Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 05
Issue: 02
Year: 2025
Page: 129-140

Citation:
Saputra, I. Y. F., & Napitupulu, D. R. W. (2025). Legal frameworks and dispute resolution mechanisms in Indonesia's fintech sector: A normative analysis. *Research Horizon*, *5*(2), 129–140.

Legal Frameworks and Dispute Resolution Mechanisms in Indonesia's Fintech Sector: A Normative Analysis

Saputra I. Y. Febrian[1], Diana RW Napitupulu[1*]

[1] Universitas Kristen Indonesia, Jakarta, Indonesia

[*] *Corresponding author: Diana RW Napitupulu (diana.napitupulu@uki.ac.id)*

Abstract

This paper examines the effectiveness of legal frameworks and regulations in Indonesia's fintech sector, focusing on consumer data protection, dispute resolution, and law enforcement. The study analyzes key regulations, including POJK No. 13/2018, SEOJK No. 14/SEOJK.07/2014, UU ITE No. 11/2008, and PBI No. 22/20/PBI/2020, to evaluate their role in safeguarding consumer data and managing digital transactions. Using a qualitative, descriptive analysis, the research highlights that these regulations establish strong foundations for data security, requiring fintech companies to implement robust security systems such as encryption and access control. However, the study also identifies gaps in enforcement, especially concerning the oversight of regulatory bodies like OJK and Bank Indonesia. Additionally, the research finds that while legal provisions are in place, there is a lack of accessible dispute resolution mechanisms for consumers, which could undermine trust in the fintech sector. The study concludes that improvements are needed in both the enforcement of these regulations and the accessibility of dispute resolution options. These findings emphasize the importance of ensuring effective legal frameworks and stronger regulatory oversight to foster a secure and trustworthy fintech environment.

Keywords

Consumer Data Protection, Dispute Resolution, Fintech, Law Enforcement, Regulatory Oversight

1. Introduction

The rapid development of technology and information worldwide has significantly transformed human habits, work dynamics, and culture. Since the invention of the steam engine in 1763, marking the beginning of Industry 1.0, technological advancements have continuously revolutionized industries—from agriculture to manufacturing and, eventually, to the digital economy (Marwan et al., 2022). The emergence of financial technology (fintech) has redefined how individuals and businesses engage in digital transactions (Muslih & Supeno, 2022l; Chaturvedi & Sinha, 2024). However, with these advancements come substantial challenges, including issues related to cybersecurity, data privacy, and consumer protection (Rohendi & Kharisma, 2024). As reliance on electronic systems and online platforms grows, the need for effective legal frameworks to ensure secure, transparent, and fair financial services becomes even more critical (Yuspin & Fauzie, 2023; Saifullah et al., 2023).The rapid development of technology and information worldwide has significantly transformed human habits, work dynamics, and culture. Since the invention of the steam engine in 1763, marking the beginning of Industry 1.0, technological advancements have continuously revolutionized industries—from agriculture to manufacturing and, eventually, to the digital economy (Marwan et al., 2022; Ye & Zhao, 2024). The emergence of financial technology (fintech) has redefined how individuals and businesses engage in digital transactions (Muslih & Supeno, 2022; Abdullah et al., 2024). However, with these advancements come substantial challenges, including issues related to cybersecurity, data privacy, and consumer protection (Rohendi & Kharisma, 2024). As reliance on electronic systems and online platforms grows, the need for effective legal frameworks to ensure secure, transparent, and fair financial services becomes even more critical (Yuspin & Fauzie, 2023; Saifullah et al., 2023).

Several studies have highlighted the importance of robust legal frameworks in promoting trust within digital financial services, particularly in the areas of data protection and fraud prevention (Hartati et al., 2023). Rahardiansah (2024) discusses the sociological aspects of fintech law enforcement, emphasizing the challenges of effectively implementing these laws in the rapidly evolving digital economy. Moreover, Noor (2023) emphasizes the role of the Financial Services Authority (OJK) in regulating fintech lending, underscoring the need for strong oversight and accountability mechanisms. Rohendi & Kharisma (2024) provide a detailed case study on personal data protection in fintech, highlighting the gaps in legal provisions and enforcement. These findings indicate that while Indonesia's legal infrastructure is extensive, there are persistent gaps in enforcement and consumer protection.

