Journal of Central Banking Law and Institutions, Vol. 3 No. 3, 2024, pp. 449 - 470
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
http://doi.org/10.21098/jcli.v3i3.251

BANK INDONESIA'S ROLE IN MITIGATING ISSUES OF MONETARY ECONOMIC SOVEREIGNTY AND HUMAN RIGHTS

Dara Salsabila
Centre for Legal and Regulation Consultancy, Universitas Padjadjaran
e-mail: darasalsabila2121@gmail.com

Abstract

Bank Indonesia has strategic authority to maintain the stability of monetary conditions in Indonesia through monetary policy. One concern is the risk is the emergence of shadow banking where fintech companies channel funds from the public. In the long term, this situation can impact the operational conditions of the banking system. One of Bank Indonesia's mandates is to supervise the provision of services by fintech companies (peer-to-peer lending) to align with the national financial and payment vision and mission, including establishing interlinks between fintech and banking to avoid risks posed by shadow banking. Interlinking works if each party is willing to share customer data. If Bank Indonesia requires fintech companies to share customer or user data, it must be based on clear and specific legislation. This is crucial because user data falls under personal data, and the state must guarantee the protection of its citizens' personal data. This article discusses the importance of legislation regarding the legitimacy of Bank Indonesia's authority to regulate interlinks between fintech companies and Bank Indonesia, as well as banking institutions, to avoid shadow banking. The article employs a normative legal approach using literature and legal sources.

Keywords: *history article, fintech companies, privacy, human rights, interlinks*

I. INTRODUCTION

The continuation of Indonesia's economic development has always required an evenly distributed, reliable, and just economic structure. This economy is managed through prudent control of the financial system, one aspect of which involves maintaining the stability of the Indonesian currency, the Rupiah. The preservation of the currency's value is the responsibility of Bank Indonesia, as part of its role in promulgating monetary policy. Various measures can be taken by Bank Indonesia to ensure the stability of the Rupiah, including controlling the money supply and interest rates. This authority is granted to the Central Bank of Indonesia (hereinafter referred as Bank Indonesia) under Law Number 23 of 1999 on Bank Indonesia (Law No. 23/1999). However, regulations established 25 years ago are often considered outdated and not keeping pace with the developments and dynamics of modern society. One such example is

the presence of technology-based collaborative financing services. Simply put, these services connect lenders and borrowers for conventional or Sharia-based financing directly through electronic systems using the internet. This financial technology utilises extensive Big Data, collecting and organising millions of data points that can be analysed based on various characteristics, including better customer segmentation, more customer-centric services, optimising operations, credit risk scoring while limiting transaction costs.[1]

The utilisation of the internet in consumer lending makes the financial and economic systems more inclusive. Technology-based collaborative financing services, commonly known as financial technology or fintech, have become increasingly prevalent, especially after the issuance of Financial Services Authority Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending and Borrowing Services. While this regulation has since been revoked, its issuance demonstrated the government's commitment to organising and improving the system of technology-based lending and borrowing services. The goal is to protect the rights and interests of users recognizing several factors that contribute to the proliferation of the fintech industry. Firstly, fintech simplifies financial transactions and can significantly impact the lower to middle-class population by providing easier access to loans. This contrasts with the traditional process of obtaining loans from banks, which tends to be more complex and time-consuming. Additionally, as startup entities, fintech companies are well capitalised, making them attractive to many consumers.

Another influential factor is the perceived flexibility of fintech companies compared to traditional lenders. The relatively limited regulations on the fintech industry create an environment that is conducive for entrepreneurs, encouraging them to venture into the sector. This perception of flexibility allows young entrepreneurs to channel their creativity into business and secure funding. According to statistical data from providers of technology-based peer-to-peer lending services, as of December 2023, there are a total of 101 service providers. These are divided into 94 conventional providers and seven Sharia-compliant providers.[2] In terms of total assets, conventional providers reached IDR 6,905,000,000,000, while Sharia-compliant providers reached IDR 139,000,000,000. This total asset figure indicates an increase compared to the same month in 2022, which consisted of IDR 5,378,940,000,000 from

[1] Ibrahim A. Zeidy, "The Role of Financial Technology in Changing Financial Industry and Increasing Efficiency in the Economy, Common Market for Eastern and Southern Africa," https://www.comesa.int/wp-content/uploads/2022/05/The-Role-of-Financial-Technology.pdf

[2] Otoritas Jasa Keuangan Republik Indonesia, "Statistik P2P Lending Periode Desember 2023," https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-P2P-Lending-Periode-Desember-2023.aspx ,13 February 2024.

conventional providers and IDR 133,640,000,000 from Sharia-compliant providers. The increase in total assets signified a significant and notable improvement.[3] The increase in total assets simultaneously indicates a rise in the amount of circulating money within these lending providers or fintech companies. However, it also suggests a diminishing role for traditional banks as lending institutions. The increasing role of fintech in providing payment and financing services illustrates the impact of digital innovation disruption in the Indonesian financial industry. This has the potential to replace the traditional financial services business model typically offered by banks, leading to what is commonly referred to as shadow banking. This situation may further result in disruptions to banking services such as credit distribution, remittances, and mutual funds.[4]

In the vision for the Indonesian payment system in 2025, the third point emphasizes the necessity of establishing interlinks between fintech companies and banking institution to avoid shadow banking risks through digital technology regulation, business collaboration, and ownership structures. This pertains not only to domestic fintech companies but also to international fintech lenders entering the Indonesian market, including Amazon, Alipay, and others. If a foreign fintech company enters Indonesia, the regulations related to fintech companies must be applied equally, without any exemptions. This development raises concerns for Bank Indonesia, as it is apprehensive of the impact on long-term stability of banking institutions. Interlinkage can be accomplished if each party is willing to open up customer data through the utilisation of technology in an open manner. From a banking perspective, this action is seen as a risk mitigation measure and a way to assert economic sovereignty over existing financial services.

