E-ISSN: 2988-2125

JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

Open Banking and Regulatory Challenges in Indonesia

Muhamad Agung Dharmajaya
STAI YAPATA Al-Jawami, Bandung, Indonesia

ARTICLE INFO

Keywords:
Open Banking, SNAP, Financial Regulation, Personal Data Protection, Legal Challenges.

ABSTRACT

The acceleration of digitalization is driving the Indonesian financial sector to transform from a conventional operational model to an open banking ecosystem. This study aims to analyze the development of open banking implementation in Indonesia and identify key regulatory challenges faced in mitigating legal and cybersecurity risks. The research method used is a normative juridical approach with a qualitative-descriptive approach through secondary data analysis in the form of Bank Indonesia regulations, the Financial Services Authority (OJK), and related literature. The results in the first sub-chapter indicate that the implementation of open banking, guided by the National Standard for Open API Payments (SNAP), based on the 2025 Indonesian Payment System Blueprint (BSPI), has successfully increased financial inclusion and the efficiency of system integration between financial actors. However, the analysis in the second sub-chapter reveals significant regulatory challenges, including an expanded cyberattack surface due to imbalances in IT protection capacity, uncertainty about legal liability in the event of system failures, fragmented cross-sectoral oversight, and difficulties in synchronizing with the Personal Data Protection Law (PDP Law). This research concludes that advances in SNAP's technical infrastructure have not been matched by an adaptive legal framework, creating legal gaps that risk consumer harm. This research recommends that Bank Indonesia and the Financial Services Authority (OJK) formulate joint regulations, shift to a principles-based approach, and strengthen the capacity of supervisory technology to create a safe and sustainable digital financial ecosystem.

Email :
agungdharmajaya456@gmail.com

INTRODUCTION

The acceleration of digitalization has fundamentally changed the global economic landscape over the past decade (Danuri, 2019). This transformation has pushed the financial sector to abandon conventional practices and shift to a more open, adaptive, and technology-driven ecosystem. One of

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

the most transformative innovations to emerge from this wave of digitalization is the concept of open banking (Mutiasari, 2020).

Conceptually, open banking is a system that allows the sharing of customer financial data with third parties through an Application Programming Interface (API) with customer consent (Adinegoro & Winengko, 2020). This mechanism breaks down the information monopoly held by large banks. Consequently, it has created close integration between banks, financial technology (fintech) companies, and other industry players (Budiman et al., 2020).

Indonesia is one of the countries with the greatest potential for open banking growth in Southeast Asia (Awanti, 2017). Its archipelagic geography and high unbanked and underbanked populations make this innovation a strategic solution. Through open banking, access to financial services can be expanded exponentially to drive national financial inclusion targets (Siagian, 2015).

Responding to this trend, Bank Indonesia has launched the 2025 Indonesian Payment System Blueprint (BSPI) and implemented the National Standard for Open Payment APIs (SNAP) (Billiam et al., 2022). This step was taken to create technical and governance standardization in the interconnected payment ecosystem. This policy marks the beginning of a new era of structured open banking in the country (Ramadhoni & Santoso, 2023).

While offering high efficiency, the implementation of open banking is a double-edged sword (Chrity & Stephanus, 2018). The massive opening of access to financial data opens up new risks that are far more complex than those encountered in the traditional banking era. Threats to cybersecurity, data leaks, misuse of customer information, and even digital financial crime now lurk within the national financial ecosystem (Iswati, 2007).

The greatest challenge facing Indonesia today lies in the readiness and adaptability of the regulatory framework (Abubakar, 2022). Existing regulations often lag behind the rapid pace of financial technology innovation, which continues to evolve daily. Law enforcement authorities and financial supervisory agencies are often caught in a dilemma between allowing innovation to flourish or restricting it for security reasons (Amrillah, 2020).

Beyond technical issues, the issue of alignment with the Personal Data Protection Law (PDP Law) is a crucial debate (Hisbulloh, 2021). Clarity regarding the limits of customer consent and legal liability in the event of system failures between financial actors remains unclear. This legal uncertainty has the potential to harm consumers and undermine public trust in banking digitalization (Nirwana, 2022).

