

Legal Reformulation and Ethics of Fintech Lending Companies In Indonesia

Rina Arum Prastyanti¹ and Arief Budiyo²

¹Business Law Faculty, Universitas Duta Bangsa, Surakarta

²Law Faculty, Universitas Muhammadiyah, Surakarta

Corresponding Authors: rina_arum@udb.ac.id

Abstract

With a large number of cases of legal and ethical violations committed by fintech lending companies, it shows that there is still a legal void considering that fintech users are not yet protected, so there need to be ideal legal and ethical rules for big data on fintech lending industry. This research uses empirical legal analysis with qualitative research. This research goes beyond the gap between philosophy and practice. The view of empirical legal research also points out non-doctrinal or socio-legal research. This observation refers to the gap among the legal norms contained in Law No. 11 of 2008 concerning Electronic Information and Transaction. The information analysis procedure used in this research is in interactive form.

Keywords: ethics, fintech lending, legal reformulation

Introduction

Fintech emerged in 2005 in England (Milne, 2016). In Indonesia, 116 fintech lending providers are registered and obtained licenses from OJK (OJK, 2021). One of the supporting system infrastructures for the implementation of fintech lending is the use of Big Data. Big information can store, transfer and digest information, this is useful for supporting decision-making (Rabhi, 2019) as well as analysis and problem-solving tools. On the other hand, the negative implications of using Big Data are the emergence of fintech lending which provides convenience through loans without collateral and direct contact (Ika Atika, 2020). Fintech lending measures funding feasibility by using the borrower's digital footprint hidden in big data (OJK, 2018). Law No. 11 of 2008 on Electronic Information and Transaction which has been amended by Law No. 19 of 2016, and supplemented by Regulation of the Minister of Communication and Information No. 20 of 2016 on Protection of Personal Data in Electronic Systems has regulated personal data protection, which covers safeguarding personal data during its acquisition, processing, analysis, maintenance, performance, notification, transmission, collaboration, and destruction.

Ethical problems occur when fintech lending companies obtain borrowers' personal data via the internet to make collections. Negative reviews regarding collection mechanisms that are carried out by unethically harassing borrowers; and their families; (Seno, 2021). Complaints to OJK during 2019-2021 (OJK, 2021) totaled 47.03% or 19,711 cases consisting of 9,270 serious complaints and the remaining 10,441 were minor and moderate violations (Aziz, 2021). The use of technology often causes problems, so anticipation is needed to be included in the legal system. The rapid advancement of technology is not free from risk. This often raises new problems that must be responded to by a legal system (Martin, 2019). The use of big data needs to be regulated considering that freedom to obtain information is a privacy right (Andrej, 2020). Privacy is not only protected by law but also by cultural norms, ethics, and business practices (Sahat, 2021). With a large number of cases of legal and ethical violations committed by fintech lending companies, it shows that there is still a legal void considering that fintech lending users are not yet protected, so there need to be ideal legal and ethical rules for big data on fintech lending.

Method

This research uses empirical legal analysis with qualitative research. This research goes beyond the gap between philosophy and practice. The view of empirical legal research also points out non-doctrinal or socio-legal research. This observation refers to the gap between the legal norms contained in Law No. 11 of 2008 concerning Electronic Information and Transaction, Financial Service Authority Regulation (POJK) No 77/POJK.01/2016 regarding Information

Technology Based Money Lending Services (*Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi* or LPMUBTI) and its implementation in the society. The population in this study was financial technology companies registered with OJK and fintech customers in Semarang and Surabaya.

The illustration collection method uses convenience sampling, with the research illustration collection method matching the availability of informants needed in the research. This research was tested on 30 informants using an in-depth question-and-method and bibliography research. The Information validity method uses information triangulation. Information analysis method using an interactive form of qualitative analysis. Inferior information is not obtained directly from fields that provide bonus data or endorse all the basic information. This information includes Law No. 11 of 2008 regarding Electronic Information and Transaction and Financial Service Authority Regulation (POJK) No 77/POJK.01/2016 regarding Information Technology Based Money Lending Services (LPMUBTI). as well as other supporting information such as daily announcements, certificates from the Financial Services Authority, the Indonesian Joint Funding Fintech Association (AFPI), and the Indonesian Sharia Fintech Association (AFSI). The information analysis procedure used in this research is an interactive qualitative information analysis method.