However, if not regulated under clear and certain legal frameworks, this conflicts with the principle of protecting personal data as essential to human rights. If banks or relevant authorities force fintech companies to disclose user data without specific and clear regulations, it would violate the human rights of the companies' users. Apart from the lack of specific and clear regulations, this situation should also be examined from a moral standpoint and based on existing principles. Therefore, there is a contradiction between efforts to maintain economic sovereignty carried out by the banking sector and the protection of human rights in Indonesia. Balancing these concerns requires

[3] Otoritas Jasa Keuangan Republik Indonesia, "Statistik P2P Lending Periode Desember 2022," https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-Fintech-Lending-Periode-Desember-2022.aspx, 13 February 2024

[4] Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia 2025 Menavigasi Sistem Pembayaran Nasional di Era Digital," https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx 13 February 2024.

careful consideration of both economic objectives and the safeguarding of individual rights within a well-defined legal framework.

Based on the background above, further examination will be conducted of the issues identified below:

1. How does the massive operation of fintech companies in Indonesia influence the potential emergence of shadow banking that affects Indonesia's economic sovereignty?
2. How does Bank Indonesia's policy "guarantee the interlink between fintech and banking to avoid shadow-banking risks through digital technology regulation (such as APIs), business collaboration, and company ownership" relate to the legality of opening fintech user data to banking institutions?

II. DISCUSSION

A. The Expansion of Financial Technology Companies Has Led to the Emergence of Shadow Banking, Affecting the Economic Sovereignty of the Banking Sector

Financial Technology companies are entities that provide technology-based joint financing services or LPBBTI *(Layanan Pendanaan Bersama Berbasis Teknologi Informasi di Indonesian)*. LPBBTI is the provision of financial services to connect lenders with borrowers for conventional or Sharia-based financing directly through an electronic system using the internet, as defined in Article 1, Number 1 of the Financial Services Authority Regulation Number 10/POJK.05 of 2022 regarding Joint Financing Services Based on Information Technology (POJK No. 10 of 2022). Furthermore, Bank Indonesia states that a payment system is a set of rules, institutions, mechanisms, infrastructure, funding sources for payments, and access to funding sources for payments used to execute fund transfers to fulfil obligations arising from economic activity. Article 1, Number 4 of Bank Indonesia Regulation Number 23/6/PBI/2021 on Payment Service Providers (PerBI No. 23 of 2021) declares that Payment Service Providers are banks or non-bank institutions that provide services to facilitate payment transactions for users. These payment service providers are what is referred to as fintech companies. There are several forms of financial technology available, including:[5]

a. Peer-to-Peer (P2P) Lending and Crowdfunding
   Peer-to-Peer (P2P) lending and crowdfunding serve as platforms that bring together those in need of funds with individuals or entities willing

[5] Ratnawaty Marginingsih, "Financial Technology (Fintech) Dalam Inklusi Keuangan Nasional di Masa Pandemi Covid-19," *Moneter: Jurnal Akuntansi dan Keuangan* 8, no. 1 (2021).

to provide capital or investments. P2P lending can be understood as a service facilitating borrowing from the community. The funds can come from the community itself or from companies that establish the platform. These models leverage technology to create a direct connection between borrowers and lenders, often streamlining the lending process and providing an alternative to traditional banking channels.

b. Payment, Clearing, and Settlement
This fintech provides services in the form of a payment gateway or fintech digital wallets. The fintech payment gateway connects online businesses with banking institutions, allowing both parties to engage in business-to-business transactions.

c. Market Aggregator
This fintech service provides information, data, tips, and other content related to finance. This market aggregator serves as a feeder for potential users to explore other forms of fintech. It can also be utilised as a platform for fintech companies to publish and market their products to the public. This type of fintech can help users gather a wealth of information before making financial decisions.

Additionally, the sources of funding for this fintech lending platform consist of :[6]

a. Balance sheet lending denotes non-bank lenders utilising their own financial resources to extend credit to borrowers through electronic channels. Funding for these lenders may come from various sources such as retail notes, loan resales, securitization, warehouse lines of credit, and stable funds provided by debt and equity investors, including hedge funds, high net worth individuals, and traditional investment funds

b. Crowdfunding, also referred to as peer-to-peer lending, involves connecting lenders and borrowers using online platforms. These platforms usually gather detailed information from borrowers or investees, conduct thorough due diligence, assign credit scores, filter out impractical funding requests, set prices based on various risk levels, and facilitate payment transactions between the involved parties. In return for their services, these platforms charge fees.

In this section, the author narrows the discussion to Peer-to-Peer (P2P) Lending. Simply put, the funding scheme involves the prospective borrower establishing a loan account by filling out and submitting several electronic

[6] Ehrentraud, Johannes, Denise Garcia Ocampo, and Camila Quevedo Vega, "Regulating FinTech Financing: Digital Banks and FinTech Platforms," 27. FSI Insights on Policy Implementation. Basel: Bank for International Settlements, https://www.bis.org/fsi/publ/insights27.pdf, 2020.

documents through the designated platform, then the platform conducting authentication, verification, and validation processes for the personal data provided by the prospective borrower, and after internal processes are completed, a decision is made on whether the prospective borrower is eligible for funding and, if so, the credit limit that can be granted. With a straightforward scheme and relatively uncomplicated requirements compared to borrowing from traditional banking institutions, the Indonesian community consistently shifts towards obtaining loans from fintech companies. As the number of Indonesians making this transition to fintech increases, traditional banking institutions have lost potential customers. This situation has given rise to the potential emergence of shadow banking in Indonesia. Furthermore, with efficient lending capabilities, these fintech companies have become an alternative to traditional banking by offering similar services while saving on transaction costs from regulatory restrictions.[7] According to a doctrine from Rosadi, all service providers must ensure that they adhere to the principles of data protection regarding consumer privacy to safeguard their rights to the fullest extent.