Although numerous studies have been conducted on financial technology, research focusing on the intersection between open banking and regulatory dynamics in Indonesia remains limited. This study aims to fill this gap by in-depth analyzing legal readiness and institutional challenges. The primary focus of this study is to evaluate the effectiveness of current regulations in mitigating open banking risks.

Based on this background, this study aims to map the challenges of open banking regulation in Indonesia and formulate policy recommendations that address these issues. Through this analysis, it is hoped that an ideal and balanced regulatory formula can be found, one that can stimulate the growth of financial innovation while providing strong legal protection for consumers.

METHOD

This study uses a normative legal research method with a descriptive qualitative approach to assess the regulatory readiness of open banking in Indonesia. The approaches employed include a statute approach and a conceptual approach (Soekanto, 2007). The primary data source is secondary data, consisting of primary and secondary legal materials. Primary legal materials include official regulations such as the Personal Data Protection Law (UU PDP), Bank Indonesia Regulations

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

concerning the National Standard for Open Payment APIs (SNAP), and Financial Services Authority (OJK) regulations. Meanwhile, secondary legal materials were obtained through library research of scientific books, accredited legal journals, theses, public documents, and financial industry reports relevant to the topic of open banking governance.

This study uses a normative legal research method with a descriptive qualitative approach to assess the regulatory readiness of open banking in Indonesia. The approaches employed include a statute approach and a conceptual approach. The primary data source is secondary data, consisting of primary and secondary legal materials. Primary legal materials include official regulations such as the Personal Data Protection Law (PDP Law), Bank Indonesia Regulations concerning the National Standard for Open API Payments (SNAP), and Financial Services Authority (OJK) regulations. Meanwhile, secondary legal materials were obtained through library research of scientific books, accredited law journals, theses, public documents, and financial industry reports relevant to the topic of open banking governance..

RESULT AND DISCUSSION

Implementation of Open Banking and API Standardization in Indonesia

The financial industry landscape in Indonesia has shifted radically from a conventional operational model to a dynamic digital ecosystem. This shift is driven by the accelerated adoption of smart devices, widespread internet penetration, and fundamental changes in consumer transaction behavior preferences. Facing this disruption, banking institutions can no longer isolate themselves within closed internal systems but are instead required to open up to cross-industry collaboration.

As a strategic foundation, Bank Indonesia (BI) formulated the Indonesian Payment System Blueprint (BSPI) 2025. This macro policy is designed to navigate the flow of digitalization in harmony with the stability of the national financial system. One of the main pillars mandated in BSPI 2025 is the integration of the digital economy and finance through the implementation of open banking.

Conceptually, open banking changes the paradigm of traditional banking data management. This system gives customers the right to securely share their financial data and transaction history with third parties. This data sharing mechanism is facilitated by an information technology bridge known as the Application Programming Interface (API).

Prior to uniform regulatory intervention by the monetary authorities, API implementation in Indonesia proceeded partially through bilateral cooperation schemes. Each bank independently built its API architecture based on its respective business interests with specific financial technology (fintech) partners. As a result, the domestic fintech market was filled with a wide variety of unconnected technical variations.

This lack of a common standard in the early days led to technological fragmentation that harmed the efficiency of the financial industry. Fintech companies and e-commerce players had to repeatedly modify their programming code architectures each time they wanted to connect with a new bank. This digital infrastructure adjustment process required high technology investment costs and prolonged product launch time to market.

Recognizing this structural inefficiency, Bank Indonesia took a progressive step by launching the National Standard for Open API Payments (SNAP). The introduction of SNAP marked the end of the era of fragmented bilateral API architectures. This regulation contains comprehensive guidelines covering technical aspects, governance, data standards, and layered security protocols for all payment service providers.

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

The implementation of SNAP had an immediate impact, resulting in a massive increase in operational efficiency in the financial sector. Through standardization of programming languages and API data structures, the time required to integrate banking systems with external platforms has been significantly reduced. The business partner onboarding process, which previously took months, can now be completed in a matter of days.

This standardization has also transformed the competitive landscape into a climate of mutually beneficial collaboration (coopetition). Conventional banks, which have advantages in liquidity and a loyal customer base, can now collaborate with agile fintechs to create user interface innovations. This synergy breaks down the rigid boundaries that have traditionally separated the formal and informal financial industries.

