Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

LEGAL ASPECTS OF OPEN BANKING AND CUSTOMER DATA PROTECTION IN THE DIGITAL ERA

William Hendrik Reba[1]*, Silvester Magnus Loogman Palit[2], Tumian Lian Daya Purba[3], Jeremy Edbert Reba[4]
Cenderawasih University, Indonesia[1,2,3], Boston University School of Law, United States[4]
***Email Correspondence:** williamreba66@gmail.com

Abstract
Open banking represents a transformative innovation in the financial sector, enabling the secure exchange of customer financial data between banks and third-party service providers through Application Programming Interfaces (APIs). This study examines the legal framework governing open banking and personal data protection in Indonesia, emphasizing its alignment with key legal theories — namely, the Theory of Legal Protection, Theory of Justice, Theory of Legal Certainty, and Theory of Responsive Law. Employing a normative juridical method, this research analyzes statutory instruments, legal doctrines, and comparative regulations, particularly drawing insights from the European Union's Payment Services Directive 2 (PSD2) and General Data Protection Regulation (GDPR). The findings reveal that Indonesia's regulatory foundation — primarily based on the Personal Data Protection Law (Law No. 27 of 2022) and financial sector regulations issued by Bank Indonesia and the OJK — provides an essential starting point but remains fragmented and limited in enforcement. Major gaps exist in preventive and repressive protection, liability allocation, and technical standardization for data security. Integrating classical legal theories with core banking principles such as prudence, transparency, accountability, and consumer protection underscores the need for a responsive, principle-based regulatory model. This study concludes that Indonesia must strengthen its regulatory framework through detailed implementing regulations, adaptive governance mechanisms, and cross-institutional coordination to achieve a balance between innovation and data protection in the era of digital finance.

Keywords: Open Banking, Personal Data Protection, Legal Protection, Legal Certainty, Responsive Law, Financial Technology, Consumer Rights, Regulatory Framework, Prudential Principle.

INTRODUCTION

The digital transformation of the financial industry has fundamentally reshaped the operational and regulatory landscape of banking and financial services. The proliferation of digital technologies, data-driven innovation, and financial technology (FinTech) has created both opportunities and challenges for regulators and institutions worldwide. Among the most significant innovations arising from this digital revolution is the concept of open banking, a framework that enables banks and financial institutions to share customer financial data securely with authorized third-party service providers through Application Programming Interfaces (APIs). This paradigm seeks to enhance transparency, foster innovation, increase competition, and ultimately deliver more efficient and personalized financial services to consumers (Zachariadis & Ozcan, 2017).

Globally, open banking has emerged as a cornerstone of digital financial ecosystems, particularly following the implementation of the European Union's Payment Services Directive 2 (PSD2) in 2018. The PSD2 mandates banks to provide data access to licensed third-party providers with explicit customer consent, thereby breaking traditional monopolies over financial data. This regulatory shift has catalyzed financial innovation while also raising pressing questions about data privacy, legal liability, consumer protection,

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

and cybersecurity. Within this evolving global context, Indonesia is gradually transitioning toward open banking through regulatory initiatives such as Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology, and more recently, the Personal Data Protection Law (Law No. 27 of 2022), which provides a comprehensive legal framework for the protection of personal data, including financial data.

However, the implementation of open banking in Indonesia is still at an embryonic stage. Despite significant legislative progress, regulatory fragmentation, infrastructural limitations, and low levels of public awareness continue to hinder effective enforcement. The Personal Data Protection (PDP) Law recognizes privacy as a fundamental human right, aligning with Article 28G of the 1945 Constitution of Indonesia, yet the institutional mechanisms for its protection remain weak. These conditions create a legal environment characterized by uncertainty and potential inequity in balancing the interests of consumers, financial institutions, and technology providers.

To examine these challenges, this study draws upon several core legal theories — namely, the Theory of Legal Protection, the Theory of Justice, the Theory of Legal Certainty, and the Theory of Responsive Law — as analytical lenses for understanding the adequacy and direction of Indonesia's open banking framework.

The Theory of Legal Protection, as articulated by *Phillipus M. Hadjon* (1987), distinguishes between *preventive* and *repressive* legal protection. Preventive protection aims to prevent disputes through proactive regulation, while repressive protection focuses on resolving conflicts through sanctions and enforcement mechanisms. In the context of open banking, preventive measures would include establishing robust technical standards for data security and clear consent protocols, whereas repressive protection would require effective mechanisms for dispute resolution and penalties for data misuse. The balance between these two forms of protection is essential to safeguard consumers' rights while enabling financial innovation.

