Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector

Abd. Aziz, Didit Darmawan, Rafadi Khan Khayru, Agung Satryo Wibowo, Mujito

Sunan Giri University of Surabaya, Indonesia

A R T I C L E I N F O

Article history:
Received 11 September 2022
Revised 9 October 2022
Accepted 3 December 2022

Key words:
Fintech,
Personal data protection,
Regulation,
Data leakage,
OJK,
Cyber security,
Legal liability.

A B S T R A C T

Regulation in the fintech sector in Indonesia aims to protect consumers' personal data and prevent leaks through a clear legal framework, including the Personal Data Protection Law and Financial Services Authority (OJK) regulations. While these regulations establish responsibilities and sanctions for violations, challenges in enforcement and industry compliance remain, impacting the effectiveness of data protection. The introduction of guidelines by the Indonesian Fintech Association has raised awareness, but many companies, especially smaller ones, still face difficulties in implementation. Gaps in understanding and resources can result in inadequate security practices, increasing the risk of data leakage. Evolving cyber threats require continuous regulatory updates. While regulations provide the basic structure for data protection, their effectiveness relies heavily on strong enforcement, industry compliance, and the ability to adapt to new challenges. This research highlights the importance of collaboration between the government, fintech providers, and the public to create a safe and secure ecosystem for digital financial services.

INTRODUCTION

The development of Financial Technology (fintech) in Indonesia has brought significant changes in the way people access financial services. With the convenience offered, fintech has become the first choice for many consumers, especially in today's digital era. This rapid growth is also accompanied by serious challenges, one of which is consumer personal data leakage (Situmeang, 2020). Personal data that should be protected is vulnerable to misuse, which can harm consumers and threaten public trust in the fintech industry.

The legal liability of fintech providers is very important. Fintech providers are expected to comply with existing regulations and properly protect consumers' personal data. Many providers have not fully understood or implemented the necessary security standards, increasing the risk of data leakage (Fadhli et al., 2022). When there is a breach or negligence in data management, consumers are often in a weak position, as there is no recovery mechanism that truly provides legal certainty and optimal protection. This creates legal uncertainty for consumers who are victims of data leakage, and raises questions about the sanctions that can be imposed on negligent providers.

One of the main problems faced in the fintech industry is the lack of understanding and awareness of fintech providers regarding their legal responsibility to protect consumers' personal data. Many fintech providers do not have adequate data security policies in place, leaving consumer data vulnerable to breaches. Personal data is a very sensitive and vital asset in digital financial activities. This is exacerbated by the lack of supervision from the authorities, which makes organizers feel no pressure to comply with existing regulations (Sari, 2021). When regulations are not accompanied by a strict monitoring system, fintech operators tend not to feel encouraged to comply with existing rules.

Legal sanctions that can be imposed on fintech providers that fail to protect consumer data are often not strict enough. While there are regulations governing personal data protection, effective implementation of sanctions remains a challenge. Many data leakage cases are not responded to quickly and appropriately by the authorities, creating the perception that fintech providers can operate without meaningful consequences. This has the potential to create a culture of permissiveness in the digital finance sector, where data security is no longer considered a priority.

** Corresponding author, email address:* ***dr.mujito@gmail.com***

Existing regulations, such as the Personal Data Protection Law, are still in the development and implementation stage. While efforts to strengthen personal data protection, the effectiveness of these regulations in preventing data leakage in the fintech sector is still questionable. Although normatively these rules provide administrative and criminal sanctions for violators, implementation in the field often faces technical and bureaucratic obstacles. Many fintech providers have yet to fully understand or adapt their operations to the provisions of the PDP Law. Many fintech providers operate without adequate supervision, creating loopholes that can be exploited by irresponsible parties (Hidayat, 2022).