Based on the case above, it is necessary to look for laws and ethics that ideally regulate the use of Big data by Fintech Lending Companies. To be able to offer the perfect design above, it is necessary to study in advance how Law and Ethics regulate the use of Big data in the fintech lending industry and how Law and Ethics govern the use of big data in the fintech lending industry.

Result Discussion

Regulating the Use of Big Data by Fintech Lending Companies

The backbone means the protection of personal data in the digital economy. Profitable digital programs accumulate, method, and acquire individual information in large ratios and generate income through promotions or by other means. The public zone body also collects and works on information for a variety of purposes, from the provision of public services to surveillance. Improper suppression of individual information takes a toll on customers, leading them to commit fraud the risk of information breaches, their privacy rights being violated, as well as the ability to use them. Protection of personal information is very important for privacy and security, it demands attention and action from the state's authorities, the private sector, and citizens. The framework for data protection activities can help encourage customer confidence and increase digital enactment, which in turn might pressure capital investment, competition, and modernization in Indonesia's digital economy. In this condition, there are two main legal issues in this growing issue:

- a. the absence of a consistent regulatory environment that oversees the digital economy, particularly regarding the protection of data stored in big data

- b. A collaborative approach to addressing new difficulties is hampered by the government's approach to policymaking.

In the digital economy, data protection is a multi-stakeholder issue. According to Aprilianti & Dina (2021), there are at least 14 ministries and government organizations that manage the digital economy sector through more than 60 rules and regulations. This is the first challenge. With a focus on particular industries, such as telecommunications, electronic information and operations, financial services, electronic system operators, management of government, and health, more than half of these rules and adjustment deal with personal data protection. However, several of the laws conflict or overlap with one another. The various classification of personal data for example Consumers are significantly impacted by improper treatment of personal data, which exposes them to fraud risks from data breaches, violation of rights of privacy, and possibilities of exploitation.

Governments, the business sector, and citizens must pay attention to and take action regarding the protection of personal data since it is important to privacy and security. Two existing regulations: the Electronic Information and Transaction Law (UU ITE) No.19/2016 and the Citizen Administration Law No.24/2013 (Riyadi, 2021). Therefore, having a Personal Data Protection Act ends up being even more important in making a thorough legal foundation for data protection and privacy.

Consumers are significantly impacted by the improper handling of personal data in big data, which exposes them to fraud threats from data breaches, violation of rights privacy, and possibilities of exploitation. Governments, the commercial sector, and citizens all need to pay attention to and take action to protect personal data, which is essential for privacy and security. An effective data protection system may boost consumers' trust and digital adoption, which will encourage investment, competition, and innovation in Indonesia's digital economy. The following issues with consumer ethics are brought on by fintech's usage of big data:

- a. The collection of personal data is unrestricted, particular, legal, ethical, and done with the knowledge and approval of the owner.
- b. No clear objectives and restrictions are established;
- c. No legal framework exists.
- d. The current legal framework for handling personal data is not compatible with its intended use.
- e. The request for authorization to the data owner does not include any information regarding the processing of personal data.
- f. Personal data processing that does not follow its intended purpose.
- g. Although there are one or more uses for processing personal data, those uses are not consistent with the objectives.
- h. If the additional objective is there, further examination to determine whether it is compatible with the primary objective is not carried out.
- i. Processing of Personal Data does not ensure the owner's rights.
- j. There is no consent for processing personal data

- k. The objective of the processing is not taken into account and the personal data is not collected in a way that is accurate, complete, factual, current, and responsible.
- l. Personal data processing is done in a way that is inaccurate, lacking, deceptive, and out-of-date.
- m. Personal data processing cannot be held accountable.
- n. Processing of Personal Data is done without taking into protecting of the owner's account from loss, abuse, unauthorized access, alteration, and impairment.
- o. Loss of personal data

The following are examples of improper use of personal data: Illegally destroying and altering personal data, Processing of personal data is done without advance notice, upholding the objectives of acquisition, processing activities, and protection of personal data violations. Except for the time necessary to fulfill the concern outlined in the laws and regulations, personal data is not deleted or erased. The storage time is not covered by any provisions. After the storage period expires, there are no steps or requirements for removing Personal Data.