Building on this, *John Rawls'* Theory of Justice as Fairness (1971) provides a philosophical framework for addressing distributive inequalities in digital finance. Rawls' *difference principle* asserts that social and economic inequalities are justifiable only if they benefit the least advantaged members of society. Applied to open banking, this principle suggests that regulations must prioritize consumer welfare, particularly given the inherent asymmetry of power between consumers and financial institutions. Empirical and normative research supports this approach, emphasizing that data protection is not merely a technical compliance issue but a human rights imperative integral to maintaining dignity and fairness in the digital economy (Palit & Purba, 2025).

Furthermore, *Gustav Radbruch's* Theory of Legal Certainty (2006) underscores the necessity for clear, predictable, and enforceable legal norms. Legal certainty becomes paramount in open banking, which involves multiple actors — banks, third-party providers, and regulators — with potentially conflicting interests. Ambiguities in technical standards or liability allocation can lead to inconsistent application of law and weaken public confidence in the system. Thus, achieving legal certainty requires not only comprehensive

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

regulations but also institutional mechanisms that ensure coherent interpretation and implementation.

Complementing these classical theories is *Nonet and Selznick's* Responsive Law Theory (2003), which advocates for laws that adapt dynamically to social and technological change. Responsive law prioritizes substantive justice and social objectives over rigid formalism, recognizing that legal systems must evolve in tandem with innovation. In the rapidly evolving FinTech landscape, responsive legal frameworks — such as regulatory sandboxes introduced by the Financial Services Authority (OJK Regulation No. 13/POJK.02/2018)— allow for controlled experimentation and iterative regulation. These mechanisms embody adaptive governance, balancing innovation promotion with consumer protection.

Indonesia's open banking framework is being constructed within a complex legal ecosystem comprising multiple statutes and regulations. Core instruments include the Banking Law (Law No. 10 of 1998), the Financial Services Authority Law (Law No. 21 of 2011), and sector-specific regulations issued by Bank Indonesia and OJK. While these frameworks collectively aim to promote innovation and safeguard financial stability, their interconnections are often fragmented. The introduction of the PDP Law was a major step toward consolidating data protection norms, yet critical implementing regulations — such as technical standards for APIs, cross-sectoral coordination mechanisms, and enforcement procedures — remain incomplete.

From a comparative perspective, the European Union's PSD2 and General Data Protection Regulation (GDPR) offer instructive models. PSD2 defines specific categories of service providers — including Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) — and mandates strong customer authentication mechanisms. Meanwhile, the GDPR enshrines principles such as *lawfulness, fairness, transparency, data minimization, purpose limitation, accuracy, storage limitation, integrity, confidentiality,* and *accountability.* Together, these frameworks exemplify how detailed technical and procedural standards can promote both innovation and data protection. Indonesia's approach, in contrast, has yet to achieve equivalent precision, particularly in defining the scope of consent, liability, and cross-border data transfers.

Beyond theoretical and regulatory considerations, open banking intersects with foundational banking legal principles, including the principle of prudence, bank secrecy, transparency, accountability, and consumer protection. The *prudential principle*, enshrined in Articles 2 and 29(2) of the Banking Law, obliges banks to act with due care and diligence. In open banking, this duty extends to assessing and monitoring third-party service providers that access customer data. The principle of bank secrecy, found in Article 40 of the Banking Law, requires banks to maintain confidentiality of depositor information, yet open banking necessitates a reinterpretation of this duty in light of customer consent mechanisms.

The principle of transparency, articulated in OJK Regulation No. 1/POJK.07/2013, demands that consumers receive clear, accurate, and comprehensible information regarding data usage, third-party access, and consent revocation. The principle of accountability, codified in Article 28 of the PDP Law, mandates that both data controllers and processors

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

demonstrate compliance with data protection obligations. Finally, the principle of consumer protection requires that regulatory frameworks incorporate effective remedies, compensation mechanisms, and proportionate sanctions. However, existing Indonesian sanctions — a maximum fine of IDR 2 billion under the PDP Law — are modest compared to the GDPR's penalties of up to 4% of global annual turnover, raising concerns about deterrence and enforcement effectiveness.