This condition shows the need for more attention to the legal responsibilities of fintech providers in protecting consumer personal data. With the increasing number of users of fintech services, the potential risk of data leakage is also increasing. Consumer data that includes sensitive information such as identity, financial data, and transaction history becomes an easy target for cybercriminals if not managed with an adequate security system. Legal responsibility does not only stop at the technical aspects, but also includes transparency in the process of collecting, storing, and deleting personal data. In the event of a breach or leak, organizers must proactively notify consumers and take remedial steps. It is important to evaluate how fintech providers can be held responsible for data leaks that occur, as well as the legal sanctions that can be imposed on those who are proven negligent in protecting consumer data.

The growth of the financial technology (fintech) sector in Indonesia has had a positive impact in facilitating access to financial services for the community. Innovations in digital payment services, online lending, and app-based investments have provided convenience for the public, especially those who were previously excluded from conventional banking services. Fintech has become a solution for financial inclusion, speeding up transactions and opening up new business opportunities. The development of fintech also poses risks related to the privacy and security of users' personal data. Reliance on digital systems makes personal data a key asset that is highly vulnerable to exploitation if not properly protected. The weakness of personal data protection in fintech services has the potential to threaten consumer information security in the event of a data leak (Fidhayanti, 2020). This is exacerbated by the many cases of data leakage in the fintech sector, which encourages the need for stricter legal responsibility for service providers.

Regulations regarding consumer personal data protection in Indonesia have been regulated by OJK and the Consumer Protection Law, but the effectiveness of sanctions for violators still needs to be improved to provide optimal protection (Bunawan & Yuningsih, 2023). Violations of personal data protection not only result in material losses for consumers but can also lead to lawsuits against fintech providers. If not taken seriously, this can damage the reputation of the organizers and reduce public trust in the fintech sector as a whole.

Examining the legal responsibility of fintech providers for consumer personal data leakage is essential to ensure adequate protection for consumers in the digital era (Permata & Haryanto, 2022). With the increasing dependence of the public on fintech services, the risk of data leakage that can harm consumers is also increasing. An evaluation of the legal sanctions that can be imposed and the effectiveness of applicable regulations will provide a clear picture of the extent to which the fintech industry can be relied upon to maintain personal data security. This will not only impact consumer trust, but also the continuous of the fintech industry itself. Consumer trust is the main foundation that supports the growth and development of the fintech sector. If consumers feel that their personal data is safe and protected, they will be more trusting and comfortable using fintech services widely.

This research aims to analyze the legal responsibility of fintech providers for consumer personal data leakage in Indonesia. It also examines the legal sanctions applicable to fintech providers who are negligent in protecting consumer data. Another goal is to evaluate the effectiveness of existing regulations in preventing personal data leaks in the fintech sector (Kesuma et al., 2021).

The results of this research are expected to contribute to legal studies related to consumer personal data protection, especially related to the growing fintech sector in Indonesia. It is also expected to serve as a guide for fintech operators and regulators in strengthening personal data protection policies to prevent data leakage and consumer harm.

RESEARCH METHOD

This research uses a normative juridical approach with a descriptive-analytical method. The normative juridical approach is used to analyze laws and regulations related to personal data protection, legal responsibility of fintech providers, and consumer rights. This normative approach is suitable for evaluating applicable regulations and legal responsibility for personal data privacy violations in the fintech sector (Virgionandy et al., 2021).

Primary data in this research include relevant laws, such as Law Number 8 Year 1999 on Consumer Protection, Law Number 11 Year 2008 on Electronic Information and Transactions (ITE), and Financial Services Authority (OJK) regulations governing fintech operations. These regulations form the basis for supervision and law enforcement mechanisms that protect consumers' personal data (Fidhayanti, 2020).

Secondary data was obtained from scientific journals, books, and articles that discuss data protection regulations in the fintech sector. This secondary data provides a comprehensive overview of the problems faced and solutions offered in personal data protection (Sinaga & Alhakim, 2022).

Data analysis was conducted using a qualitative descriptive approach, which involves identifying, interpreting, and evaluating the regulations applicable to data leakage cases in the fintech sector. This qualitative descriptive approach is effective in highlighting the weaknesses and strengths of the existing legal protection system, as well as providing recommendations to improve the system (Agustina et al., 2018).