Another issue is that, despite the Ministry of Communication and Information Technology's (MOCIT) efforts to maintain its authority as the supervisor of personal data through a variety of legal means (including Electronic System Operator (ESO) registration, investigations, monetary penalties, and termination of access), the current strategy still excludes the involvement of the private sector:

- a. There are no organized efforts to enhance the quality of human resources to address privacy and security issues. The key to privacy and security's best practices is a solid professional talent that will protect the platform from data breaches or privacy breaches. To do so, there needs to be continuing professional education and executive learning programs for relevant professionals. A similar model can be found in the financial sector, where continuing executive education for certain types of skills, such as risk management, is mandatory.
- b. Precautions are still lacking. As the Ministry of Communication and Information Technology's data shows, 93% of incidents are the result of a data breach that has already occurred. Precautions require more effort in creating technical standards and ensuring that they are applied consistently, regardless of any privacy incident.
- c. As platforms are expanding dramatically as the digital economy grows, the Ministry of Communication and Information Technology may not have sufficient capacity and resources to oversee the entire industry. To date, there are more than 4,000 ESOs registered on the Ministry of Communication and Information Technology's ESO portal which includes Indonesian and foreign companies (<https://pse.kominfo.go.id/>) and the number will continue to grow. The Ministry of Communication and

Information Technology will need a large number of investigators and monitors to carry out its mandate. Having a co-regulatory approach with trusted partners will reduce the burden on the Ministry of Communication and Information Technology's resources, combining the need to seriously enforce personal data protection rules while maintaining a light-touch approach to internet regulation.

- d. As the presence of several regulators active in the digital space, and the possibility of using their regulations for the same activity, the question arises as to who has the authority to decide whether a security measure by a company meets a degree of protection equivalent to the PDP bill has been complied with whether it is the Ministry of Communication and Information Technology or a sectoral supervisory authority (e.g., OJK in the fintech sector, or the Ministry of Trade in the e-commerce sector) who take on this role.

For instance, Articles 58 and 59 of PP 80/2019 require business people to manage personal data by "standard business practices" in e-commerce. There may be a conflict between the legal obligations to produce and manage personal data lawfully, ensure its accuracy, put in place an adequate protection mechanism, and only gather data necessary for specific, pertinent reasons. Article 17 of Permendag No. 50/2020 states that the use of personal data also should fit to the "principles of consumer protection and ensuring fair competition" for specific activities like internet marketing and advertising. The rules of business organizations must "provide at least a standard degree of protection similar to that of the legal draft," according to the legal draft on the protection of personal data's article 55.

Legal Reformulation of the use of Big data by Fintech Lending Companies

The upcoming legal draft Personal Data Protection provides many opportunities for associations of Data Protection Officers (DPOs) to assist in upholding professional rules, standards, ethics, and qualifications or competency standards in the field of personal data protection, despite the fact that there are currently procedures in the digital finance industry that can serve as a basis for co-regulation on personal data protection. Focusing laws and enforcement at the board and individual level to support corporate responsibilities and obligations (i.e., DPO within a firm), has the potential to increase standards of personal data protection. The Personal Data Protection Officer (DPO) is a crucial component of the data secure ecosystem that the Ministry has established based on the Existing Regulations and the Legal Draft.

This was acknowledged by the Ministry of Communication and Information Technology Strategic Plan 2020-2024 which included the "development of the DPO ecosystem" as one of the Ministry of Communication and Information Technology's priorities (Menkominfo, 2021). Although the legal draft for personal

data protection in Indonesia popularized the term "DPO," the need for experts to manage personal data in the digital sphere has long existed. In fact, Article 28 of the Ministry of Communication and Information Technology Regulation No. 20 of 2016 concerning the Protection of Personal Data was the first to address data owners' concerns about the acquisition and management of their personal information. Later, the law draft for protecting personal data broadened this responsibility. The functions and responsibilities of DPOs are directly tied to the draft personal data protection law's legal requirements for personal data processors and owners.