The convergence of these theoretical, legal, and practical elements reveals persistent challenges in Indonesia's open banking ecosystem. First, preventive legal protection remains underdeveloped due to the absence of detailed technical standards and mandatory certification schemes for data security. Second, repressive legal protection mechanisms, such as administrative sanctions and consumer dispute resolution procedures, are inadequate for ensuring redress. Third, legal uncertainty persists because of fragmented and overlapping regulations. Fourth, accountability gaps in multi-stakeholder data ecosystems — where responsibility may be diffused among banks, third-party providers, and regulators — undermine consumer trust.

The need for a responsive and adaptive regulatory framework is therefore paramount. As open banking continues to evolve, Indonesia must shift from a fragmented regulatory model toward a principle-based and technologically adaptive system. This transformation requires coordination between regulatory authorities, the establishment of a unified national API standard, robust enforcement mechanisms, and a clear liability regime.

Against this backdrop, this research aims to analyze the legal framework for open banking in Indonesia through the lens of these interrelated theories and principles, identifying the extent to which existing laws provide effective legal protection for customer data. By integrating classical legal theory with contemporary digital challenges, the study seeks to contribute both theoretically and practically.

Theoretically, the research advances an interdisciplinary understanding of how normative legal principles — justice, certainty, protection, and responsiveness — can inform digital-era regulatory design. Practically, it offers policy recommendations to strengthen Indonesia's open banking ecosystem: establishing enforceable technical standards, designing proportional liability frameworks, enhancing preventive and repressive protection mechanisms, and institutionalizing adaptive governance through regulatory sandboxes and continuous regulatory review.

Ultimately, the integration of Legal Protection Theory, Justice Theory, Legal Certainty Theory, and Responsive Law Theory within the framework of banking legal principles presents a holistic approach to addressing the legal, ethical, and regulatory complexities of open banking in Indonesia. It reflects the necessary evolution of legal thought — from static regulation to responsive governance — ensuring that innovation and consumer protection progress hand in hand in the digital financial era.

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

METHOD

This research uses a normative legal research method or doctrinal legal research. Normative legal research is conducted by examining library materials or secondary data as a basis for research (Soerjono Soekanto, 2001).

The approaches used are the statute approach, the conceptual approach, and the comparative approach. The statutory approach is conducted by examining all regulations related to open banking and personal data protection. The conceptual approach is conducted by examining relevant legal theories. The comparative approach is conducted by comparing open banking practices in Indonesia with those of other countries such as the European Union and the United Kingdom.

Primary legal sources include Law Number 27 of 2022 concerning Personal Data Protection, Law Number 10 of 1998 concerning Banking, Law Number 21 of 2011 concerning the Financial Services Authority, Financial Services Authority (OJK) and Bank Indonesia regulations regarding financial technology, and international regulations such as GDPR and PSD2. Secondary legal sources include law books, scientific journals, and related research results. Tertiary legal materials include legal dictionaries and encyclopedias.

Data collection techniques were conducted through library research, reviewing legislation, legal literature, and scientific journals. Qualitative analysis was conducted using descriptive analytical methods, employing grammatical, systematic, historical, and teleological interpretations. This research employed deductive reasoning by applying legal theories to the concrete case of open banking.

RESULTS AND DISCUSSION

Preventive Legal Protection and the Prudential Principle

In the context of open banking, preventive legal protection plays a pivotal role in safeguarding consumer rights before disputes arise. According to *Phillipus M. Hadjon* (1987), preventive legal protection enables individuals to avoid potential harm through regulatory safeguards and administrative mechanisms. Applied to open banking, this principle requires the establishment of clear standards for data processing, security mechanisms, and consent procedures to ensure that customers maintain control over their personal data.

In Indonesia, preventive protection is primarily derived from the Personal Data Protection Law (Law No. 27 of 2022) and several sectoral regulations, including Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Service Providers and OJK Regulation No. 3 of 2023 on Payment Support Services. These instruments mandate data controllers to maintain the confidentiality, integrity, and availability of personal data. However, the absence of a uniform national API security standard and mandatory security certification for third-party providers creates vulnerabilities that undermine preventive protection.

The prudential principle, as stipulated in Articles 2 and 29(2) of the Banking Law, requires banks to conduct their operations with due care and diligence. Within open banking, prudence extends to ensuring that third-party service providers accessing customer data meet stringent security and compliance requirements. Nonetheless, existing Indonesian

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

regulations do not explicitly define the due diligence standards required of banks when collaborating with third-party providers. This regulatory gap leads to inconsistent practices and exposes consumers to risks such as unauthorized access, data breaches, and identity theft.