From a macroeconomic perspective, the acceleration of SNAP-based open banking is a vital instrument in increasing national financial inclusion. Indonesia faces massive geographical challenges, with millions of unbanked and underbanked residents. The presence of payment APIs facilitates the penetration of digital financial services into remote areas beyond the reach of traditional bank branches.

Through open banking, people can enjoy financial services that are seamlessly integrated into their daily activities. From automatically topping up your digital wallet, instant payments on e-commerce platforms, to consolidating balances from multiple bank accounts in a single third-party app, all of this convenience is made possible by secure, real-time data exchange via API.

The benefits of open banking also extend to the financing and productive lending sectors for Micro, Small, and Medium Enterprises (MSMEs). Open access to transaction data enables financing institutions to use alternative risk assessment methods (alternative credit scoring). Sales transaction histories on digital platforms can serve as a valid database to assess the creditworthiness of businesses without formal collateral.

In aggregate, the implementation of open banking provides a significant stimulus to the growth of Indonesia's digital economy. The smooth flow of money within the digital ecosystem reduces overall transaction costs at the retail level. This stimulates global and domestic digital trade volume, which in turn accelerates economic recovery and increases national Gross Domestic Product (GDP).

However, despite these potential economic benefits, the expansion of open banking implementation fundamentally alters the risk landscape of the financial industry. Opening data gateways to third parties expands the attack surface of banking security systems. Operational risks, once within the bank's internal controls, are now spread throughout the digital supply chain involving numerous external actors.

This phenomenon is forcing banks to structurally deconstruct their business models. Banks no longer act as the sole entity controlling the financial value chain (silo). They are transforming into providers of basic financial infrastructure (banking-as-a-service), whose business performance is highly dependent on the health of the interconnected digital ecosystem at the macro level.

This high interdependence between financial actors gives rise to new types of risks in the form of digital systemic vulnerabilities. A technical disruption on a leading fintech platform or a system failure at a payment gateway provider can have a domino effect. This problem has the potential to disrupt the operational stability of banks connected within the same API network.

This shift in the risk landscape underscores the inadequacy of conventional approaches to financial industry supervision. Monetary authorities are required to develop technology-based supervisory technology (SupTech) capable of monitoring API data traffic in real time. SNAP technical standardization must be balanced by dynamic operational compliance oversight.

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

Facts on the ground show that the level of readiness of financial institutions to adopt SNAP standards varies widely. Large banks with strong core capital generally encounter no significant obstacles in upgrading their IT infrastructure. In contrast, smaller banks, regional Islamic banks, and fintech startups often face limited capital and skilled human resources to meet the stringent security criteria set by SNAP.

Regulatory Challenges: Legal Loopholes, Cybersecurity, and Alignment of the PDP Law

The adoption of open banking architecture brings highly complex legal consequences unprecedented in the history of Indonesian banking law. While technical frameworks like SNAP have successfully standardized connectivity, the regulatory aspect faces the challenge of catching up with the law (lagging regulation). The imbalance between the speed of technological innovation and legal development creates a gap that is vulnerable to exploitation.

The most pressing regulatory challenge lies in the cybersecurity domain. The open banking concept, which relies on API interconnection, inherently expands the cyberattack surface. Financial data, previously stored in banking data centers with multi-layered defenses, must now flow outward via the internet to third-party application systems.

Field analysis reveals a wide gap in cybersecurity capacity among financial actors in Indonesia. Large banks in KBMI categories 3 and 4 have the capital to establish 24-hour cybersecurity operations centers. In contrast, many fintech startups and rural banks (BPR) operate with minimal security systems, making them the weakest link in the ecosystem.

Current regulations are considered to lack rigid standards for mandating regular third-party cybersecurity audits by certified independent auditors. The SNAP framework does establish technical security guidelines, but the mechanisms for comprehensive penetration testing and vulnerability assessment of third parties are often left to the discretion of internal business agreements.

Weaknesses in API coding governance risk triggering advanced cyberattacks, such as Broken Object Level Authentication (BOL) parameter manipulation or mass data leaks through scraping methods. Failure to secure a single API path not only threatens a single platform but can also provide a gateway for hackers to infiltrate the core banking of the connected primary banking system.