In Indonesia, legal regulations such as the Electronic Information and Transactions Law (UU ITE) play a key role in addressing these challenges, providing guidelines for the operation of fintech companies. While Indonesia has established a comprehensive regulatory landscape for fintech, enforcement remains a challenge. There is a significant need for clearer guidelines and stronger oversight to ensure consumer data protection and the efficient resolution of disputes. The increasing reliance on digital financial services, paired with rising concerns over privacy and fraud, underscores the importance of this issue. By examining the current laws and regulations—such as UU ITE, POJK, and related frameworks—this paper aims to contribute to the ongoing discourse on improving the regulatory framework for fintech, ensuring better protection for consumers, and fostering a more secure digital financial environment.

This paper seeks to examine two critical aspects within this regulatory framework: 1) legal provisions and sanctions in the fintech sector and 2) mechanisms for dispute resolution in digital transactions. The research will focus on the enforcement of laws related to data protection, fraud prevention, and consumer

rights. Furthermore, it will assess how well these laws are implemented and the penalties imposed on fintech companies that fail to comply with regulations. The study also aims to evaluate the mechanisms available for resolving disputes between fintech platforms and users, both judicially and non-judicially. This research aims to examine the effectiveness of legal frameworks and regulations in the fintech sector, with a particular focus on consumer data protection, dispute resolution, and law enforcement. Specifically, the study will analyze the regulations outlined in PBI No. 22/20/PBI/2020, Surat Edaran OJK (SEOJK) No. 14/SEOJK.07/2014, POJK No. 13/2018, and UU ITE No. 11/2008 and UU ITE No. 19/2016, within the context of Indonesia's fintech industry.

2. Literature Review

The rapid development of financial technology (fintech) in Indonesia has introduced significant legal challenges, particularly in terms of personal data protection and regulation. As fintech becomes increasingly integrated into sectors like payments, lending, and crowdfunding, concerns regarding data privacy, security breaches, and the improper use of personal information have grown. Muslih & Supeno (2022) highlight that the rise of online loans presents legal issues in Indonesia, including the need for updated legislation to address emerging concerns such as fraud and security. Their study emphasizes the necessity of effective governance and legal frameworks to mitigate these challenges. The shift toward a cashless society has further amplified risks related to cybercrime, as noted by Mauladi et al. (2022). Their research connects the surge in cybercrime activities, such as phishing and DDoS attacks, with the increased use of digital transactions. They stress the importance of stronger data protection laws and international cooperation to safeguard digital transactions. Furthermore, legal concerns related to fintech operations are explored through the lens of regulatory technology (regtech). Wiwoho et al. (2022) identify risks like money laundering and terrorism financing, which exploit the borderless nature of digital payments. They advocate for a robust legal framework to prevent the misuse of fintech for illicit activities, ensuring the integrity of Indonesia's financial system.

Saifullah et al. (2023) focus on illegal fintech practices, which remain insufficiently addressed by current laws. They argue that a cohesive regulatory framework, bolstered by regtech, could improve transparency and accountability, reducing illegal activities and enhancing compliance. Kharisma (2021) highlights the urgent need for a dedicated fintech law in Indonesia, criticizing the existing regulations for not offering sufficient consumer protection or enabling regulatory authorities like Bank Indonesia (BI) and the Financial Services Authority (OJK) to enforce criminal provisions. Rohendi & Kharisma (2024) emphasize the importance of personal data privacy in fintech, stating that improper handling of personal data can lead to significant financial losses, crimes, and violations of privacy. Their study advocates for the establishment of a Personal Data Protection Commission (PDPC) and improving financial literacy among consumers to address these challenges. They suggest that these measures will enhance data protection and empower consumers to better navigate the fintech landscape. Amalia et al. (2022) focus on the legal issues related to consumer protection and personal data security in Open API payments. The paper highlights the need for stricter laws governing data disclosure in open banking to protect consumers. The authors argue that while existing regulations cover essential aspects of Open API payments, further legal amendments are required, particularly in Indonesian Consumer Law, to enhance consumer rights in this emerging sector.