The treatment of personal data regarding individual privacy and data owners' rights is the responsibility of both data controllers and processors. As a result, processors and controllers are required to use and treat personal data in a responsible, transparent, and limited manner to fulfill these responsibilities by existing data protection laws, DPO supports data controllers and processors. Not every controller and processor, nevertheless, is needed to name a DPO. The proposed legislation adopts a risk-based approach similar to the General Data Protection Rule of the European Union to secure personal data (GDPR).

The proposed legislation for the protection of personal data encourages processors and controllers to put protective measures in place that are proportionate to the amount of risk involved in their data handling operations. As a result, The following activities are required of processors and authorities in order to hold the title of DPO: Making decisions on behalf of data for public services, general, extensive, and systemic monitoring of personal information, and mass processing of particular personal data and/or personal data pertaining to scandalous activities are all examples of processing personal data. The phrase "official or officer who carries out the personal data protection function" (Personal Data Protection Officer or PPPDP) is used in the legal draft of Personal Data Security to refer to DPOs. The term "official" denotes the requirement for DPOs to be appointed by public entities handling personal data.

According to the Ministry of Communication and Information Technology's Strategic Plan 2020–2024, if the Parliament approves the law draft for personal data protection, the rules and regulations for implementing the DPO order will pursue.

Ethics Reformulation the use of Big data by Fintech Lending

At least two significant industry associations, the Indonesian Fintech Association (AFTECH) and the Indonesian Joint Funding Fintech Association recognize the importance of industry organizations in safeguarding personal data in Indonesia's digital economy environment. Although the debate over the proposed law governing personal data privacy has stalled, In Indonesia, according to AFTECH, there are a number of important regulations and best practices that may be used to make sure that digital financial services manage to develop responsibly.

Therefore, AFTECH developed and issued a Personal Data Protection Code of Conduct for its members to promote responsible digital finance innovation through its implementation (AFTECH, 2021).

The Indonesian Fintech Association (AFTECH), which was established in 2016, has developed into a venue for many fintech businesses in Indonesia to communicate and work with different stakeholders to promote technical innovation and increase the competitiveness of the domestic fintech industry. On August 9, 2019, three years after its founding, the Financial Services Authority (OJK) formally designated AFTECH as the Organization of Digital Financial Innovation Providers (IKD). The co-regulation strategy in Indonesia's fintech industry has been proved by this appointment. AFTECH currently includes around 350 members, including fintech companies, providers of technology services, and other financial services. AFTECH's four primary pillars—community involvement, literacy and education, policy advocacy, and intelligence and understanding—serve as the foundation for its objective, which is to support the government's financial inclusion aims. AFTECH's vision is "Encouraging Financial Inclusion through Digital Financial Services in Indonesia."

With the help of twelve groups working, AFTECH has assisted the Indonesian legislature and government, particularly the Ministry of Communication and Informatics, in developing the law draft for personal data protection by contributing knowledge about the fintech sector. Public and consumer complaints about the illegal use of personal information have increased, and the legal certainty surrounding the personal data protection laws has increased public confidence in the fintech industry's offerings.

The Financial Technology Sector's Code of Conduct for Personal Data Security and Integrity Protection, also known as AFTECH's Code of Conduct for Personal Data Protection, will be used in this sentence. The concern of its members for consumers' legal certainty as Personal Data Owners about the security of personal data served as the impetus for the creation of this Code of Ethics.

It also aims to show how committed AFTECH members are to hold the government and other financial service players accountable when implementing digital financial innovations, as well as to boost public confidence in the use of financial technology. This AFTECH Code of Ethics for Personal Data Protections builds on the two primary regulations regarding Personal Data Protection Permendiknas No. 20/2016 concerning the Protection of Personal Data in Electronic Systems and Government Regulation No. 71/2019 regarding the Implementation of Electronic Systems and Transactions; while acknowledging the policy-making authority of the government.