From *Gustav Radbruch's* Theory of Legal Certainty, this lack of detailed technical standards represents a deficiency in legal predictability and clarity. Radbruch emphasized that laws must not only exist but also be clear, enforceable, and consistent in application. Without such certainty, financial institutions face difficulty interpreting their legal obligations, and consumers remain uncertain about the protection of their data.

Thus, preventive legal protection in Indonesia's open banking framework can be strengthened through:

1. Establishing national technical standards for API security, covering encryption, authentication, and authorization protocols.
2. Requiring third-party certification and registration with an independent supervisory authority.
3. Implementing mandatory periodic audits to ensure continuous compliance with security and privacy obligations.
4. Developing a standardized consent framework, ensuring consumers understand what data are shared, for what purposes, and for how long.

Such reforms would operationalize the prudential principle and reinforce public trust in open banking initiatives.

Repressive Legal Protection, the Principle of Justice, and Consumer Protection

Repressive legal protection refers to mechanisms activated after a violation occurs, including administrative sanctions, dispute resolution, and judicial remedies. *Hadjon's* repressive dimension complements the preventive aspect by ensuring accountability and restitution when consumers' rights are violated.

The Personal Data Protection Law (PDP Law) provides both administrative and criminal sanctions. Article 57 stipulates administrative sanctions such as written warnings, temporary suspension of data processing, deletion of data, and monetary fines up to IDR 2 billion. Article 67 provides criminal penalties of up to six years' imprisonment or fines up to IDR 6 billion. While these sanctions represent progress, they remain modest when compared to the European Union's GDPR, which imposes penalties up to 4% of a company's annual global turnover. This disparity raises questions about the effectiveness of Indonesian sanctions in deterring large-scale data violations.

From the lens of *John Rawls'* Theory of Justice, equitable legal protection demands that laws serve to protect the most vulnerable parties—namely, consumers. The difference principle suggests that inequalities, such as the power imbalance between financial institutions and consumers, can only be justified if they benefit the disadvantaged. Accordingly, Indonesian regulations should ensure that consumers bear minimal liability for unauthorized transactions and that institutions assume greater responsibility for data misuse.

Under the EU's PSD2 framework, liability allocation reflects this principle. Article 74

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

of PSD2 limits consumer liability for unauthorized transactions to EUR 50, unless the consumer acted with gross negligence or fraud. In contrast, Indonesian law lacks an explicit liability regime specifying the division of responsibility between banks, third-party providers, and consumers. This ambiguity undermines justice and consumer confidence.

The principle of consumer protection, embedded in OJK Regulation No. 1/POJK.07/2013, reinforces consumers' rights to transparent information, equitable treatment, and accessible dispute resolution. However, implementation remains limited due to low public awareness and the absence of specialized digital dispute mechanisms.

To align Indonesia's framework with the principles of justice and consumer protection, several reforms are necessary:

1. Introducing a clear liability framework in open banking that limits consumer responsibility for losses.
2. Establishing a mandatory compensation mechanism for affected consumers.
3. Creating specialized dispute resolution bodies within OJK for data-related cases.
4. Increasing sanction severity to ensure deterrence and compliance, proportional to institutional capacity and turnover.

These reforms would translate the normative ideals of *Rawls'* justice theory into practical regulatory instruments that protect consumers and promote fairness in the digital economy.

Integration of the Principle of Confidentiality and Informed Consent

The principle of confidentiality, as enshrined in Article 40 of the Banking Law, obliges banks to safeguard depositor information. However, open banking introduces a structural tension between confidentiality and the need for controlled data sharing. The key to reconciling these principles lies in the mechanism of informed consent.

Article 20 of the PDP Law mandates that consent must be given explicitly, voluntarily, and for specific purposes. Consent must also be verifiable, allowing individuals to withdraw approval at any time. This principle ensures that customers retain autonomy over their personal data while enabling innovation within a regulated framework.

Nevertheless, the current practice of consent management in Indonesia remains rudimentary. Many institutions rely on broad or ambiguous consent clauses embedded within general terms and conditions, which consumers often overlook or misunderstand. This practice contravenes the spirit of the PDP Law and undermines the transparency principle established by OJK Regulation No. 1/POJK.07/2013.

To ensure compliance, regulators should mandate:

1. Granular consent mechanisms, enabling consumers to select specific categories of data to share.
2. Comprehensive information disclosure regarding data recipients, purpose, and duration of access.
3. Simplified revocation procedures for consumers to withdraw consent easily.
4. Mandatory notification for any changes in data use or third-party arrangements.