Although fintech companies provide a solution to high borrowing costs, their services can pose a threat to the traditional banking sector. Given fintech companies' role in financial intermediation, there needs to be specific regulations, especially regarding accountability for any existing or potential claims. The second necessary guideline is to create a secure environment to attract funding from external investors.[8] With the large amount of money circulating in fintech companies, it can disrupt the banking system and may even lead to systemic bank failures. The severity of this condition is then known as shadow banking. The Financial Stability Board defines shadow banking as a credit intermediation system involving entities and activities outside the regular banking system. Commercial banks are financial institutions regulated by financial authorities and subject to established rules and regulations, ensuring that banks operate safely, fairly, and in accordance with sound financial principles.[9] The volume of Shadow bank financing appears to dwarf traditional bank financing.[10] The term shadow banking also includes the provision of financing by finance

[7] Ordonez G, Confidence Banking, paper presented at the 2010 Meeting Papers, 2010.

[8] Claessens, S. Pozsar Z., Ratnovski L & Singh, M. "Shadow Banking: Economics and Policy Priorities," https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Shadow-Banking-Economics-and-Policy-40132, 2012.

[9] Soehaditama, Josua Panatap, "Sustainability in Bank: Deposits, Investment and Interest Rate." *Formosa Journal of Sustainable Research,* 2, no. 5, 1069–1078. https://doi.org/10.55927/fjsr.v2i5.3912, 2023.

[10] Zoltan Pozsar et al., Federal Reserve Bank of New York Staff Reports, No. 458: Shadow Banking, 2010.

companies, hedge funds, money market mutual funds, non-bank government-sponsored enterprises, securities lenders, and investment banks.[11]

The shadow banking system is complex, with a multitude of nonbank agents, and many links to traditional banks and dealer banks.[12] The shadow banking system transforms debt instruments through securitization and tranching into safe, money-like claims. The securitization-based production of safe, short-term, liquid assets mimic the classic banking functions of credit, maturity, and liquidity transformation. Unlike in traditional banks, though, such lending takes the form of risk transfer (risk stripping) and is performed in steps along a chain of balance sheets.[13] Unlike commercial banks, which combine deposit creation and loan origination under one roof, the shadow banking system separates the intermediation process into different entities.[14]

Although fintech companies must implement effective risk management for all financial activities, such as lending money to borrowers, there is still a prevalence of defaults and other breaches of contract. Article 35 POJK No. 10 of 2022 states that fintech companies are obligated to implement effective risk management for their borrowers or customers for other financial services, which should include at least conducting a risk analysis of the funding proposed by users, verifying user identities and document authenticity, optimising the collection of distributed funds, facilitating the transfer of funding risk, and facilitating the transfer of risk related to collateral, if applicable.

The Financial Stability Board (FSB) states that there are several approaches to minimise the effects of shadow banking:

a. Conducting detection and mapping of existing shadow banking systems against cash flow data to understand the scale of industry activities and emerging trends;
b. Identifying shadow banking activities that have the potential to create vulnerabilities or systemic risks, such as non-bank maturity transformation, liquidity transformation, credit risk transfer, and leverage; and
c. Conducting a comprehensive assessment of systemic risk potential and existing legal regulations.

The role of legal regulations becomes significant when associated with Bank Indonesia's policy to implement interlinks between fintech and

---

[11] Steven L. Schwarcz, "Shadow Banking, Financial Risk, and Regulation in China and Other Developing Countries," GEG Working Paper 2013/83, The Global Economic Governance Programme, University of Oxford. https://www.geg.ox.ac.uk/publication/geg-wp-201383-shadow-banking-china-and-other-developing-countries.

[12] Stijn Claessens, Zoltan Pozsar, Lev Ratnovski, and Manmohan Singh, IMF Staff Discussion Note, SDN/12/12 December 4, 2012.

[13] Ibid.

[14] Kairong Xiao, "Monetary Transmission through Shadow Banks," *The Review of Financial Studies* 33, no. 6 (2020): 2379–2420, https://doi.org/10.1093/rfs/hhz112.

traditional banking by opening up customer data. The government, at the very least, emphasises principles in formulating guidelines against shadow banking, including:[15]

a. Focus: Regulatory measures should be carefully designed to target the externalities and risks the shadow banking system creates;
b. Proportionality: Regulatory measures should be proportionate to the risks shadow banking poses to the financial system;
c. Forward-looking and adaptable: Regulatory measures should anticipate and adapt to emerging risks;
d. Effectiveness: Regulatory measures should be designed and implemented in an effective manner, balancing the need for international consistency to address common risks and to avoid creating cross-border arbitrage opportunities against the need to account for differences between financial structures and systems across multiple jurisdictions.
e. Assessment and review: Regulators should regularly assess the effectiveness of their regulatory measures after implementation and make adjustments to improve them as necessary in the light of experience.

Preventive measures have been implemented by Bank Indonesia, which has formulated policies related to efforts to minimise the effects of shadow banking. As stated in point 3 of the Vision of the Indonesian Payment System (SPI) 2025, SPI 2025 ensures interlinkages between Fintech and banking to avoid shadow banking risks through the regulation of digital technology, including Application Program Interfaces (APIs), business collaboration, and ownership of companies.