Components of the Financial Technology Industry's General Principles Code of Ethics Regulations are: a. Reliability, Justice, and Transparency Have a distinct justification for handling personal data legally and abide by all rules and legislation that pertain to personal data. Utilize personal information in a way that is acceptable for the situation and does not harm the person. b. Data reduction Only

uses Personal Data for the reasons that the Personal Data Owner has authorized and stated. c. Members of AFTECH are required to process personal data accurately and kept up to date. Integrity and confidentiality of the data The procedures that must be followed in order to secure Personal Data under AFTECH members' control are not particularly outlined in this PDP Code of Conduct. However, in compliance with the relevant laws and regulations, this PDP Code of Conduct commits AFTECH members to take reasonable and accountable measures to protect Personal Data against breach, loss, abuse, deficiency, or unintentional modification or destruction. e. Responsibility Every Personal Data is handled carefully and in accordance with the rules of the relevant laws and regulations. Along with being done in a secure and transparent manner, the control and processing of personal information are also done in conduct that is proportionate to its intended use. f. The PDP Code of Ethics maintains that all Personal Data processing by AFTECH members is carried out with the consent of the Personal Data Owner and in compliance with the requirements of the relevant laws and regulations; and that AFTECH members have justifications and resolution processes in place to deal with accusations and accident of violations and/or lack of safeguarding Personal Data.

The PDP Code of Ethics does not provide detailed clarification and settlement mechanisms and commits all mechanisms, declarations, and notifications relating to AFTECH members' Personal Data to the regulations of the relevant laws and regulations. The Code of Conduct for Responsible IT-Based Lending Services from AFPI's different collaborative regulatory efforts was the creation and application of the Joint Code of Conduct (CoC) by AFPI, AFTECH, and AFSI (2019). The CoC of the Joint Responsible IT-Based Borrowing Services (Guidelines of Conduct for Financial Technology Operators in the Financial Services Sector that Accept Responsibility), formed in 2019, aims to be a guideline for association members, which include hundreds of fintech associations, to operate their business. responsibly. This Code of Ethics is primarily based on three general ethics: a. Product Visibility and Product Service Offering Mechanism; b. New Product Risk Mitigation; and c. Good Faith Principles Application. The AFP I's Role The Indonesian Funding Fintech Association (AFPI) was formed to bridge the gap between the Financial Services Authority (OJK) and a number of Indonesian peer-to-peer lending players. Similar to AFTECH, which uses a co-regulatory model, AFPI has given OJK a structural role in performing supervisory tasks, based on OJK Letter No. S-D.05/IKNB/2019 and OJK Regulation No.77 (POJK 77). This means that peer-to-peer lending providers must register with the AFPI and follow its Code of Conduct. As a result, the AFPI becomes the protector in charge of supervising its members. It can also state that if one of its members violates the Code of Ethics, the government, in this case, the OJK, will conduct additional investigations and review the fintech company's business license.

Conclusion

Regulation of Fintech Lending's Use of Big Data Poses Legal and Ethical Issues Legal issues include, among other things, the absence of a consistent regulatory environment that oversees the digital economy, especially in regard to the security of huge data stored data. The government's approach to policymaking stifles collaboration in responding to emerging challenges. While ethical issues include the collection of personal information that is unlimited and specific, lawful, fair, and carried out with the owner's knowledge and approval, there are no explicit goals and restrictions established, and there is no legal structure dealing with the processing of personal data, the existing legal framework for the processing of personal information is not in agreement with its original purpose, and there is no legal framework dealing with the processing of personal information that is not in accordance with its original purpose. In the request for permission from the data owner, There is no notification concerning personal data processing, and the processing of personal information is not consistent with its intended purpose. There are one or more purposes for the processing of personal data, but the process does not match the goals set out; in cases where extra purposes are present, additional analysis is not carried out to establish whether the extra purposes are in line with the original purposes; and the Processing of Personal Data does not assure the owner's rights. Reformulation of Law and Ethics in Regulating Fintech Lending's Use of Big Data keeping personal information secure in Indonesia's digital economy was at least realized by two big industry organizations, namely the Indonesian Fintech Association (AFTECH) and the Joint Funding Fintech Association Indonesia, through legal reform in the Personal Data Law and the reformulation of ethical rules for Bigdata users by Fintech (AFPI).***

References

- Anita L Allen Castellito, (2020). Origins and Growth of US Privacy Law, 701 PLI/Pat83,
- Andrea Sestino a,* , Maria Irene Prete b , Luigi Piper b, Gianluigi Guido, (2020). Internet of Things and Big Data as enablers for business digitalization strategies, Technovation 98.
- Andrea De Mauro, Marco Greco, and Michele Grimaldi, A Formal Definition of Big Data Based on its Essential Features, Published on Library Review, Vol. 65 Iss: 3, pp.122 – 135, DOI: 10.1108/LR-06-2021-0061
- Abbà, G. (2020). Quale impostazione per la filosofia morale? Ricerche di filosofia morale. Roma: LAS, Libreria Ateneo Salesiano
- Annas, J. (2019). The Morality of Happiness. Oxford: Oxford University Press
- Aristotle. (2020). Nicomachean Ethics. Cambridge, U.K.; Cambridge University Press