RESULT AND DISCUSSION

The legal responsibility of fintech providers in Indonesia for consumer personal data leakage is regulated in various regulations aimed at protecting personal data. One of the main regulations is Law Number 11 Year 2008 on Electronic Information and Transactions (ITE) which has been updated with Law Number 19 Year 2016. In this law, fintech providers are required to maintain the privacy and security of consumers' personal data. In case of data leakage, the organizer may be subject to administrative or criminal sanctions, depending on the level of violation committed. Enforcement of this legal responsibility is important to provide a deterrent effect while encouraging fintech providers to always prioritize the security of consumers' personal data. With clear and firm sanctions, it is expected that fintech providers can be more careful in managing personal data, so that consumer protection becomes more optimal.

Financial Services Authority (OJK) Regulation No. 77/POJK.01/2016 on Information Technology-Based Money Lending and Borrowing Services also provides clear guidelines regarding the responsibilities of fintech organizers. In this regulation, organizers are required to implement an adequate information security system to protect consumers' personal data (Sylfi et al., 2021). This includes data management, leak prevention, and risk mitigation against cyberattacks that can harm consumers. Failure to fulfill this obligation may result in administrative sanctions, including revocation of business licenses.

Fintech providers must also comply with the principles of personal data protection stipulated in the Minister Indonesia of Communication and Information Technology Regulation Number 20 Year 2016 on Personal Data Protection in Electronic Systems. This regulation emphasizes the importance of consumer consent before their personal data is collected and used. This consent should be given explicitly after clear information is provided regarding the purpose of the collection, the type of data collected, and how the data will be used and stored. If providers do not obtain valid consent or do not protect data properly, they can be held legally liable for any data leaks that occur (Ministry of Communication and Information, 2016). It is important for fintech providers to not only understand these regulations, but also implement them strictly to prevent legal risks and build public trust in their services.

In practice, the legal responsibility of fintech providers also includes the obligation to report data leakage to the competent authority and to affected consumers. This is regulated in Article 26 of the ITE Law which states that the organizer must immediately notify the affected party in the event of a data breach. This obligation aims to provide transparency and enable consumers to take the necessary protective measures. Notification to affected consumers is essential so that they can take immediate mitigation steps, such as changing passwords, blocking accounts, or taking legal action if necessary. If the organizer fails to provide information to consumers, then in addition to potentially being subject to legal sanctions, the organizer's reputation can also be significantly affected, which ultimately affects their business continuity in the midst of increasingly fierce competition in the fintech industry.

In Indonesia, fintech providers are obliged to protect their consumers' data in accordance with the regulations stipulated in the ITE Law as well as OJK regulations. Every fintech operating in Indonesia has a legal responsibility to implement data protection standards, both from a technical and administrative perspective, to prevent information leaks that could harm consumers. Strict supervision and regulation of personal data is necessary, especially as the risk of data breaches in this sector remains high (Fidhayanti, 2020). Oversight of consumer data in the digital payments sector has become a priority, with Bank Indonesia and OJK as the main regulators. Fintech providers must also ensure that the systems they use meet security standards and can anticipate potential threats to consumer data. Given the high risk of data breaches in this sector, stricter oversight and strict sanctions for violations are crucial to improve compliance and ensure overall consumer protection.

Virgionandy et al. (2021) also highlighted that consumer data is often misused by fintech providers, particularly in the online lending process where access to users' phone contacts and photo galleries is granted without adequate security. They emphasized that civil, criminal, and administrative liability mechanisms can be applied in case of data privacy violations. This mechanism should be a controlling tool for service providers to be more responsible for the protection of consumer data. There are obstacles in law enforcement, such as lack of technical resources and weak legal framework, making data protection enforcement in the fintech sector less effective (Sinaga & Alhakim, 2022). Although privacy violations occur frequently, enforcement efforts are not optimal, and consumers are still in a vulnerable position to violations of their digital rights.