Interlinkages can occur when each party is willing to open their customer data through the open utilisation of API technology. Collaboration between banks and fintech can take various forms, including financing patterns and guidance from banks to fintech entities. In this context, the interlinking of banks and fintech can mitigate the risks of shadow banking. However, the challenge lies in the legality of enforcing a prudent interlink policy, as it has not been explicitly stated in existing laws and regulations. Therefore, Bank Indonesia cannot enforce the mandatory opening of customer data by fintech companies without clear regulatory guidelines.

Although the relevant regulatory authorities are fundamentally aimed at preventing larger macroeconomic crises, it is acknowledged that it represents a form of economic sovereignty over Indonesia's economic resources carried out by Bank Indonesia. However, if not further addressed, the regulation of this could be perceived as Bank Indonesia accessing personal data of fintech

[15] Financial Stability Board, "Strengthening Oversight and Regulation of Shadow Banking Policy," 29 August 2013, https://www.fsb.org/wp-content/uploads/r_130829c.pdf, 13 February 2024.

customers without proper authorization. The position of fintech companies is not only as non-bank institutions providing financing and funding but also as entities collecting personal data from the public. Therefore, it is essential to establish clear regulations to govern practices that involve sensitive customer information.

Article 40 PerBI No. 23 of 2021, states that Bank Indonesia has the authority to request prospective Payment Service Providers to submit additional data and/or information related to institutional, capital, financial, risk management, and information system capabilities aspects in the licensing of Payment Service Providers. This authority, however, does not specify that Payment Service Providers or fintech companies are required to disclose customer data to Bank Indonesia.[16]

This is stated in Article 1, number 4 of Law Number 27 of 2022 on Personal Data Protection (Law No. 27/2022), which defines the data controller as any individual, public entity, and international organisation acting individually or jointly in determining the purpose and exercising control over the processing of personal data. This means that fintech companies are bound by regulations governing two sectors, namely the financial sector and the personal data protection sector. Customers of fintech companies are considered personal data subjects under data protection laws. Personal data subjects are individuals in whom personal data is inherent based on Article 1 number 6 of Law No. 7 of 2022. In Article 44, paragraph (1) of Financial Services Authority Regulation No. 10/2022 (POJK No. 10/2022), it is stated that the organiser (a fintech company) is obligated to: a. Maintain the confidentiality, integrity, and availability of personal data, transaction data, and financial data it manages from the time the data is obtained until the data is destroyed; b. Ensure the availability of authentication, verification, and validation processes that support repudiation in accessing, processing, and executing personal data, transaction data, and financial data it manages; c. Ensure that the acquisition, use, utilisation, and disclosure of personal data, transaction data, and financial data obtained by the Organizer are based on the consent of the owner of the personal data, transaction data, and financial data, unless otherwise specified by regulations; d. Notify the owner of personal data, transaction data, and financial data in writing in case of a failure to protect the confidentiality of personal data, transaction data, and financial data it manages. In this regulation, personal data is defined as any data about an individual, whether identified and/or can be individually identified or combined with other information, both directly and indirectly through electronic and/or non-electronic Systems.

[16] Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia (BSPI) 2025," https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx 15 February 2024.

However, requests for and opening of user or customer data conducted by the Financial Services Authority (*Otoritas Jasa Keuangan* or OJK) and Bank Indonesia differ. In the case of the Financial Services Authority, there is a legal basis for the opening of such data, as stated in Article 40 POJK No. 10 of 2022. This regulation declares that fintech companies can engage in data exchange cooperation to enhance the quality of jointly provided technology-based financial services, outlined in a data confidentiality agreement. Fintech companies must ensure that the data recipient complies with the data confidentiality agreement, which includes, at a minimum, the parties involved, types of data, data usage and disclosure, rights and obligations of the parties, responsibilities of the parties, and the duration of data usage and storage.

Furthermore, in paragraph (5), it is stated that the data exchange cooperation mentioned above must be reported to the Financial Services Authority, accompanied by the business licence from the authority when implementing the cooperation and the draft of the data confidentiality agreement. This paragraph contains the term "mandatory," indicating an obligation of fintech companies. This correlates with the authority issuing permits, namely the Financial Services Authority, so there is a causal and dependency relationship between fintech companies and the Financial Services Authority. This is different from Bank Indonesia's role, which until now does not have a legal basis for the exchange of data and information like the Financial Services Authority. It means that the exchange of information and personal data only occurs between the organiser (fintech company) and the prospective fund recipient or borrower, with no other parties involved in the process. However, the introduction of an interlink policy between fintech and traditional banking creates a linear relationship between the fund recipient, the organiser, and the bank. Yet, regulations regarding the permissibility of opening the personal data of fintech company customers are not yet available. Even though in PerBI No. 23 of 2021 Article 20 paragraph (2) it is stated that in supervising fintech company activities, Bank Indonesia can establish policies regarding the assessment of controls for fintech companies in the form of non-bank institutions, including publicly traded fintech companies take into account a materiality scale and/or other aspects to ensure the creation of a balance between innovation, stability, and national interests. This does not automatically serve as a basis for fintech companies to directly disclose customer data or user data to Bank Indonesia. This is what has drawn the attention of Bank Indonesia.

It should be acknowledged that Bank Indonesia plays a crucial role in monetary policy, particularly in the banking sector. As the central bank, which is a state institution with the authority to issue valid payment instruments

for a country, Bank Indonesia formulates and implements monetary policy, regulates, and ensures the smooth operation of the payment system, oversees and regulates the banking sector, and functions as the lender of last resort. One of the monetary policies implemented involves the regulation of credit or financing, including a determination of the growth of credit or financing distribution by the banking institutions as a whole, related to monetary control.