Rahardiansah (2024) presents a sociological analysis of fintech law enforcement in Indonesia, emphasizing the complexities that law enforcement agencies face in regulating fintech in the digital age. The study highlights the necessity for a

cooperative approach among various institutions to ensure effective regulation, as fintech evolves rapidly and presents challenges to traditional legal frameworks, particularly concerning data privacy and cybersecurity. Noor (2023) further elaborates on the regulatory landscape of fintech lending in Indonesia, specifically focusing on the Financial Services Authority Regulation No. 10/POJK.05/2022. This updated regulation aims to create a more comprehensive legal framework for fintech lending, addressing issues such as consumer protection, data security, and operational supervision. Noor (2023) emphasizes the importance of robust regulations to tackle the challenges posed by fintech, particularly the protection of personal data. Building on this, Yuspin & Fauzie (2023) examine the impact of the same regulation, highlighting the requirement for a Sharia Supervisory Board (SSB) in Sharia fintech companies. This addition enhances governance by ensuring operations align with Islamic principles, improving both performance and financial stability within Sharia fintech institutions. Syarif & Aysan (2024) explore the regulatory environment surrounding Sharia fintech and crowdfunding in Indonesia, focusing on the role of the Financial Services Authority (OJK) in ensuring fintech security, especially regarding data protection. Their study underscores the need for clear, effective regulations to foster the growth of Sharia fintech and crowdfunding platforms, which are gaining traction among micro, small, and medium enterprises (MSMEs). Azizah (2023) examines the adoption of fintech in Islamic banking and its broader economic impact in Indonesia, noting the lack of a comprehensive legal framework for Islamic fintech. She highlights that while conventional fintech laws exist, there is insufficient legal protection for digital assets in Islamic fintech, although Fatwas issued by the National Shariah Board offer some guidance.

Muryanto et al. (2022) explore the prospects and challenges of Islamic fintech in Indonesia, pointing out that despite its potential, the market lags behind countries like Saudi Arabia and Malaysia. Barriers include inadequate regulations, the misuse of fintech for terrorism financing, and consumer disputes. They propose an Islamic Fintech Act to address these issues and encourage growth. Hartati et al. (2023) discuss the intersection of human rights and Sharia fintech, suggesting that while it promotes financial inclusion and social justice, regulatory gaps, particularly in data privacy and cybersecurity, need addressing through laws like the Personal Data Protection Law. Marwan et al. (2022) argue that good governance, based on principles of transparency, accountability, and participation, is essential for regulating the digital economy and addressing fintech-related legal challenges. Utami et al. (2022) examine public sentiment surrounding fintech lending, concluding that although skepticism exists, the industry has room to grow with proper regulation and support. Lastly, Annas & Ansori (2021) analyze regulatory issues in peer-to-peer lending, particularly regarding interest rate determination, suggesting that current regulations by the Indonesian Joint Funding Fintech (AFPI) may violate competition laws and create cartel-like behavior, highlighting the need for clearer regulations in the fintech lending sector.

3. Methods

This research aims to examine the effectiveness of legal frameworks and regulations in the fintech sector, focusing on consumer data protection, dispute resolution, and law enforcement. Specifically, the research will analyze the regulations outlined in PBI No. 22/20/PBI/2020, Surat Edaran OJK (SEOJK) No. 14/SEOJK.07/2014, POJK No. 13/2018, and UU ITE No. 11/2008 and UU ITE No. 19/2016, in the context of Indonesia's fintech industry. The research follows a normative juridical approach, where legal documents and regulations are the primary objects of study. The design of the study is qualitative, employing a descriptive analysis to explore how these legal instruments have been implemented and enforced. This method allows the study to provide an in-depth understanding of

the current legal landscape and its effectiveness in ensuring consumer protection, especially regarding data privacy and dispute resolution. The research process begins with identifying the core legal instruments that govern fintech in Indonesia. After establishing the research question, the next step is to gather relevant legal documents and regulations such as PBI No. 22/20/PBI/2020, SEOJK No. 14/SEOJK.07/2014, POJK No. 13/2018, and UU ITE No. 11/2008 and UU ITE No. 19/2016. This will be followed by analyzing the content of these documents to understand the frameworks they establish for fintech operations. Through descriptive analysis, the study will synthesize the regulations and identify insights regarding their application in real-world scenarios. The findings will be reported to highlight any gaps in enforcement or areas of improvement. In the discussion, the study will interpret these findings and discuss their broader implications for the fintech industry in Indonesia. Conclusions will be drawn to summarize the main findings, offering recommendations for improving the enforcement of consumer protection regulations and dispute resolution mechanisms in fintech. The methodology section usually has several sub-sections:

4. Results

4.1. Legal Provisions and Sanctions in the Fintech Sector

In addition, the Financial Services Authority Regulation (POJK) No. 13/2018 regulates digital financial innovations, including consumer data protection, outlining the responsibilities of digital financial service providers, such as fintech companies, in managing consumer data. Specifically, Article 30, Paragraph 1 mandates that service providers implement security systems to protect consumer data from unauthorized access. This provision is crucial in the fintech sector as it ensures the security of sensitive data, including financial and personal information. The article emphasizes the need for fintech providers to employ strong security measures, such as encryption, server protection, and system activity monitoring, to safeguard against illegal access. Article 30, Paragraph 2 further reinforces data protection by requiring fintech providers to restrict access to consumer data to authorized individuals or those who have received explicit consent from consumers. This provision supports the principle of data minimization, as outlined in the UU PDP and the General Data Protection Regulation (GDPR). It ensures that fintech companies can only use personal data for purposes approved by consumers, and any third parties receiving this data must obtain explicit consent from the users.

Moreover, Article 37 stresses the importance of legal enforcement and OJK's supervision of fintech operators, particularly regarding consumer data protection. Operators who violate the provisions in this article may face administrative sanctions, including fines or even the revocation of their business licenses. This provision serves as a strong incentive for fintech providers to comply with data protection regulations. Furthermore, the OJK Circular Letter (SEOJK) No. 14/SEOJK.07/2014 on the confidentiality and security of consumer data provides detailed guidelines for financial service providers, including fintech, on how to protect personal data and prevent misuse. This circular is more technical and specific compared to the broader POJK, aiming to ensure the confidentiality and security of consumer data managed by financial service providers, including fintech operators. It provides clear instructions on how these providers should handle and protect consumer data to prevent unauthorized access or misuse.

One of the key provisions is OJK Circular Letter (SEOJK) No. 14/SEOJK.07/2014 related to the protection and security of personal data within the fintech sector. Article 1 defines personal data as information that can be used to identify an individual either directly or indirectly. This broad definition underscores the importance of protecting any data that can potentially identify a consumer in the

digital financial ecosystem. Article 2 highlights the obligation of service providers to store personal data securely and for no longer than necessary. It also stresses the importance of safeguarding the data from unauthorized access. This provision is particularly critical in the context of fintech, where personal data is integral to transactions and service delivery. Ensuring data is only retained for as long as necessary and protected from unauthorized access is essential to prevent misuse and maintain consumer trust.

Article 3 emphasizes that service providers must implement adequate security systems to protect personal data from potential breaches or illegal access. In the context of fintech, which operates within the digital sphere and relies on information technology and the internet for transactions, it is vital for providers to apply advanced security measures, such as encryption, firewalls, and continuous monitoring, to prevent unauthorized access to sensitive data. Article 4 specifies that only authorized parties with legitimate interests may access personal data. Fintech providers are required to restrict access to personal data to ensure that it is only used for legitimate purposes. This helps protect consumers' privacy and ensures data is not misused. Article 5 dictates that service providers must not disclose personal data to third parties without consumer consent, except in cases prescribed by law. This provision ensures that consumers' data is only shared when legally justified, reinforcing the importance of maintaining transparency and consumer control over their personal information.

Article 6 outlines the responsibility of data controllers to implement clear procedures for managing, securing, and deleting personal data once it is no longer needed. This helps ensure that personal data is properly handled throughout its lifecycle. Finally, Article 7 grants OJK the authority to supervise the implementation of these policies and impose administrative sanctions for any violations. This supervisory role underscores the importance of enforcement in ensuring compliance with personal data protection regulations within fintech. Articles 2 and 3 are particularly significant, as they highlight the responsibilities of fintech providers to safeguard consumer data. Given the nature of fintech, where transactions often involve sensitive information like ID numbers, transaction histories, account balances, and loan details, ensuring the security of this data is crucial. Implementing strong data security systems not only helps prevent illegal access but also fosters consumer trust, which is essential for the continued growth of the fintech industry.