The legal liability of fintech providers related to data leakage includes the obligation to provide adequate data security in accordance with applicable regulations. This includes safeguards on data access, encryption, and strict internal controls on consumer data management. Fintechs that fail to provide adequate security protection may be subject to administrative, criminal, or civil sanctions, depending on the level of fault and the impact of the data breach on consumers (Dharmawan et al., 2019). The greater the impact of data leakage on consumers, the more severe the potential sanctions will be. Fintech providers are not only required to fulfill formal legal obligations, but are also required to have a moral responsibility in maintaining the integrity of consumer data. This step is important to create a safe and transparent digital financial ecosystem in Indonesia.

Under the Indonesian legal framework, including the Consumer Protection Law and the ITE Law, fintech providers have a responsibility to ensure consumer data security. The Consumer Protection Law requires business actors to provide correct, clear and honest information to consumers and be responsible for losses incurred as a result of using the products or services they offer. This responsibility is even greater given the volume and sensitivity of the data being managed, including financial data, personal identities and other digital information. Dharmawan et al. (2019) highlighted that data protection liability also includes compensating consumers if their personal data is leakage due to the negligence of the service provider. This compensation is a form of restoration of consumer rights as well as a form of legal responsibility from the organizers. Not only financial in nature, compensation can also include restoration of goodwill or corrective measures to prevent similar incidents in the future.

The application of legal responsibility to fintech providers who experience data leakage must be emphasized. Current policies, such as the ITE Law, provide a legal foundation but do not fully cover the aspect of strong sanctions to create a deterrent effect. Increased supervisory capacity by OJK and Bank Indonesia needs to be considered in order to minimize the risk of data leakage in fintech services (Stevani & Sudirman, 2021). Institutions and human resources with in-depth understanding of information technology need to be improved in order to supervise fintech activities thoroughly and in a timely manner. Without proactive and responsive supervision, potential violations will continue to occur, causing great harm to consumers and damaging the digital ecosystem.

Legal sanctions for fintech providers who fail to protect consumer data in Indonesia are regulated in various regulations, including the OJK Regulation and the Personal Data Protection Law. Organizers may be subject to administrative sanctions, such as fines or revocation of business licenses, if proven to violate existing provisions. More serious violations can lead to criminal sanctions, especially if the data leak results in harm to consumers. In this case, providers may face more severe legal charges, including imprisonment, depending on the level of culpability and the impact caused (Pessy, 2022). Regulations governing sanctions aim to encourage fintech providers to be more responsible in protecting consumers' personal data. With strict sanctions, it is expected that organizers will be more careful in data management and implement adequate security systems. The importance of these sanctions is also reflected in the obligation of organizers to report data leaks to the authorities and affected consumers. This obligation is regulated in the ITE Law, which emphasizes transparency and consumer protection.

The protection of consumers' personal data in the fintech sector should be viewed as part of consumers' human rights. Consumers should be protected from the risk of data misuse by fintech companies, which may include unauthorized access to users' personal information in online lending services (Fidhayanti, 2020). When consumers have no control over their personal information, they are in a vulnerable position to rights violations, including exploitation, discrimination, or even extortion. The government and regulators need to develop stronger and more comprehensive policies, including requiring providers to obtain explicit consent from consumers, limiting the types of data that can be accessed, and ensuring effective complaint and dispute resolution mechanisms.

Data leakage in the fintech sector may be sanctioned under the ITE Law and OJK regulations. Octavia (2019) points out that consumers have the right to file a lawsuit if their personal data is misused by fintech providers, especially in cases involving illegal activities or negligence in personal data management. Octavia (2019) also highlighted that consumer have a basic right to privacy of their data and are entitled to compensation if their data is misused by fintech providers. The theory of legal responsibility through regulations set by OJK and Bank Indonesia ensures that fintechs must maintain consumer data in accordance with security standards.

Personal data leakage in the fintech sector is often caused by inadequate security systems, which leaves consumers vulnerable to data theft. Weaknesses in regulation and supervision increase the risk of personal data falling into the hands of irresponsible parties (Stevani & Sudirman, 2021).