Thus, if Bank Indonesia wishes for fintech companies to disclose the personal data of their customers, it should be done through the establishment of legislation. Bank Indonesia should choose appropriate policy instruments from those available, if necessary, to mitigate the risks associated with shadow banking and non-bank financial entities in their jurisdiction from a financial stability perspective and should implement them consistently and effectively. The right policy instruments to be adopted may already exist or may need to be introduced. When implementing policy instruments, authorities should ensure that they are proportional to the level of risk faced by non-bank financial entities and should consider the adequacy of existing regulatory frameworks as well as the relative costs and benefits of implementing such instruments.

This is what is then referred to as Bank Indonesia, which maintains the sovereign authority over Indonesia's monetary economy.

Economic monetary sovereignty has various meanings. The concept of economic monetary sovereignty revolves around the consolidation and expression of common values such as equality, accountability, and legitimacy and more specific goals like economic development, the maintenance of financial integrity and the promotion of financial and monetary stability.[17] Furthermore, improving the central bank's capacity to advance monetary stability—a vital component of contemporary monetary sovereignty.[18] One approach to addressing this is to set up regulations delineating Bank Indonesia's authority to interconnect customer data, as well as data pertaining to borrowers or fund users from fintech companies. This measure ensures that Bank Indonesia operates with a transparent legal foundation in its actions.

B. The Interlink Policy Between Fintech and Banking is Designed to Prevent Shadow Banking Risks while Respecting the Human Rights of Users

With the widespread use of fintech companies by the Indonesian population for borrowing money and obtaining funding, an interlink policy serves as a means for these fintech companies to acquire personal information from potential

[17] Claus D. Zimmermann, "The Concept of Monetary Sovereignty Revisited," *European Journal of International Law* 24, no. 3 (2013): 797-818, https://doi.org/10.1093/ejil/cht041.

[18] ibid

and existing customers. Currently, the collection of personal data from online loan users is predominantly carried out by financial institutions or lenders, not by Bank Indonesia. This implies that Bank Indonesia is not directly involved in the funding or lending transactions between the parties. Bank Indonesia itself typically does not have direct access to the personal data of individuals using online loan services unless there is involvement in investigations related to legal violations or compliance with applicable regulations. The collection and processing of personal data by financial institutions in Indonesia are regulated by Law Number 19 of 2016 on Electronic Information and Transactions Law as amended by Law Number 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law (hereinafter referred as Law 19 of 2016), as well as other relevant laws and regulations concerning privacy and personal data protection. One of the doctrines espoused by Rosadi said that the principles of data protection related to consumer privacy should be fulfilled by the service providers in order to protect their rights on the highest level.[19]

When a prospective customer applies for a loan or seeks other funding, they are required to register on the relevant website or application. During the registration and application process, the prospective customer provides their personal information to the fintech company. In this situation, the prospective customer is considered a subject of personal data protected by their rights under the Personal Data Protection Law Number 27 of 2022. Rights under this law include, among other provisions:

a. the right to terminate the processing, delete, and/or destroy Personal Data about oneself in accordance with the provisions of the prevailing regulations;
b. the right to withdraw consent for the processing of Personal Data about oneself that has been given to the Personal Data Controller;
c. the right to postpone or limit the processing of Personal Data proportionally according to the purposes of processing Personal Data;
d. the right to obtain and/or use Personal Data about oneself from the Personal Data Controller in a form that is in line with the common structure and/or format that can be used or read by electronic systems; and
e. the right to transmit Personal Data about oneself to other Personal Data Controllers, as long as the systems used can communicate securely in accordance with the principles of Personal Data Protection under this Law.

However, Article 15 paragraph (1) of Law No. 27 of 2022 provides for exemptions for:

[19] Sinta Dewi Rosadi, *Cyberlaw: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional* (Bandung: Refika Aditama, 2015).

a. National defence and security interests;
b. Law enforcement processes;
c. Public interests in the framework of state administration;
d. Oversight interests in the financial services, monetary, payment systems, and financial system stability sectors conducted in the framework of state administration; or
e. Statistical and scientific research interests.

As part of the obligation to protect data, the Indonesian Government mandates the enactment of statutory law that state data uses and data protection. In consideration part of Law No. 27 of 2022 states that personal data protection is one of the human rights that constitutes personal protection, therefore it is necessary to provide a legal basis to provide security for personal data, based on the 1945 Constitution of the Republic of Indonesia. The Indonesian Government ensures all government institutions, and many specialised industries simultaneously protect the data from users. This applies in other jurisdictions. Other countries and regions have a basic debate related to the privacy or data security and both require the personal data must be processed fairly and lawfully, collected for legitimate and specified reasons, adequate, relevant and not excessive in relation to the purposes for which it is collected, accurate and where necessary, kept up to date, and retained as identifiable data for no longer than necessary to serve the purposes for which the data were collected.[20]

If Bank Indonesia undertakes data retrieval or interlinks with these fintech companies, it falls under the classification of supervisory interests in the financial and monetary services sector. However, this authority emerges as a form of "compulsion" for fintech companies to disclose customer data. Nonetheless, the term "interlink" is meant to be voluntary and regularly executed. This is in line with Article 162 paragraph (5) of Bank Indonesia Regulation Number 23/6/PBI/2021 concerning Payment Service Providers (PerBI No. 23 of 2021), which states that Bank Indonesia has the authority to conduct examinations and/or request reports, documents, data, information, explanations, and/or clarifications from parties conducting fund management activities. This mechanism indicates that fintech companies can only disclose customer data after a request from Bank Indonesia and is not a voluntary act by fintech companies to provide data.

However, the disclosure of customer data could violate an individual's human rights if there was no consent from the customer. For example, in the terms and conditions when someone borrows money from a fintech company,

[20] McKay Cunningham, "Complying with International Data Protection Law," *University of Cincinnati Law Review* 84, no. 2 (2018).

there is no explicit statement or approval from the customer to disclose their data to third parties, even if it is the Bank of Indonesia. In Article 177 PerBI No. 23 of 2021, it is stated that for consumer protection, fintech companies conducting fund management activities through the issuance of electronic money are obligated to limit their requests for and use of data and/or information of electronic money users only to the extent necessary for the provision of electronic money services. With the provisions of Article 177 PerBI No. 23 of 2021, it is possible that fintech companies may not provide customer data to Bank Indonesia even if requested for supervision purposes.