- Crampton J, Graham M, Poorthuis A, et al. (2021) Beyond the Geotag? Deconstructing 'Big Data' and Leveraging the Potential of the Geoweb. Available at: http://www.uky.edu/tmute2/geography_methods/readingPDFs/2012-Beyond-the-Geotag-2012.10.01.pdf
- Cumming, D.Hou,W.LeeE.(2021).Business Ethics and Finance in Greater China: Synthesis and Future Directions in Sustainability,CSR,and Fraud. Journal of Business Ethics 138(4),pp.601-626
- Gregory N. Mandel, a History lesson for a General Theory of Law and Technology, Minnesota Journal of Law in Science and Technology, Vol. 8:2, 2017, hlm. 551
- Ika Atikah, Consumer Protection and Fintech Companies in Indonesia: Innovations and Challenges of the Financial Services Authority. Jurnal Hukum dan Peradilan – ISSN: 2303-3274 (p), 2528-1100 (e) Vol. 9, no. 1 (2020), pp. 132-153, doi: 10.25216/JHP.9.1.2020.132-153
- Lawrence W. Friedman, American Law: An invaluable guide to the many faces of the law, and how it affects our daily lives, W.W. Norton & Company, New York, 1984, Legal Culture and Social Development, Stanford Law Review, New York, 1002-1010, Law in America: a Short History, Modern Library Chronicles Book, New York, 2022, 4-7
- Milne, Alistair, and Paul Parboteeah. 2016. "The Business Models and Economics of Peer-to-Peer Lending. European Credit Research Institute, no. May:1–35. Eupean CreditResearch Institute, no. May:1–35.
- Mochtar Kusumaatmadja, Konsep-Konsep Hukum Dalam Pembangunan (Kumpulan Karya Tulis) (2022). Penerbit Alumni, Bandung.
- Manovich, L. (2022). Trending: The Promises and the Challenges of Big Social Data. In M. K. Gold (Ed.), Debates in the Digital Humanities (pp. 460–475). Minneapolis, MN: the University of Minnesota Press
- Mayer-Schönberger, V., & Cukier, K. (2019). Big Data: A Revolution That Will Transform How We Live, Work and Think. London: John Murray
- Mah-Noor Bint-Tariq, Haitham Nobanee, Business Ethics, and Finance: A Mini-Review, SSRN Electronic Journal · February 2019
- OJK, Penyelenggara Fintech Lending Terdaftar dan Berizin di OJK per 25 Agustus 2021 <https://www.ojk.go.id/id/kanal/iknb/financial-technology> Diakses 5 Oktober 2021 Jam 16.44 WIB
- OJK, Laporan Tahunan OJK, 2018, Laporan Tahunan OJK 2018.pdf Diakses 2 Oktober 2021 Jam 12.13 WIB
- Rabhi L, Falih N, Afraites A, Bouikhalene B. Big data approach and its applications in various felds: review. Proc Comput Sci. 2019;155(2018):599–605. <https://doi.org/10.1016/j.procs.2019.08.084>
- Rob Kitchin, (2014), Big Data, new epistemologies and paradigm shifts, Big Data & Society April–June 2014: 1–12

International Journal of Global Community
Volume VI No.1 (March), 2023

Seno wibowo gumbira,Dhiana Puspitawati, Kukuh tejo Murti, Unefficiency Settlement Of Fintech Lending Disputes And How Legal Framework To Settle It: Indonesia Perspective, Journal of Contemporary Issues in Business and Government Vol. 27, No. 2, 2021 <https://cibg.org.au/> P-ISSN: 2204-1990; E-ISSN: 1323-6903 DOI: 10.47750/cibg.2021.27.02.413 Published by Society of Business and management.

Schwab, K. (2016). The Fourth Industrial Revolution. New York: Crown Business