Consumer data protection in Indonesia still faces various challenges, mainly due to the lack of technical expertise in e-law enforcement. Without stronger regulation and effective enforcement, the risk of personal data leakage remains high in the fintech sector (Sinaga & Alhakim, 2022). Although regulatory frameworks are in place, the effectiveness of these measures is often hampered by a lack of understanding and resources among smaller fintech players. This gap may result in inadequate security practices, thereby increasing the risk of data leakage (Pesik, 2022).

Although regulations are in place, challenges in law enforcement remain. Many fintech providers still lack an understanding of their legal responsibilities, increasing the risk of data breaches. The evolving nature of cyber threats requires continuous updating of regulations and practices. Existing laws may not fully address emerging risks, demonstrating the need for continuous adaptation and improvement in regulatory measures. Regulations applicable to the fintech sector in Indonesia aim to protect personal data and prevent leakage through legal frameworks such as the Personal Data Protection Law and OJK regulations. While these laws establish clear liabilities and sanctions for violations, challenges remain in enforcement and industry compliance, impacting overall effectiveness.

Overall, while regulations in Indonesia's fintech sector provide a basic structure for data protection, their effectiveness in preventing leakage relies heavily on strong enforcement, industry compliance, and the ability to adapt to new challenges in cybersecurity.

Legal sanctions for fintech providers who fail to protect consumer data in Indonesia aim to create a safe and reliable ecosystem in digital financial services. Cooperation between the government, organizers, and the public is needed to increase awareness and compliance with personal data protection, so that public trust in fintech services can be maintained. Government efforts to support fintech providers in strengthening data security are needed. Providing training and technology for data security can help fintech providers prevent data leakage. A partnership between the government, regulators, and the private sector in cybersecurity can be an effective solution to strengthen personal data protection in Indonesia (Dharmawan et al., 2019).

CONCLUSION

The legal liability of fintech providers in cases of consumer personal data leakage in Indonesia falls under regulations that include the ITE Law, regulations from OJK, and consumer protection regulations. These liabilities include the obligation of fintech providers to ensure the security of consumers' personal data and avoid harmful practices. Weaknesses in the implementation of data security by fintechs can have serious impacts on consumer privacy and security. While there are regulations in place, their effectiveness still needs strengthening. Stronger preventive measures and sanctions against data security violations will create a deterrent effect and increase consumer trust.

Some recommendations from this research are that stricter supervision is needed to ensure that fintech providers comply with personal data security standards. Increased capacity of law enforcement in understanding and addressing the risk of data leakage is also needed to deal with this issue more effectively. Fintech providers should be proactive in protecting consumer data by adopting security systems that comply with international standards. Fintechs can work with cybersecurity providers to prevent data leaks that could harm consumers. Consumers need to be educated about their rights related to personal data to be more careful in providing information to fintech providers. Thus, consumers can play an active role in reducing the risk of misuse of their personal data.

This research provides important implications for consumer protection policies in the fintech sector. As financial technology advances, the risks to the security of consumers' personal data are also becoming more complex and difficult to predict. The government is expected to develop more adaptive policies to deal with technological developments and data security risks. Collaboration between regulators, government, and fintech providers is essential to create a safe and sustainable ecosystem for consumers.

REFERENCES

Agustina, E., Prasetyo, H., & Subakdi. (2018). Teori Tanggung Jawab Berjenjang (Cascade Liability Theory) dalam Tindak Pidana Korporasi di Indonesia. *Jurnal Hukum*, 15(2), 169-194.

Ali, Z. (2016). *Metode Penelitian Hukum*. Sinar Grafika, Jakarta.

Asikin, Z. (2011). *Pengantar Ilmu Hukum*. Rajawali Pers, Bandung.

Bunawan, K. R., & Yuningsih, H. (2023). Perlindungan Hukum terhadap Data Nasabah dalam Penyelenggaraan Layanan Pinjam Meminjam Uang berbasis Teknologi Informasi. *Lex LATA*, 5(1), 77-86.

