must demonstrate that its legitimate interest is compelling enough to rebut that presumption, through documented assessment of: (a) the nature and sensitivity of the data; (b) the reasonable expectations of data subjects in the specific processing context - drawing on Nissenbaum's contextual integrity framework; (c) the likely impact on data subjects' rights, including downstream and algorithmic impacts; (d) the effectiveness of available safeguards; and (e) the accessibility of the right to object. The balancing test is not a neutral cost-benefit calculation; it is a constitutional evaluation that requires the controller to demonstrate, not merely assert, that the processing is proportionate in the constitutional sense.

The Legitimate Interest Assessment (LIA) functions as the accountability infrastructure of the normative parameters framework: the mechanism through which the rights-first proportionality model acquires external verifiability. The constitutional logic of the LIA requirement derives from Barak's account of the relationship between proportionality and accountability: proportionality review has no disciplinary function if the assessment is conducted invisibly and without a record that can be independently evaluated. The LIA must document the purpose test analysis, the necessity test analysis, the balancing assessment and its outcome, the safeguards applied, and the mechanism for the exercise of the right to object. It must be maintained as part of the controller's accountability records under the accountability principle, and must be available to the supervisory authority on request. In the institutional context of Indonesia, where ex-ante supervisory review is not yet possible, the LIA serves an additional function: it shifts accountability to an ex-ante self-assessment that is subject to ex-post scrutiny, creating a structural deterrent against frivolous or bad-faith legitimate interest claims.

The anti-catchall principle - which this article proposes should be codified as a positive statutory obligation in Indonesia's implementing regulations rather than merely articulated in supervisory guidelines - is not merely an interpretive constraint but an independent doctrinal safeguard against the systematic erosion of the PDP Law's more specific and rights-protective legal bases. Its constitutional logic derives from the positive obligation analysis: a legislature that has identified consent as the appropriate legal basis for a given category of processing cannot fulfil its constitutional obligation to protect informational self-determination if a residual provision can effectively substitute for consent without any equivalent protective regime.

The anti-substitution principle, deriving from the CJEU's analysis in *Planet49* and from EDPB Guidelines 06/2020, extends this logic to the specific context of marketing and behavioral profiling: data controllers whose business model depends on using personal data for targeted advertising cannot resort to legitimate interest as a substitute for the individual consent that their processing activities require. In the Indonesian context, where the absence of a functioning supervisory authority means that this principle cannot be enforced by regulatory guidance, it must be given statutory force in the implementing regulations to Article 20(f) of the PDP Law.

The normative parameters framework calibrates the rigor of the LIA to the risk level of the processing activity, acknowledging that not all legitimate interest processing carries the same potential for rights harm. For high-risk processing - including large-scale profiling, processing of sensitive data categories, and automated decision-making with significant effects - the framework requires a full Data Protection Impact Assessment

(DPIA) in addition to the LIA, and the implementation of enhanced safeguards including privacy by design measures as developed by Cavoukian.²⁶

The right to object must be operationalized as a substantive, not merely nominal, right: data subjects must be informed of the legitimate interest relied upon at the point of data collection, must be provided with a cost-free objection mechanism, and must receive a substantive response that either ceases processing or provides documented justification for continuing on compelling legitimate grounds. This operationalization mirrors Article 21 of the GDPR and gives practical content to the constitutional dimension of informational self-determination: the individual's right to control information about themselves must include the right to effectively challenge its use. The normative effectiveness of the proposed framework depends on institutional preconditions that do not yet fully exist in Indonesia, but whose establishment is itself a constitutional obligation of the state. The Personal Data Protection Authority (PDPA) mandated by Chapter IX of the PDP Law must be constituted as a genuinely independent body, free from executive and legislative interference, and resourced with the regulatory capacity to engage in proactive supervisory review rather than merely reactive enforcement. As Bennett and Raab (2006) have demonstrated through comparative governance research, the effectiveness of data protection law is a function not merely of its normative content but of the institutional infrastructure that implements and enforces it. Indonesia's constitutional commitment to data protection will remain nominal until the institutional architecture capable of giving that commitment operational force is in place. The normative parameters framework proposed in this article is designed to be operationally effective within the constraints of Indonesia's current institutional environment, but the long-term realization of informational self-determination as a constitutional right requires investment in supervisory capacity that is commensurate with the scale and sophistication of the digital economy it is designed to govern.