Article 4 states that only parties with legitimate interests are allowed to access personal data. This aligns with the principle of data minimization in the UU PDP and GDPR, which stipulate that personal data should only be used for clear and lawful purposes. In the fintech industry, restricting access to data is crucial, especially when third parties such as cloud service providers or business partners are involved in processing personal data. Fintech providers must ensure that only authorized parties can access the data and that it is protected from unauthorized access. Article 5 stipulates that fintech service providers are not allowed to disclose personal data to third parties without the consent of the consumer, except in cases specified by law. This is directly related to the requirement for explicit consent from the data subject, as outlined in the UU PDP and GDPR. Fintech providers must be transparent about which third parties will receive personal data and the purposes for which the data will be used. If the provider discloses data without the user's consent or violates these principles, they may face legal consequences, including administrative penalties as outlined in Article 7.

Article 6 establishes that fintech providers, acting as data controllers, are responsible for managing, securing, and deleting personal data that is no longer necessary. This is in line with the principles of data minimization and storage limitation under the UU PDP and GDPR. In the fintech context, if personal data is no longer required for legitimate purposes (such as after a transaction is completed),

the provider must delete the data to prevent misuse or unauthorized access. Article 7 grants OJK the authority to supervise the implementation of policies regarding the confidentiality and security of personal data in the fintech sector. If fintech providers fail to meet data protection obligations, OJK can impose administrative penalties, including operational changes, fines, or even revoking business licenses. The supervision by OJK is essential to ensure that fintech providers comply with data protection regulations and maintain strong safeguards for consumer data.

4.2. Legal Provisions and Sanctions in Dispute Resolution in the Fintech Sector

The findings of the study indicate that the Law on Information and Electronic Transactions (UU ITE) provides provisions related to law enforcement for those who violate regulations in electronic transactions and the use of electronic systems. Fintech companies that fail to comply with UU ITE, such as those involved in data protection violations or online fraud, may face criminal sanctions or fines as stipulated in the law. For example, online lending platforms that offer products illegally or violate personal data protection rules can be subjected to penalties in accordance with the provisions of UU ITE. These violations are specifically addressed in Articles 27 to 37, which discuss the violations related to electronic transactions and the corresponding sanctions.

Furthermore, the UU ITE also regulates mechanisms for resolving disputes in electronic transactions, including those involving fintech platforms. Disputes between users and service providers regarding transactions or data management are common in the fintech industry. UU ITE outlines how these disputes can be settled, either through mediation mechanisms or through legal proceedings. The provisions for dispute resolution in electronic transactions are laid out in Articles 45B to 45I. The Financial Services Authority (OJK), as the regulator of the financial sector, has issued POJK No. 6/POJK.07/2022 regarding the protection of consumers and the public in the financial services sector. This regulation outlines the obligations of fintech providers to protect consumer data and implement stringent consumer protection principles. Specifically, POJK No. 6/POJK.07/2022 focuses on safeguarding consumers from harmful practices and ensuring the safety of personal data.

Article 3 emphasizes consumer protection principles, stating that businesses must provide consumer protection based on transparency, fairness, and personal data protection. This is particularly relevant in the fintech sector as it requires service providers to clearly inform users about the data they collect and how it will be used. It aligns with the Personal Data Protection Law (UU PDP), which mandates transparency and explicit consent from users. Article 19 outlines the obligation to disclose information to consumers, requiring businesses to provide clear, accurate, and non-deceptive information about products or services offered, including the use of personal data. This ensures transparency in fintech transactions and helps prevent misuse of personal data while empowering consumers to control their information. Article 21 provides that consumers who feel aggrieved may file complaints with supervisory authorities or designated dispute resolution bodies. In the context of fintech, if personal data violations or misuse occur, consumers have the right to lodge complaints or even pursue legal action against the fintech provider. Fintech operators are mandated to establish clear and efficient complaint mechanisms to handle data misuse, thereby ensuring consumer protection.