The second regulatory challenge stems from Indonesia's fragmented financial oversight structure. The conventional banking industry is under the supervision of the Financial Services Authority (OJK), while retail payment systems, including SNAP standards, are controlled by Bank Indonesia (BI). On the other hand, fintech financing is supervised by the Financial Services Authority (OJK), but e-commerce platforms utilizing APIs fall under the jurisdiction of the Ministry of Trade and the Ministry of Communication and Digital (Kemenkomdigi).

This institutional fragmentation creates a legal gray area and potential sectoral egos that hinder cross-border supervision. When an open banking innovation involves vertical integration between banks, digital wallets, and marketplace platforms, oversight overlaps. This unclear authority boundary slows down legal enforcement when data governance violations occur.

To date, Indonesia does not have a comprehensive joint regulation between Bank Indonesia (BI) and the Financial Services Authority (OJK) specifically governing integrated supervision and sanctions procedures in the open banking ecosystem. This lack of an integrative legal framework complicates holistic compliance enforcement. As a result, industry players often have to meet multiple compliance requirements with two different institutions, each with bureaucratic procedures.

Another crucial legal issue arises in determining civil and criminal liability in the event of transaction system failures or data breaches. In traditional banking transactions, the legal

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

relationship is simple between the customer and the bank. However, in the open banking ecosystem, the data processing chain involves the originating bank, payment gateway providers, API aggregators, and third-party applications.

If a financial loss occurs due to cybersecurity or a personal data breach, customers face a highly complex legal burden of proving which party was negligent. Did the breach occur on the bank's server, due to weak encryption on the API, or due to negligence on the part of the third-party platform's security system? This uncertainty is exacerbated by standard clauses in application terms of service, which often unilaterally shift legal responsibility to the customer.

The introduction of the Personal Data Protection Law (PDP Law) introduces a new paradigm that must be aligned with open banking practices. The PDP Law grants individuals (data subjects) full rights over their data, including the right to delete, update, and revoke consent for the use of their financial data by any digital platform.

One of the main pillars of the PDP Law is the obligation for service providers to obtain explicit consent from data owners before processing or sharing their data. In the context of open banking, the regulatory system must ensure that customer consent is not general or hidden behind lengthy legal language. Consent must be given specifically for a particular type of data and for a clear processing purpose.

Operational challenges arise when customers wish to exercise their right to withdraw consent. In a data architecture already integrated through APIs, withdrawing consent requires sophisticated system coordination to ensure that customer data is completely deleted or access is cut off from all third-party servers. This data withdrawal clearing mechanism is not yet technically regulated in current open banking operational procedures.

The PDP Law also mandates the principle of data minimization, where data processors may only retrieve data strictly necessary to provide services. Conversely, for the purposes of credit scoring algorithms or targeted marketing, third parties tend to attempt to extract as much historical customer data as possible through APIs. Indonesian financial regulations still need to formulate strict limits on which categories of banking data may and may not be disclosed through open access. The legal status of "Data Controller" and "Data Processor" as defined in the PDP Law continues to spark debate in the open banking industry. Banks often position themselves as mere processors when distributing data at the request of customers, while third parties claim they only use the data for temporary services. This unclear status has direct implications for the magnitude of administrative fines that can be imposed under the PDP Law.

The PDP Law stipulates very high administrative fines for data protection violations, up to two percent of the company's annual revenue or turnover. For banking institutions, this penalty can reach significant levels and potentially disrupt the stability of the bank's core capital. Therefore, the uncertainty surrounding the implementation of this regulation has created anxiety among industry players about fully implementing open banking innovations.

The effectiveness of law enforcement under the Personal Data Protection Law (PDP) in the financial ecosystem also depends heavily on the existence and effectiveness of the Personal Data Protection Agency (PDP). Regulations need to map out how this PDP Agency will coordinate with the Financial Services Authority (OJK) and Bank Indonesia (BI) in resolving financial data disputes, given that financial data has special confidentiality characteristics that are regulated separately in the Banking Law.