Such measures would harmonize the principles of bank secrecy, transparency, and

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

consumer autonomy, creating a balanced legal environment where open banking can thrive without compromising individual privacy.

Responsive Law and Accountability as Solutions to Regulatory Uncertainty

Technological innovation in financial services evolves faster than traditional regulatory mechanisms can adapt. *Nonet and Selznick's* Theory of Responsive Law provides a framework for addressing this challenge by advocating for adaptive, participatory, and principle-based regulation. Responsive law emphasizes flexibility, stakeholder engagement, and ongoing evaluation of legal norms in response to societal and technological developments.

In Indonesia, the regulatory sandbox mechanism introduced by OJK Regulation No. 13/POJK.02/2018 embodies this responsive approach. The sandbox allows financial innovators to test new products under regulatory supervision, providing insights for future rulemaking. Expanding this mechanism to cover open banking services would enable regulators to assess technological risks, consumer responses, and compliance capabilities before full-scale implementation.

Complementing responsive law, the principle of accountability (Article 28 of the PDP Law) requires data controllers and processors to demonstrate compliance with data protection obligations. Accountability is critical in open banking, where data flows through multiple entities, creating complex chains of responsibility. To operationalize accountability, regulators should require:

1. Joint liability frameworks among banks and third-party providers for data breaches.
2. Periodic compliance reporting to supervisory authorities.
3. Independent audits of data security practices.
4. Publication of transparency reports to build consumer trust.

These mechanisms would ensure that all actors within the open banking ecosystem bear collective responsibility for maintaining data integrity and consumer protection.

Comparative Insights from the European Union

The European Union's PSD2 and GDPR frameworks provide instructive lessons for Indonesia. PSD2 establishes a structured open banking ecosystem by defining clear categories of service providers — Account Information Service Providers (AISPs), Payment Initiation Service Providers (PISPs), and Card-Based Payment Instrument Issuers. It mandates Strong Customer Authentication (SCA) and comprehensive technical standards for APIs, ensuring security and interoperability.

Meanwhile, the GDPR enforces stringent principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. Enforcement under GDPR is robust, with supervisory authorities empowered to impose significant fines and corrective actions.

Indonesia can adapt several best practices from the EU:

1. Developing a centralized open banking directory to register and monitor authorized third-party providers.

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

2. Introducing mandatory technical API standards similar to the EU's SCA framework.
3. Strengthening enforcement capacity through an independent supervisory authority for data protection.
4. Adopting risk-based compliance mechanisms, where stricter requirements apply to entities processing sensitive financial data.
5. Enhancing public awareness programs to educate consumers on digital rights and data security.

Such adaptations would allow Indonesia to harmonize innovation with robust consumer protection, ensuring legal certainty and international competitiveness.

Synthesis and Policy Implications

Integrating the four theoretical perspectives — legal protection, justice, legal certainty, and responsive law — reveals that Indonesia's open banking framework remains fragmented but evolving. Preventive protection mechanisms are incomplete, repressive measures are modest, and accountability structures are weak. However, the foundational elements for reform already exist within the PDP Law and financial regulations.

To bridge these gaps, Indonesia must pursue a three-pronged reform strategy:

1. Substantive reform, by issuing detailed implementing regulations and liability frameworks.
2. Institutional reform, by strengthening coordination between OJK, Bank Indonesia, and a prospective data protection authority.
3. Procedural reform, through adaptive regulatory mechanisms and ongoing evaluation of emerging risks.

By adopting a responsive, principle-based approach grounded in fairness and certainty, Indonesia can develop a robust open banking ecosystem that supports innovation, ensures justice, and protects consumers in the digital era.

CONCLUSION

Based on an analysis integrating legal theories with banking legal principles in the context of open banking in Indonesia, this study concludes that the legal framework for open banking in Indonesia has a basic foundation through the PDP Law and OJK/Bank Indonesia regulations but still faces significant gaps in implementation.

From the perspectives of Legal Protection Theory, Justice Theory, Legal Certainty Theory, and Responsive Legal Theory, fundamental challenges exist in preventive and repressive protection, balanced risk distribution, certainty of technical regulations, and adaptation to technological developments. The integration of banking legal principles demonstrates that the principle of bank secrecy can be aligned with data transparency through a robust informed consent mechanism. Meanwhile, the principles of prudence, transparency, accountability, and consumer protection must be operationalized through clear technical standards, protective forms of responsibility, and effective oversight mechanisms.

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

REFERENCES

Bank Indonesia. (2021). *Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyelenggaraan Penyedia Jasa Pembayaran.* Jakarta: Bank Indonesia.