F. Indonesia as a Test Case for Global South Digital Governance

The scholarly significance of this article extends beyond its contribution to Indonesian data protection law. Indonesia represents, with its combination of large and rapidly digitalizing population, heavy platform economy dependency, newly enacted but institutionally immature data protection framework, and constitutional commitment to human dignity and fundamental rights, a paradigm case for a set of questions of global importance: how should developing economies with limited regulatory capacity design legitimate interest doctrine so that it provides genuine rights protection rather than a formal compliance facade? How should constitutional rights frameworks be adapted to govern the specific conditions of informational inequality produced by global digital capitalism? And how should proportionality doctrine be reconstructed to resist the systematic bias toward rights restriction that its formal-neutral application tends to produce in asymmetric power conditions? The normative parameters framework proposed in this article offers provisional answers to these questions: rights-first proportionality, mandatory and externally reviewable LIAs, statutory anti-catchall obligations, and institutional architecture designed to enable genuine supervisory capacity over time. These are not answers specific to Indonesia; they are contributions to

²⁶ Ira Rubinstein, "Regulating Privacy by Design," *Berkeley Technology Law Journal* 26 (2012): 1409–1456; Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario, 2009).

the global legal-theoretical project of constructing data protection frameworks adequate to the governance challenges of the twenty-first-century digital economy.

G. Conclusion

This article has examined whether the formal proportionality model underlying the GDPR's legitimate interests framework can adequately protect informational self-determination as an international human right. Through analysis of international human rights law (ICCPR Article 17, regional instruments), proportionality doctrine, and CJEU jurisprudence, the article has demonstrated that the GDPR's legitimate interest framework, while sophisticated, contains structural deficiencies when assessed against binding international legal obligations. The article has argued that the transplantation of proportionality-based balancing models into diverse legal systems without adequate institutional preconditions risks producing an accountability gap: formal compliance with the three-part test's external structure combined with systematic substantive deficiency in human rights protection. In response to these findings, the article has proposed a rights-first proportionality framework derived from international human rights law, comprising four normative parameters: a mandatory three-step test, a documented Legitimate Interests Assessment, an anti-catchall doctrine, and a human rights-grounded allocation of the burden of proof onto data controllers. This framework ensures that the balancing stage begins not from a neutral position but from a presumption in favour of informational self-determination derived from binding international legal obligations, which data controllers must affirmatively rebut through documented, externally reviewable evidence. The framework is rights-protective without being rights-absolute; it channels legitimate interest to its proper scope rather than eliminating it. For future research, three directions are recommended: first, empirical investigation of how data controllers in non-European jurisdictions interpret legitimate interest under the GDPR's influence; second, comparative studies of legitimate interest doctrine across international human rights systems; and third, institutional analysis of the conditions necessary for effective data protection supervision in developing economies. The findings of this article are offered not as a final word but as a theoretical and doctrinal foundation for continued integration of data protection law with international human rights law

Reference

- Alexy, Robert. *A Theory of Constitutional Rights*. Oxford University Press, 2002.
- Article 29 Data Protection Working Party. *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP217)*. Brussels: European Commission, 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
- Barak, Aharon. *Proportionality: Constitutional Rights and Their Limitations*. 1st ed. Cambridge Studies in Constitutional Law. Cambridge, U.K. ; New York: Cambridge University Press, 2012. <https://doi.org/10.1017/CBO9781139035293>.
- Bundesverband Der Verbraucherzentralen Und Verbraucherverbände v. Planet49 GmbH (October 1, 2019). <https://curia.europa.eu/juris/liste.jsf?num=C-673/17>.
- Cavoukian, Ann. *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, 2009.