From a legal dogmatic perspective, the concept of open banking also contradicts the principle of bank secrecy stipulated in Law Number 10 of 1998 concerning Banking. The Banking Law imposes criminal penalties on anyone who discloses customer savings data without a valid exception. Although open banking is based on customer consent, the conceptual tension between the past

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

banking secrecy legal regime and the current data disclosure regime requires a more stringent reconciliation of normative rules.

To bridge this legal gap, authorities need to intensify the use of adaptive financial technology innovation testing spaces, known as Regulatory Sandboxes. Through this framework, BI and the OJK can test new open banking business models involving complex data sharing with industry players before issuing generally binding regulations.

Facing the dynamic nature of API technology, a rigid legal approach based on detailed written rules (rule-based regulation) is considered ineffective and will quickly become outdated. Indonesia must shift towards principles-based regulation. The government establishes high-level standards for consumer safety, transparency, and cybersecurity, while the details of technical implementation are left to agreements by industry associations that are regularly monitored.

Consumer protection should not be limited to the technical aspects of data protection, but should also encompass aspects of literacy and rapid dispute resolution. The majority of Indonesians have a disproportionate level of digital financial literacy compared to their level of inclusion. Mandatory regulations should force open banking providers to provide an integrated complaint channel capable of resolving disputes over digital transaction losses within hours.

In refining its legal framework, Indonesian regulators need to learn from the implementation of international regulations such as the Revised Payment Services Directive (PSD2) in the European Union or the Consumer Data Rights (CDR) framework in Australia. This comparative study is crucial to ensure that national open banking regulations are not only secure domestically but also have globally interoperable standards to support future regional digital economic integration.

Table 1 Analysis Implementation and Challenges Regulation *Open Banking* in Indonesia

Dimensions Analysis	**Condition Existing & Implementation**	**Legal / Technical Challenges & Risks**	**Recommendation Policies & Solutions**
Infrastructure & Connectivity	Adoption National Standard Open API Payments (**SNAP**) based System Blueprint Indonesian Payments (**BSPI 2025**)	The gap capacity IT security between large banks (KBMI 3/4) and fintech startups or People's Economic Bank (BPR). API expands surface attack cyber (*attack surface*).	Enforcement obligation **cyber audit periodically by** independent auditors certified for all levels of *Third-Party Providers* (TPP).
Data Protection Governance	Starting to align with Constitution Personal Data Protection (**PDP Law**).	1. Mechanism withdrawal dynamic withdrawal *of* consent Not yet integrated in the API system. 2. There is potential excessive data retrieval that violates principle data minimization.	Development feature **transparent *consent management* on** the interface application as well as restrictions types of financial data that are allowed opened via API.
Legal Certainty & Responsibility	Connection law shift from bilateral (bank- customer)	**Chaos not quite enough answer legal** *liability* at the time	Standardization clause standard contract Work the same one that **forbids**

E-ISSN: 2988-2125
JURNAL RESTORASI
Hukum dan Politik
https://jurnal.seaninstitute.or.id/index.php/restorasi
Volume 1 No 02, 2023

	to multilateral (involving party third /fintech).	happen data leak or failure system. Proof scheme errors along the way chain digital supply is very complicated.	**diversion not quite enough answer unilateral** to customers, accompanied by scheme fast dispute *resolution*.
Architecture Supervision Institutional	Supervision separated between **Bank Indonesia** (system payment) and **OJK** (institution banking and fintech *lending*).	Occurrence **gray area** *of* supervision cross sectoral and sectoral ego risk moment handling integrative platforms (eg : banks integrated in *e-commerce*).	Formulation **Joint Regulation** between BI, OJK, and the *PDP* Supervisory Agency for supervision time real
Approach Regulation & Bankruptcy	Still dominated by the approach rigid based rule written detailed (*rule-based regulation*).	Rule written fast obsolete because rate innovation technology growing financial far more fast than the legislative process.	Transition going to **Regulation Based Principles** (*principle-based regulation*) and optimization digital testing platform (*Regulatory Sandbox*).
Protection & Literacy Consumer	Inclusion digital finance is on the rise rapidly until to population *unbanked/underbanked*.	Inequality between level inclusion (access) with level **literacy digital finance** society, triggering height risk engineering social *engineering*.	Obligation provision channel complaint integrated and educational together literacy massive cyber - finance by associations industry.