European Union. (2015). *Directive (EU) 2015/2366 on Payment Services in the Internal Market (PSD2).* Official Journal of the European Union.

European Union. (2016). *Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation – GDPR).* Official Journal of the European Union.

Hadjon, P. M. (1987). *Perlindungan Hukum Bagi Rakyat di Indonesia.* Surabaya: Bina Ilmu.

Hofmann, H., & Soriano, J. (2021). The legal foundations of open banking: Between innovation and regulation. *Computer Law & Security Review, 41*(1), 105524. https://doi.org/10.1016/j.clsr.2021.105524

Indonesia. (1998). *Law No. 10 of 1998 concerning Amendment to Law No. 7 of 1992 on Banking.* State Gazette of the Republic of Indonesia No. 182 of 1998.

Indonesia. (2011). *Law No. 21 of 2011 concerning the Financial Services Authority.* State Gazette of the Republic of Indonesia No. 111 of 2011.

Indonesia. (2022). *Law No. 27 of 2022 concerning Personal Data Protection.* State Gazette of the Republic of Indonesia No. 195 of 2022.

Indri, I. S. (2024). Regulatory sandbox and its implementation in financial technology innovation. *Journal of Law and Applied Science, 2*(1), 16–27. https://doi.org/10.33478/jlas.v2i1.16

Kerr, I., & Earle, J. (2018). Prediction, preemption, presumption: The legal aspects of predictive data analytics. *Computer Law & Security Review, 34*(3), 540–553. https://doi.org/10.1016/j.clsr.2018.01.007

Kuner, C. (2017). The Internet and the global reach of EU data protection law. *International Data Privacy Law, 7*(2), 76–89. https://doi.org/10.1093/idpl/ipx002

Mayer-Schönberger, V., & Cukier, K. (2014). *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* Boston: Houghton Mifflin Harcourt.

Nonet, P., & Selznick, P. (2003). *Law and Society in Transition: Toward Responsive Law.* New Brunswick, NJ: Transaction Publishers.

OECD. (2022). *Open Banking Policies and Data Governance in Asia.* Paris: OECD Publishing. https://doi.org/10.1787/9789264754301-en

Otoritas Jasa Keuangan (OJK). (2013). *Peraturan OJK Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.* Jakarta: OJK.

Otoritas Jasa Keuangan (OJK). (2018). *Peraturan OJK Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan.* Jakarta: OJK.

Otoritas Jasa Keuangan (OJK). (2023). *Peraturan OJK Nomor 3 Tahun 2023 tentang Penyelenggaraan Layanan Pendukung Pembayaran.* Jakarta: OJK.

Palit, S. M. L., & Purba, T. L. D. (2025). Legal perspective on data privacy protection as a human right in Indonesia. *Easta Journal of Law and Human Rights, 4*(1), 24–32. https://doi.org/10.58812/eslhr.v4i01.783

DOI: https://doi.org/10.54443/sibatik.v5i1.4161

Puschmann, T. (2017). Fintech and financial services: Disruptive innovation or incremental innovation? *Electronic Markets, 27*(4), 1–11. https://doi.org/10.1007/s12525-017-0266-2

Radbruch, G. (2006). *Rechtsphilosophie* (S. L. Paulson, Trans.). Oxford: Oxford University Press.

Rawls, J. (1971). *A Theory of Justice.* Cambridge, MA: Harvard University Press.

Soekanto, S., & Mamudji, S. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat.* Jakarta: Raja Grafindo Persada.

Thakor, A. V. (2020). Fintech and banking: What do we know? *Journal of Financial Intermediation, 41*(1), 100833. https://doi.org/10.1016/j.jfi.2019.100833

World Bank. (2021). *Open Banking: A Toolkit for Financial Regulators.* Washington, DC: World Bank Group.

Zachariadis, M., & Ozcan, P. (2017). The API economy and digital transformation in financial services: The case of open banking. *SWIFT Institute Working Paper No. 2016-001.*

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2020). Decentralized finance (DeFi). *European Banking Institute Working Paper Series, 80*(1), 1–45. https://doi.org/10.2139/ssrn.3571335

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Barberis, J. N. (2021). Regulating fintech: Lessons from Asia. *Asian Journal of Law and Economics, 12*(2), 305–329. https://doi.org/10.1515/ajle-2021-0013

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: PublicAffairs.

DOI: https://doi.org/10.54443/sibatik.v5i1.4161