This creates two anomalous conditions. First, Bank Indonesia has the authority to oversee the financial services sector, monetary affairs, payment systems, and financial system stability, conducted in the context of state administration. Therefore, Bank Indonesia can request all data and information related to fintech companies along with their customer data. Second, fintech companies are obliged to limit their request for and use of data and/or information of electronic money users. Due to this anomaly, Bank Indonesia cannot automatically request customer data because of the protection efforts by fintech companies, as stated in Article 177 PerBI No. 23 of 2021.

In Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, it is stated that everyone has the right to the protection of their personal self, family, honour, dignity, and possessions under their control. They also have the right to security and protection from threats or fear to do or not do something. In the explanatory notes of Article 26 of Law No. 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (the Informasi dan Transaksi Elektronik or ITE Law), it is stated that in the utilisation of information technology, the protection of personal data is an essential privacy right. Privacy rights include the right to enjoy one's life free from all matters of interference, the right to communicate with others without eavesdropping, and the right to supervise access to information about one's personal life and data.

If considering a supervision evaluation based on rights, attention to data is one aspect. However, focusing on the individual's right to live without unwanted surveillance and intrusion is also crucial. Privacy is considered a basic but not absolute right. The state places a great deal of importance on its rights and even its obligation to establish national security, detect and prosecute crimes, maintain public health, and prioritise the safety of others with a high level of importance.[21] This aligns with the principles of human rights as stated

[21] Gary T. Marx in Kristie Ball, Kevin Haggerty, and David Lyon (eds) *Routledge Handbook of Surveillance Studies* (New York: Routledge, 2012).

in Law No. 39 of 1999 on Human Rights, Article 1 number 1, which declares that human rights are a set of inherent rights in the essence and existence of human beings as creatures of the One Almighty God. These rights are divine gifts that must be respected, upheld, and protected by the state, the law, the government, and every individual for the dignity, honour, and protection of the humans. This article is related to Article 21 of the Human Rights Law that protects every person's right to personal integrity, both spiritual and physical, and therefore there can be no object of research without consent from him.

Article 38 prohibits every person from engaging in acts that may cause physical and electromagnetic interference on telecommunications services. Under Article 40, every person is prohibited from conducting wiretaps on information transmitted over telecommunications networks in any form. Furthermore, Article 42 states, (1) the telecommunication service provider is obliged to keep confidential the information that is sent and or received by its telecommunications service customers through telecommunications networks and/or telecommunications networks and or telecommunications services provided. In paragraph (2) for the purposes of the criminal justice process, the telecommunications service provider may record information sent and/or received and may provide the necessary information upon: a. written request from the Attorney General or the Chief of Police of the Republic of Indonesia for certain criminal acts; or b. investigator's request for certain criminal acts in part a.

In addition, Article 12 of the Universal Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Therefore, even though users or customers of fintech companies may avail themselves of financial services, they also have the right to privacy. The concept of the right to privacy is also found in Article 17 of the International Covenant on Civil and Political Rights (hereinafter referred to as ICCPR), which regulates privacy rights. This article has similar wording to Article 12 of the UDHR. The distinction between Article 12 of the UDHR and Article 17 of the ICCPR lies in paragraph 2 of Article 17 of the ICCPR, which provides clarification regarding the protection of the right to privacy. While the ICCPR itself does not explicitly state that personal data is part of the right to privacy, the United Nations Human Rights Committee (HRC) has provided detailed guidelines explaining the scope of the right to privacy. This explanation is found in ICCPR General Comment No. 16: Article 17 (Right to Privacy).[22] In that General Comment, it is mentioned that for the purpose of

[22] Christopher Kuner, "The European Union and the Search for an International Data Protection Framework", *Groningen Journal of International Law*, 2, no. 2 (2014).

obtaining the most effective protection of an individual's private life, everyone should have the right to ascertain, in a comprehensible form, what personal data is stored in automatic data files and for what purpose. Additionally, every individual should also be able to determine which public authority, individual, or private entity might control their data. If the data contains incorrect personal information or has been collected, processed, or used contrary to the law, then every person is entitled to the right to request deletion or correction.[23] Along with it, Article 17 of the ICCPR 1966 outlines privacy as follows: 1. 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; and 2. Everyone has the right to the protection of the law against such interference or attacks. In 1988, this was further elaborated on in General Comment No. 16 on Article 17 ICCPR. This Comment explained:

a. Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his privacy, family, home, or correspondence, as well as against unlawful attacks on his honour and reputation. In the view of the Committee, this right must be guaranteed against all such interferences and attacks, whether they originate from state authorities or from natural or legal persons. The obligations imposed by this article require the state to adopt legislative and other measures to give effect to the prohibition against such interferences and attacks, as well as to the protection of this right; and
b. In this context, the Committee would like to emphasise that the reports submitted by States parties to the Covenant lack adequate focus on information related to how the right specified in the Covenant is safeguarded by legislative, administrative, or judicial authorities, as well as by the relevant entities established within the State. There is a notable deficiency in addressing the dual aspect of protection against both unlawful and arbitrary interference outlined in Article 17 of the Covenant. This underscores the importance of incorporating provisions in state legislation specifically to protect the right outlined in that article. Currently, the reports either omit details about such legislation or offer insufficient information on this matter.[24]

Privacy has consistently been defined in the context of personal autonomy or having the innate control over the personal intimacies or having control over

[23] United Nations, 1988, General Comment No. 16 of Article 17 on The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.