There are several key provisions regarding the supervision and penalties related to consumer protection in the fintech sector. According to Article 40, the Financial Services Authority (OJK) is empowered to supervise and impose sanctions on fintech operators who fail to comply with consumer protection regulations. This emphasizes the importance of OJK's oversight in the fintech sector, particularly in ensuring compliance with the Personal Data Protection Law (UU PDP). If fintech providers

fail to protect personal data or do not adhere to transparency requirements, they may face sanctions. Additionally, Bank Indonesia (BI) also plays a role in regulating personal data protection within fintech services as stipulated in PBI No. 22/20/PBI/2020. This regulation requires fintech providers under BI's supervision to implement high standards of data security to protect personal data. Furthermore, it highlights the importance of obtaining explicit consent from data owners before processing or sharing their data. PBI No. 22/20/PBI/2020 is a regulation issued by Bank Indonesia that governs the operation of payment systems involving information technology and the digitalization of financial services, including fintech transactions. The primary aim of this regulation is to regulate the operations of payment systems, specifically how fintech platforms are used in digital financial transactions. It establishes clear standards for fintech providers to follow, particularly in terms of ensuring the security, confidentiality of data, and overall consumer protection.

The regulation emphasizes several key areas. For instance, Article 8 focuses on ensuring data security by requiring fintech providers to implement adequate security procedures to protect consumer data from unauthorized access. This highlights the importance of securing personal data, especially in digital payment systems, where sensitive user information is involved. Furthermore, Article 12 stresses that fintech providers can only use consumer data for purposes that have been explicitly approved by the consumer, aligning with principles such as data minimization and purpose limitation, as set out in both the UU PDP and GDPR. Article 15 grants Bank Indonesia the authority to supervise payment system providers and enforce compliance with data protection regulations. If fintech providers fail to meet these standards, they may face administrative sanctions. This underscores the crucial role of Bank Indonesia in regulating and monitoring fintech operations to ensure data protection standards are maintained. Additionally, Article 17 requires fintech service providers to have robust policies and procedures in place to manage data security risks, ensuring the confidentiality, integrity, and availability of consumer data. This is critical given the reliance on personal data in the fintech industry.

5. Discussion

The regulation of fintech services in Indonesia, particularly with regard to personal data protection, has been an evolving landscape shaped by various legal frameworks aimed at safeguarding consumers in the digital era. The Financial Services Authority Regulation (POJK) No. 13/2018 plays a pivotal role in ensuring that digital financial service providers, including fintech companies, adopt robust security systems for protecting consumer data. Article 30, Paragraphs 1 and 2 of POJK No. 13/2018 emphasize the need for encryption, server protection, and system monitoring to safeguard sensitive personal and financial data from unauthorized access. This is vital as fintech services are heavily reliant on personal data for transactions and service delivery, underscoring the importance of data protection in the sector (Rohendi & Kharisma, 2024).

The legal provisions laid out in POJK No. 13/2018 align with global data protection norms, such as the General Data Protection Regulation (GDPR), through principles like data minimization and explicit consent from consumers for data processing (Rahardiansah, 2024). The requirement that access to consumer data be restricted to authorized individuals and parties with explicit consent is a key measure that ensures fintech providers maintain high standards of consumer privacy and trust. Furthermore, the imposition of sanctions under the regulation, including fines or revocation of business licenses, incentivizes compliance and reinforces the accountability of fintech providers in the protection of consumer data (Noor, 2023).

In addition to POJK No. 13/2018, the OJK Circular Letter (SEOJK) No. 14/SEOJK.07/2014 provides more detailed and technical guidelines for protecting

consumer data, including the need for fintech companies to store data securely and for no longer than necessary. This aligns with the broader legal frameworks, such as Indonesia's Personal Data Protection Law (UU PDP), which also emphasizes the need to secure data and only retain it for legitimate purposes (Rohendi & Kharisma, 2024). These guidelines highlight the crucial role that fintech companies must play in ensuring data security, particularly in a digital ecosystem where data breaches can have severe consequences for consumers and businesses alike (Mauladi et al., 2022).