- Couldry, Nick, and Ulises A. Mejias. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Culture and Economic Life. Stanford, California: Stanford University Press, 2019. <https://doi.org/10.1515/9781503609754>.
- Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II) (July 16, 2020). <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>.
- De Hert, Paul, and Vagelis Papakonstantinou. "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals." *Computer Law & Security Review* 28, no. 2 (April 2012): 130–42. <https://doi.org/10.1016/j.clsr.2012.01.011>.
- European Data Protection Board. *Binding Decision 01/2023 on the Dispute Submitted by the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Facebook)*. European Data Protection Board, 2023. https://www.edpb.europa.eu/our-work-tools/consistency-findings/binding-decisions_en.
- . *Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR*. Brussels: European Data Protection Board, 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062020-interplay-second-payment-services_en.
- European Data Protection Board (EDPB). *Guidelines 06/2020 on the Interplay of the Second Payment Services Directive and the GDPR; See Also EDPB Recommendations on Legitimate Interests*. EDPB, 2020.
- Floridi, Luciano. "Open Data, Data Protection, and Group Privacy." *Philosophy & Technology* 27, no. 1 (March 2014): 1–3. <https://doi.org/10.1007/s13347-014-0157-8>.
- Fuller, Lon L. *The Morality of Law*. Yale University Press, 1964.
- Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD), Case C-131/12 (2014).
- Greenleaf, G. "The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108." *International Data Privacy Law* 2, no. 2 (May 2012): 68–92. <https://doi.org/10.1093/idpl/ips006>.
- Hart, H. L. A. *The Concept of Law*. Oxford University Press, 1961.
- Indonesian 1945 Constitution.
- Kumm, Mattias. *Political Liberalism and the Structure of Rights: On the Place and Limits of the Proportionality Requirement*. 2007.
- Kuner, Christopher. "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law." *Bloomberg BNA Privacy and Security Law Report (2012) February* 6, no. 2012 (2012): 1–15.
- Kusniati, Retno. "Free, Prior, and Informed Consent Principles as Indigenous Peoples' Right: Soft Law or Hard Law?" *Jambe Law Journal* 7, no. 1 (July 2024): 169–93. <https://doi.org/10.22437/home.v7i1.350>.
- Law Number 27 of 2022 on Personal Data Protection (2022). <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>.
- Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford Studies in European Law. Oxford, GB: Oxford University Press, 2015.

- Ministry of Communication and Informatics of the Republic of Indonesia. *Report on Data Breach Incidents and Failures in Electronic System Protection for 2024*. Ministry of Communication and Informatics of the Republic of Indonesia, 2025.
- Möller, Kai. *The Global Model of Constitutional Rights*. Oxford University Press, 2012.
- Natamiharja, Rudi, Febryani Sabatira, Muhammad Fakihi, Orima Melati Davey, and Haidir Anam. "Patient Rights During the Covid-19 Pandemic: The Dilemma between Data Privacy and Transparency in Indonesia." *The Age of Human Rights Journal*, no. 19 (December 2022): 121–36. <https://doi.org/10.17561/tahrj.v19.7004>.
- Nissenbaum, Helen. "Privacy in Context: Technology, Policy, and the Integrity of Social Life." In *Privacy in Context*. Stanford University Press, 2009.
- Pavlakos, George, and Robert Alexy, eds. *Law, Rights and Discourse: The Legal Philosophy of Robert Alexy*. Oxford ; Portland, Or: Hart Pub, 2007.
- Purtova, Nadezhda. "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law." *Law, Innovation and Technology* 10, no. 1 (January 2018): 40–81. <https://doi.org/10.1080/17579961.2018.1452176>.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), L119 Official Journal of the European Union 1 (2016). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika, 2023.
- Rubinstein, Ira. "Regulating Privacy by Design." *Berkeley Technology Law Journal* 26 (2012): 1409.
- Rudy, Rudy, Rudi Natamiharja, Jalil Alejandro Magaldi Serna, and Ahmad Syofyan. "Implementation of Civil Rights against Vulnerable Groups in the Legal and Constitutional System in Indonesia." *Hasanuddin Law Review* 8, no. 3 (February 2023): 299. <https://doi.org/10.20956/halrev.v8i3.4229>.
- Ryngaert, Cedric, and Mistale Taylor. "The GDPR as *Global Data Protection Regulation*?" *AJIL Unbound* 114 (2020): 5–9. <https://doi.org/10.1017/aju.2019.80>.
- Salim, Andi Agus, Maulidina Sari, Nova Bela Dhyta, Ahmad Sholihin Muttaqin, and Try Hardyanthi. "Protecting Critical National Infrastructure Against Cyber Operations Under International Humanitarian Law: Lessons for Southeast Asia." *International Law Discourse in Southeast Asia* 5, no. 1 (July 2026): 296–329. <https://doi.org/10.15294/ildisea.v5i1.42796>.
- Solove, Daniel J. *Understanding Privacy*. Harvard University Press, 2008.
- Sujadmiko, Bayu, Iskardo P. Panggar, Ade Sofyansah, and Intan Fitri Meutia. "The Concept of E-Voting Mechanism Based on Law of General Election and Information Security." *Jambe Law Journal* 3, no. 1 (November 2020): 19–36. <https://doi.org/10.22437/jlj.3.1.19-36>.
- United Nations Human Rights Committee. *General Comment No. 16 (1988): Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. General Comment. New York: United Nations, 1988. <https://www.refworld.org/docid/453883f922.html>.
- Voigt, Paul, and Axel Von Dem Bussche. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing, 2017. <https://doi.org/10.1007/978-3-319-57959-7>.
- Westin, Alan Furman. *Privacy and Freedom*. New edition. New York: IG Publishing, 2015.