[24] United Nations Human Rights Commission, General Comment No 16 Article 17 on the Right to Respect of Privacy, Family Home and Correspondence and Protection of Honour and Reputation, 8 April 1988, UN Doc., HRI/GEN/Rev9.

the personal data about oneself.[25] Solove breaks down the right to privacy into six different concepts: (1) The right to be left alone; (2) the ability to limit access or shield oneself from unwanted access by others; (3) the right to secrecy or the concealment of certain matters from others; (4) the ability to control personal information and the ability to exercise control over information about oneself; (5) the protection of personhood, or the protection of ones' personality, individuality and dignity; and (6) Intimacy, control over or limited access to ones' intimate relationships or aspects of life.[26] It means that legislation must enforce provisions on privacy, both morally and legally. Considering that some lending services from fintech companies do not include privacy clauses, there should be limitations on fintech companies' use of customer data.

In Southeast Asia, the ASEAN organisation has conceptualised a framework that identifies four strategic priorities of digital data governance supporting the ASEAN digital economy, namely:[27] (a) Data Life Cycle and Ecosystem; (b) Cross Border Data Flows; (c) Digitalization and Emerging Technologies; and (d) Legal, Regulatory, and Policy. The complete set of regulations in Indonesia must encompass, at a minimum, these four elements. This includes rules concerning Bank Indonesia's jurisdiction to establish connections with fintech companies. It has become imperative for Bank Indonesia and banking institutions to pay attention to and consider fintech user data as part of human rights.

While recognizing the interlinkage between fintech and banking to avoid the risks associated with shadow banking through digital technology regulation, business collaboration, and company ownership, it is essential not to neglect user rights. Especially at present, many fintech lending platforms in Indonesia do not include clauses consenting to the sharing of customer/user data with Bank Indonesia or other banking institutions. Therefore, if Bank Indonesia takes such actions without proper consent, it would contradict human rights principles and legal regulations. Although it has been regulated in PerBI No. 23 of 2021, However, the extended authority to affirm the existence of an interlink between banking institutions, Bank Indonesia, and fintech companies in the form of user data or customer data disclosure is not yet fully robust. Indonesia has to establish a good integrated and coordinated system to make

[25] T. Gerety, "Redefining Privacy," *Harvard Civil Rights-Civil Liberties Law Review* 12, no. 2 (1977): 236 and William Parent, "Privacy Morality and the Law," *Philosophy and Public Affairs* 12, no. 4 (1983).

[26] Daniel J. Solove *Understanding Privacy* (Cambridge: Harvard University Press, 2009) 13.

[27] ASEAN Telecommunications and Information Technology Ministers Meeting Framework on Digital Data Governance, https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf.

a legal certainty by recognizing and balancing private rights and public rights, determining the restriction of such rights and regulating such rights.[28]

This is based on Article 257 PerBI No. 23 of 2021, which states that, in the processing of payment system-related information, fintech companies and/or parties collaborating with fintech companies are obligated to implement principles of personal data protection, including meeting the consent aspects of Service Users regarding the use of their personal data, which include:

1. Personal data collection is conducted in a limited and specific manner, legally valid, fair, and transparent;
2. Personal data processing is carried out in accordance with its purpose;
3. Personal data processing is conducted while ensuring the rights of the data owner;
4. Personal data processing is done accurately, completely, not misleading, up-to-date, accountable, and considering the purpose of personal data processing;
5. personal data processing is carried out by protecting the security of personal data from loss, misuse, unauthorised access and disclosure, as well as alteration or destruction of personal data;
6. Personal data processing is carried out by informing the purpose of collection, processing activities, and failures in personal data protection; and
7. Personal data processing is destroyed and/or deleted unless it is still within the retention period according to the needs based on regulatory provisions.

Data processing must be carried out considering the aspects of public interest and/or other requirements set forth by authorities. However, the aspects of public interest and the specific circumstances that would lead to a violation of public interest are not specifically stated in PerBI No. 23 of 2021. But, this article only states the implementation of personal data protection in the scope of fintech and person, and does not explicitly regulate Bank Indonesia as principal. Article 17 of Law Number 30 of 2014 concerning Government Administration states that government bodies and/or officials are prohibited from abusing their authority, which includes prohibitions on exceeding authority, mixing authorities, and/or acting arbitrarily. If Bank Indonesia and fintech companies transfer data without clear legal basis, then any decision and/or action established and/or taken that exceeds authority or is arbitrary is deemed invalid if there is a final and binding court decision.

[28] Rosco Pond, My Philosophy of Law, Julius Rosenthal Foundation Lecture Series, Northwestern University 1941, 249, as quoted from Sinta Dewi Rosadi, "Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia," *Brawijaya Law Journal* 5, no. 1 (2018): 143-157. https://doi.org/10.21776/ub.blj.2018.005.01.09.

Bank Indonesia's authority regarding the interlinkage between fintech and banking to mitigate shadow banking risks, including the sharing of customer data, must be based on specific legal provisions that affirm such authority. If any government body or official, including Bank Indonesia, takes actions contrary to legal regulations or without a legal basis, such actions would be considered arbitrary under Article 18 of Law Number 30 of 2014 on Government Administration and its amendments. To address this situation, there must be specific legislation that establishes the authority of Bank Indonesia to request data and ensures an interlink with fintech companies. The authority of Bank Indonesia is regulated by law, and in the context of cooperation to access customer data, a government-business collaboration must be executed through a cooperation agreement. It then becomes the obligation of fintech companies to add clauses in the terms and conditions, to be signed by prospective borrowers or users, regarding their consent for their data to be linked with the Bank Indonesia system for supervision purposes.