Legal provisions related to the enforcement of data protection regulations in the fintech sector are further strengthened by the Financial Services Authority's (OJK) authority to supervise and penalize non-compliant fintech providers. Article 7 of SEOJK No. 14/SEOJK.07/2014 grants OJK the power to impose administrative sanctions on operators failing to comply with these regulations, highlighting the regulator's role in upholding the integrity of Indonesia's financial ecosystem (Syarif & Aysan, 2024). This regulatory oversight is crucial in maintaining the trust of consumers and ensuring the long-term sustainability of the fintech sector.

On the other hand, the Law on Information and Electronic Transactions (UU ITE) provides an additional layer of legal protection by offering sanctions for fintech companies that violate data protection norms or engage in unlawful activities like online fraud (Azizah, 2023). The law's provisions on criminal sanctions, coupled with dispute resolution mechanisms, contribute to building a more transparent and secure digital financial environment (Hartati et al., 2023). This legal framework not only addresses violations but also provides a pathway for resolving disputes that may arise between consumers and fintech providers, thereby reinforcing consumer protection in the digital financial space (Saifullah et al., 2023).

Additionally, Bank Indonesia's regulation PBI No. 22/20/PBI/2020 places a strong emphasis on data security within the digital payment systems used by fintech platforms. This regulation requires fintech providers to implement adequate security measures to protect consumer data, aligning with global standards for data protection (Muslih & Supeno, 2022). By requiring explicit consent from consumers before processing or sharing their data, this regulation fosters a culture of transparency and accountability in the fintech sector (Marwan et al., 2022).

This shows that Indonesia's regulatory framework for fintech services—comprising POJK No. 13/2018, SEOJK No. 14/SEOJK.07/2014, UU ITE, and PBI No. 22/20/PBI/2020—forms a comprehensive approach to ensuring data protection in the digital financial ecosystem. These regulations not only prioritize consumer privacy and security but also provide robust mechanisms for enforcement, dispute resolution, and the imposition of penalties, thus fostering a secure environment for both consumers and businesses in the fintech sector. However, as the fintech industry continues to grow, further refinement and adaptation of these regulations will be necessary to address emerging challenges and maintain the integrity of the financial system (Rahardiansah, 2024). However, while these regulations provide a comprehensive framework for data protection in fintech, the real challenge lies in their implementation and oversight. To address this, greater coordination between regulatory bodies such as OJK, Bank Indonesia, and the Ministry of Communication and Information Technology (Kominfo) is necessary to ensure fintech providers are fully compliant with the established regulations.

6. Conclusion

This paper aimed to examine the effectiveness of legal frameworks and regulations in Indonesia's fintech sector, focusing on consumer data protection, dispute resolution, and law enforcement. The research analyzed key regulations such as POJK No. 13/2018, SEOJK No. 14/SEOJK.07/2014, UU ITE No. 11/2008, and PBI No. 22/20/PBI/2020, revealing that these provisions have established strong foundations for securing consumer data and managing disputes in the fintech sector.

Specifically, POJK No. 13/2018 mandates fintech companies to implement robust security measures like encryption and access control, which are crucial for safeguarding sensitive financial and personal data. SEOJK No. 14/SEOJK.07/2014 provides detailed technical guidelines for these security measures, further strengthening the protection of personal data.

The Law on Information and Electronic Transactions (UU ITE) outlines penalties for data protection violations, including fraud, and provides mechanisms for resolving disputes between users and service providers, ensuring that consumers have recourse in case of breaches. Moreover, PBI No. 22/20/PBI/2020 enforces strict data security standards for fintech providers, reinforcing the need for compliance to protect consumer privacy. While these legal frameworks are well-defined, the research highlights some gaps in enforcement, particularly the need for stronger oversight by regulatory bodies like OJK and Bank Indonesia to ensure consistent compliance among fintech companies. The study also emphasizes that although legal provisions are in place, there is a lack of transparency and accessible mechanisms for consumers to resolve disputes quickly, which could undermine trust in the fintech sector. These findings underscore the necessity for continuous improvements in legal enforcement and dispute resolution mechanisms within Indonesia's fintech industry.

References

Abdullah, F.D., Witro, D., Makka, M.M., Is, M.S., & Wiwaha, S.M. (2024). Contemporary Challenges for Sharia Financial Institutions to Increase Competitiveness and Product Innovation Perspective of Sharia Economic Law: Evidence in Indonesia. *MILRev: Metro Islamic Law Review*, *3*(2), 141-173.