Dharmawan, N., Kasih, D., & Stiawan, D. (2019). Personal Data Protection and Liability of Internet Service Providers: A Comparative Approach. *International Journal of Electrical and Computer Engineering*, 9(4), 3175-3184.

Fadhli, Z., Rahayu, S. W., & Gani, I. A. (2022). Perlindungan Data Pribadi Konsumen pada Transaksi Paylater. *Jurnal Hukum Magnum Opus*, 5(1), 119-132.

Fidhayanti, D. (2020). Pengawasan Bank Indonesia Atas Kerahasiaan dan Keamanan Data/ Informasi Konsumen Financial Technology pada Sektor Mobile Payment. *Jurisdictie Journal*, 11(1), 16-47.

Huijber, T. (1995). *Filsafat Hukum*. Kanisius, Yogyakarta.

Kementerian Komunikasi dan Informatika. (2016). *Peraturan Kementerian Komunikasi dan Informatika Tahun 2016 Nomor 20*. Berita Negara Republik Indonesia Tahun 2016 Nomor 1829. Jakarta.

Kesuma, A. N. D. H., Budiartha, I. N. P., & Wesna, P. A. S. (2021). Perlindungan Hukum terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial dalam Transaksi Elektronik. *Jurnal Preferensi Hukum*, 2(2), 411-416.

Negara, D. S., D. Darmawan, & P. Saktiawan. (2022). Privacy Violations on Social Media and Interpersonal Trust Among Young Generations, *Journal of Social Science Studies*, 2(2), 151 – 156.

Octavia, S. (2019). Perlindungan Nasabah Layanan Fintech Atas Penggunaan Data Pribadi Terkait Tindakan Penagihan Pinjaman Kredit *Thesis,* Universitas Brawijaya.

Permata, S., & Haryanto, H. (2022). Perlindungan Hukum terhadap Pengguna Aplikasi Shopee Pay Later. *Krisna Law: Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana*, 4(1), 33-47.

Pesik, A. N. (2022). Perlindungan Hukum terhadap Data Pribadi dalam Transaksi Bisnis Berbasis Online. *Gorontalo Law Review*, 5(2), 326-333.

Pessy, R. A. (2022). Tanggung Jawab Kreditur terhadap Debitur yang Mengalami Kebocoran Data Pribadi pada Aplikasi Pinjam Meminjam Uang Secara Online (Fintechlending) *Thesis*. Universitas Tanjungpura.

Republik Indonesia. (2016). *Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.* Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251. Sekretariat Negara, Jakarta.

Republik Indonesia. (1999). *Undang-undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.* Lembaran Negara Republik Indonesia Tahun 1999 Nomor 22. Sekretariat Negara, Jakarta.

Sinaga, E. P., & Alhakim, A. (2022). Tinjauan Yuridis terhadap Perlindungan Hukum bagi Pengguna Jasa Pinjaman Online Ilegal di Indonesia. *UNES Law Review*, 4(3), 283-296.

Situmeang, D. S. (2020). Perlindungan Hukum terhadap Data Pribadi Konsumen Belanja Online (Studi Kasus Tokopedia) *Thesis*. Universitas Atma Jaya Yogyakarta.

Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. *Jurnal Jurisprudence*, 23(2), 197-216.

Sylfia, A., Amrullah, M. F., & Djaja, H. (2021). Tanggungjawab Yuridis PT. Tokopedia Atas Kebocoran Data Pribadi dan Privasi Konsumen dalam Transaksi Online. *Bhirawa Law Journal*, 2(1), 21-27.

Virgionandy, R., Husni, L., & Muhaimin, M. (2021). The Legal Liability of Fintech Companies for Accessing Telephone Contact Lists and Photo Galleries in the Online Loan Process. *International Journal of Multicultural and Multireligious Understanding*, 8(2), 191-205.

*Aziz, A., D. Darmawan, R. K. Khayru, A. S. Wibowo, & Mujito. (2023). Effectiveness of Personal Data Protection Regulation in Indonesia's Fintech Sector, *Journal of Social Science Studies*, 3(1), 23 – 28.