III. CONCLUDING REMARKS

As the authority over Indonesia's economic and monetary sovereignty, Bank Indonesia does not yet have specific regulations regarding monetary supervision through interlinking with fintech companies to avoid shadow banking. Therefore, Bank Indonesia currently lacks specific authority to ensure the implementation of interlinking with fintech companies.

The interlinking policy with fintech companies involving the sharing of user data with Bank Indonesia should prioritise respect for human rights and the protection of privacy under the law.

REFERENCES

Books and Journals

Christopher Kuner, "The European Union and the Search for an International Data Protection Framework", *Groningen Journal of International Law*, 2, no. 2 (2014).

Claessens, S. Pozsar Z., Ratnovski L & Singh, M. "Shadow Banking: Economics and Policy Priorities," https://www.imf.org/en/Publications/Staf*f-Discussion-Notes/Issues/2016/12/31*/Shadow-Banking-Economics-and-Policy-40132, 2012.

Claus D. Zimmermann, "The Concept of Monetary Sovereignty Revisited," European Journal of International Law 24, no. 3 (2013): 797-818, https://doi.org/10.1093/ejil/cht041.

Daniel J. Solove *Understanding Privacy* Cambridge, Harvard University Press, 2009.

Ehrentraud, Johannes, Denise Garcia Ocampo, and Camila Quevedo Vega, "Regulating FinTech Financing: Digital Banks and FinTech Platforms," 27. FSI Insights on Policy Implementation. Basel: Bank for International Settlements, https://www.bis.org/fsi/publ/insights27.pdf, 2020

Financial Stability Board, Strengthening Oversight and Regulation of Shadow Banking Policy, 29 August 2013, https://www.fsb.org/wp-content/uploads/r_130829c.pdf.

Gary T. Marx in Kristie Ball, Kevin Haggerty, and David Lyon (eds) *Routledge Handbook of Surveillance Studies* (New York: Routledge, 2012).

Ibrahim A. Zeidy, "The Role of Financial Technology in Changing Financial Industry and Increasing Efficiency in the Economy, Common Market for Eastern and Southern Africa," https://www.comesa.int/wp-content/uploads/2022/05/The-Role-of-Financial-Technology.pdf

Kairong Xiao, "Monetary Transmission through Shadow Banks," *The Review of Financial Studies* 33, no. 6 (2020): 2379–2420, https://doi.org/10.1093/rfs/hhz112.

McKay Cunningham, "Complying with International Data Protection Law," *University of Cincinnati Law Review* 84, no. 2 (2018).

Ordonez G, Confidence Banking, paper presented at the 2010 Meeting Papers, 2010.

Ratnawaty Marginingsih, "Financial Technology (Fintech) Dalam Inklusi Keuangan Nasional di Masa Pandemi Covid-19," *Moneter: Jurnal Akuntansi dan Keuangan* 8, no. 1 (2021).

Rosco Pond, My Philosophy of Law, Julius Rosenthal Foundation Lecture Series, Northwestern University 1941, 249, as quoted from Sinta Dewi Rosadi, "Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia," *Brawijaya Law Journal* 5, no. 1 (2018): 143-157. https://doi.org/10.21776/ub.blj.2018.005.01.09.

Sinta Dewi Rosadi, Cyberlaw: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional (Bandung: Refika Aditama, 2015).

Soehaditama, Josua Panatap, "Sustainability in Bank: Deposits, Investment and Interest Rate." *Formosa Journal of Sustainable Research*, 2, no. 5, 1069–1078. https://doi.org/10.55927/fjsr.v2i5.3912, 2023.

Steven L. Schwarcz, "Shadow Banking, Financial Risk, and Regulation in China and Other Developing Countries," GEG Working Paper 2013/83, The Global Economic Governance Programme, University of Oxford. https://www.geg.ox.ac.uk/publication/geg-wp-201383-shadow-banking-china-and-other-developing-countries.

Stijn Claessens, Zoltan Pozsar, Lev Ratnovski, and Manmohan Singh, IMF Staff Discussion Note, SDN/12/12 December 4, 2012.

T. Gerety, "Redefining Privacy," *Harvard Civil Rights-Civil Liberties Law Review* 12, no. 2 (1977): 236 and William Parent, "Privacy Morality and the Law," *Philosophy and Public Affairs* 12, no. 4 (1983).

Zoltan Pozsar et al., Federal Reserve Bank of New York Staff Reports, No. 458: Shadow Banking, 2010.

Regulations

Bank Indonesia Regulation Number 23/6/PBI/2021 on Payment Service Providers.

Financial Services Authority Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending and Borrowing Services

Law No. 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Law Number 23 of 1999 on Bank Indonesia.

Law Number 27 of 2022 on Personal Data Protection

International Covenant on Civil and Political Rights

United Nations, 1988, General Comment No. 16 of Article 17 on The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.

United Nations Human Rights Commission, General Comment No 16 Article 17 on the Right to Respect of Privacy, Family Home and Correspondence and Protection of Honour and Reputation, 8 April 1988, UN Doc., HRI/GEN/Rev9.

Media

ASEAN, ASEAN Telecommunications and Information Technology Ministers Meeting Framework on Digital Data Governance, https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf

Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia (BSPI) 2025," https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx 15 February 2024.

Bank Indonesia, "Blueprint Sistem Pembayaran Indonesia 2025 Menavigasi Sistem Pembayaran Nasional di Era Digital," https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx

Otoritas Jasa Keuangan Republik Indonesia, "Statistik P2P Lending Periode Desember 2023," https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-P2P-Lending-Periode-Desember-2023.aspx.

Otoritas Jasa Keuangan Republik Indonesia, "Statistik P2P Lending Periode Desember 2022," https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-Fintech-Lending-Periode-Desember-2022.aspx.