Amalia, C., Poetry, E.G., Kono, M.K., Dadang, A.K., & Kurniawan, A. (2022). Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments. *Journal of Central Banking Law and Institutions*, *1*(2), 323–352.

Annas, M., & Ansori, M.A. (2021). Problems in Determining Interest in Peer-to-Peer Lending in Indonesia. *Jurnal Media Hukum*, *28*(1), 102–116.

Azizah, S.N. (2023). The adoption of FinTech and the legal protection of the digital assets in Islamic/Sharia banking linked with economic development: A case of Indonesia. *Journal of World Intellectual Property*, *26*(1), 30-40.

Chaturvedi, P., & Sinha, S. K. (2024). Regulation of Fintech Innovations through Policy Frameworks: Ensuring Consumer Protection Whilst Promoting Innovation. *BSSS Journal of Management*, *15*(1), 83-104.

Hartati, S.Y., Kontesa, E., & Baskara, A. (2023). Sharia Fintech In The Digital Age: Human Rights in Sharia Fintech Through Criminal Law Safeguards. *Indonesian Journal of Criminal Law Studies*, *8*(2), 289-314.

Kharisma, D.B. (2021). Urgency of Financial Technology (Fintech) Laws in Indonesia. *International Journal of Law and Management*, *63*(3), 320–331.

Marwan, A., Garduno, D.O.-C., & Bonfigli, F. (2022). Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia. *Bestuur*, *10*(1), 22-32.

Mauladi, K.F., Jaya, I.M.L.M., & Esquivias, M.A. (2022). Exploring the Link between Cashless Society and Cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, *10*(3), 58-76.

Muryanto, Y.T., Kharisma, D.B., & Ciptorukmi Nugraheni, A.S. (2022). Prospects and Challenges of Islamic Fintech in Indonesia: A Legal Viewpoint. *International Journal of Law and Management*, *64*(2), 239–252.

Muslih, M., & Supeno. (2022). Financial Technology: Digital Legal Challenges and Indonesia's Economic Prospects After Covid-19 Outbreak. *Legality: Jurnal Ilmiah Hukum*, *30*(2), 255-266.

Noor, A. (2023). Regulating Fintech Lending in Indonesia: A Study of Regulation of Financial Services Authority No. 10/POJK.05/2022. *Qubahan Academic Journal*, *3*(4), 42-50.

Rahardiansah, T. (2024). Sociological Analysis of Fintech Law Enforcement in the Digital Era. *Revista de Gestao Social e Ambiental*, *18*(2), e0683.

Rohendi, A., & Kharisma, D.B. (2024). Personal Data Protection in Fintech: A Case Study from Indonesia. *Journal of Infrastructure, Policy and Development*, *8*(7), 4158.

Saifullah, S., Supriyadi, A.P., Bahagiati, K., & Munawar, F.A.A. (2023). The evaluation of the Indonesian fintech law from the perspective of regulatory technology paradigms to mitigate illegal fintech. *Jurisdictie: Jurnal Hukum dan Syariah*, *14*(2), 233-264.

Syarif, M.F., & Aysan, A.F. (2024). Sharia crowdfunding in Indonesia: A regulatory environment perspective. *Journal of Science and Technology Policy Management.*

Utami, S.H., Purnama, A.A., & Hidayanto, A.N. (2022). Fintech Lending in Indonesia: A Sentiment Analysis, Topic Modelling, and Social Network Analysis Using Twitter Data. *International Journal of Applied Engineering and Technology (London)*, *4*(1), 50–56.

Wiwoho, J., Kharisma, D.B., & Wardhono, D.T.K. (2022). Financial Crime in Digital Payments. *Journal of Central Banking Law and Institutions*, *1*(1), 47–70.

Ye, N., & Zhao, Z. (2024). The reform of consumer protection in mobile payment services in China: Legislation, regulation, and dispute resolution. *Computer Law & Security Review*, *54*, 106007.

Yuspin, W., & Fauzie, A. (2023). Good Corporate Governance In Sharia Fintech: Challenges and Opportunities In The Digital Era. *Quality - Access to Success*, *24*(196), 221-229.