CONCLUSION

The implementation of open banking in Indonesia has achieved significant progress in terms of technological infrastructure. The National Standard for Open API Payments (SNAP), mandated in the 2025 Indonesian Payment System Blueprint (BSPI), has successfully ended the era of fragmented and inefficient bilateral connectivity [BSPI]. This programming language standardization has created an interoperable open financial ecosystem, accelerated strategic collaboration between conventional banks and fintech companies, and served as a key driver in expanding financial inclusion for populations underserved by formal banking services. However, these transformative technological achievements have not been matched by the readiness of an adaptive national legal framework. The acceleration of financial data interconnection has instead created new, multidimensional legal loopholes, particularly related to the expansion of the cyberattack surface due to the disparity in IT protection capacity between financial actors, the uncertainty in determining civil and criminal legal liability in the event of system failures, and the existence of gray areas in supervision due to institutional fragmentation between Bank Indonesia and the Financial Services Authority. Furthermore, the operationalization of consumer protection principles stipulated in the Personal Data Protection Law (PDP Law), such as explicit consent

management mechanisms and the right to withdraw customer consent instantly, still faces major synchronization challenges within the current open banking operational architecture..

REFERENCES

1. Abubakar, L. (2022). Penguatan regulasi: Upaya percepatan transformasi digital perbankan di era ekonomi digital. *Masalah-Masalah Hukum*.
2. Adinegoro, A., & Winengko, M. (2020). To close or not to close: Assessing the impact of open API to the bank performance in Indonesia. *Buletin Riset Kebijakan Perbankan*, *2*(1), 91-113.
3. Amrillah, M. U. (2020). Urgensi Pembentukan Undang-Undang Digital Banking Bagi Perbankan Syariah Di Indonesia. *Lex Renaissance*, *5*(4), 928-945.
4. Awanti, E. (2017). Analysis of The Financial Inclusion Effect on The Stability of The Financial System in South East's Developing Countries. *Jurnal Ilmu Ekonomi Terapan (JIET)*, *2*(2).
5. Billiam, B., Abubakar, L., & Handayani, T. (2022). The urgency of Open Application Programming Interface Standardization in the implementation of open banking to customer data protection for the advancement of Indonesian banking. *PADJADJARAN Jurnal Ilmu Hukum (Journal of Law)*, *9*(1), 67-88.
6. Budiman, H., Seminar, K. B., & Saptono, I. T. (2020). Formulasi Strategi Pengembangan Digital Banking (Studi Kasus Bank Abc). *Jurnal Aplikasi Bisnis Dan Manajemen (JABM)*, *6*(3), 489-489.
7. Christy, Y. E., & Stephanus, D. S. (2018). Pendeteksian kecurangan laporan keuangan dengan Beneish M-score pada perusahaan perbankan terbuka. *Jurnal Akuntansi Bisnis*, *16*(2), 148.
8. Danuri, M. (2019). Perkembangan dan transformasi teknologi digital. *Jurnal ilmiah infokam*, *15*(2).
9. Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum UNISSULA*, *37*(2), 119-133.
10. Iswati, S. (2007). Memprediksi kinerja keuangan dengan modal intelektual pada perusahaan perbankan terbuka di Bursa Efek Jakarta. *EKUITAS (Jurnal Ekonomi dan Keuangan)*, *11*(2), 159-174.
11. Mutiasari, A. I. (2020). Perkembangan industri perbankan di era digital. *Jurnal Ekonomi Bisnis Dan Kewirausahaan*, *9*(2), 32-41.
12. Nirwana, M. A. (2022). Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual. *AL WASATH Jurnal Ilmu Hukum*, *3*(2), 93-104.
13. Ramadhoni, M., & Santoso, H. (2023). Zero knowledge proof for snap (standar nasional open api pembayaran) in indonesia. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(3).
14. Siagian, P. (2015). Analisis Pengaruh Kinerja Keuangan Terhadap Perataan Laba Pada Perusahaan Perbankan Terbuka di Indonesia. *Binus Business Review*, *6*(1), 57-66.
15. Soekanto, S. (2007). Penelitian hukum normatif: Suatu tinjauan singkat.