Jurnal Kajian Ilmiah
e-ISSN: 2597-792X, ISSN: 1410-9794
Vol. 21 No. 2 (Mei 2021), Halaman: 51 – 60
Terakreditasi Peringkat 5 (SINTA 5) sesuai SK RISTEKDIKTI Nomor. 3/E/KPT/2019

The Fintech Phenomenon: Protection of Consumer Privacy Data in Online Lending

Ika Dewi Sartika Saimima [1,*], Valentino Gola Patria [1]

[1] Fakultas Hukum; Universitas Bhayangkara Jakarta Raya; Jl. Perjuangan 081, Marga Mulya, Bekasi Utara, 021-88955882; e-mail: ikasaimima@gmail.com, tvalen223@gmail.com

* Korespondensi: e-mail: ikasaimima@gmail.com

Submitted: **08/04/2021**; Revised: **15/04/2021**; Accepted: **22/04/2021**; Published: **27/05/2021**

Abstract

Financial technology innovation that occurs nowadays leads to accelerated changes in the financial sector. However, these developments are like double-edged swords, on the one hand they provide convenience for consumers, on the other hand pose risks for consumers related to the confidentiality of their personal data. Money lending business through Peer to Peer lending (P2P lending) system often results in consumers receiving threats when they are late making payments. This paper presents several cases that result in consumers experiencing personal data theft, receiving threats directed at relatives or acquaintances. Even committing fraud by taking money from borrowers or customers without following the regulations made by the Financial Services Authority (OJK). The research data is carried out in a qualitative normative way where the data is translated based on legal norms and uses legal theory that can explain and answer existing legal problems.

***Keywords**: Consumer Protection, Peer to Peer lending (P2P lending), Private Data Protection*

Abstrak

Inovasi teknologi keuangan yang terjadi saat ini mengarah pada akselerasi perubahan di sektor keuangan. Namun perkembangan tersebut ibarat pedang bermata dua, di satu sisi memberikan kemudahan bagi konsumen, di sisi lain menimbulkan risiko bagi konsumen terkait kerahasiaan data pribadinya. Bisnis money lending melalui sistem Peer to Peer lending (P2P lending) seringkali mengakibatkan konsumen mendapat ancaman ketika mereka terlambat melakukan pembayaran. Makalah ini menyajikan beberapa kasus yang mengakibatkan konsumen mengalami pencurian data pribadi, menerima ancaman yang ditujukan kepada kerabat atau kenalan. Bahkan melakukan penipuan dengan mengambil uang dari debitur atau nasabah tanpa mengikuti ketentuan Otoritas Jasa Keuangan (OJK). Data penelitian dilakukan secara normatif kualitatif dimana datanya diterjemahkan berdasarkan norma hukum dan menggunakan teori hukum yang dapat menjelaskan dan menjawab permasalahan hukum yang ada.
Kata kunci: Peer to Peer lending (P2P lending), Perlindungan Konsumen, Perlindungan Data Pribadi

Kata Kunci*:* Perlindungan Konsumen*, Peer to Peer lending (P2P lending),* Perlindungan Data Pribadi

1. Introduction

The growth of the financial technology (fintech) industry phenomenon in Indonesia currently has great opportunities in conducting transactions online. Online money lending applications are spread across various internet and social media platforms. Offering easy loan applications quickly, without collateral requirements is an attraction for the community. The

development of financial technology that is currently developing consists of Peer to Peer lending (P2P lending), Crowdfunding, Market Aggregator, Digital Payment, and Risk and investment management. The rapid growth experienced by P2P lending in 2016 was 16% while in 2017 it grew to 32%.(Sari, 2018) The development of P2P lending eventually resulted in a high enough risk related to protecting personal data of consumers because they registered themselves on an online platform and involved third parties who received threats of violence via telephone or text. As a result of this act, the borrower of funds or fintech consumers are very disadvantaged because they have been defamed in which the personal data that has been entrusted given to the organizer of fintech is disseminated to others without the consent of the borrower of the fund.

Protection of personal data is an important factor so that consumers can be protected and ensure that there is no misuse that can harm financial consumers, including the use of data that requires consumer approval if a financial service institution is to be used to offer financial products and/or services (OJK, 2019). Protection of personal data is a government effort and a form of recognition of human rights so that people do not just enter into someone's private domain. Lending money through P2P lending on financial technology must look at the balance between the ease and flexibility of the technology offered. Aspects of regulation and consumer protection are important (Anagnostopoulos, 2017) because they relate to the security of a person's personal data. Regulators must be able to ensure and supervise financial technology by taking into account several factors such as security, consumer protection, services and criminal acts that occur in cyberspace (Dehghan & Haghighi, 2015).

Personal data is certain personal data that is stored, maintained, and maintained for the truth and is protected by its confidentiality (Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Dalam Sistem Elektronika, 2016).

Some cases that occur in financial technology in Indonesia can be seen in the following table:

Table 1. Financial Technology Case In Indonesia

No	Year	Company	Cases
1	2018	RupiahPlus (RP)	Billing is done to debtor friends who do not know about the loan. Billing is done roughly and discriminatively through text messages or telephone
2	2018	PT Vcard Technology Indonesia.	Case YI (51), a woman from Solo, Central Java. The picture was distributed and said to be willing to commit immoral acts to repay online lendings.
3	2018		Z (35), a taxi driver was found dead hanging himself in a boarding house on Jalan Prapatan VII, Tegal Parang, South Jakarta. Experienced severe stress due to being continuously billed with interest that continued to rise every day. Z had written a letter containing his application to the Financial Services Authority (OJK) and the authorities to

No	Year	Company	Cases
			eradicate parties who provide loans online (OJK).
4	2019	PT Vega Data dan Barracuda Fintech	Illegal and unregistered company in OJK. The modus used is by utilizing text message blast to hook hundreds of thousands of customers. The company does not charge interest for residents who borrow money from them. However, they deducted the customer's loan fund at the beginning for administrative reasons.

Source: Research Data (2019)

Based on the description of some of these cases, this paper would like to discuss criminal sanctions that can be imposed on companies that commit criminal acts of theft of personal funds, make distributions related to consumer personal loans and legal remedies that consumers can do if experiencing intimidation.

2. Methodology

The research method in this paper uses a juridical normative approach, which uses library data search. The use of legislation such as Law Number 19 Year 2016 concerning Information and Electronic Transactions and the Draft Law (Draft) on Protection of Personal Data and the Financial Services Authority (OJK Law) regulations. Secondary legal materials in the form of literature and documents relating to problems in this study. Data analysis method is qualitative normative, that is the data obtained will be interpreted based on legal norms and relevant legal theory in the form of sentence descriptions so that the answers to the problem can be obtained as a conclusion.

3. Result and Discussion

This financial technology is also inseparable from the borrower's responsibility if it defaults on the lender. The basic principle of accountability on the basis of mistakes means that a person must be responsible because he made a mistake and harmed others. According to civil law, the basis of responsibility is divided into two types, namely liability based on error (lilability without based on fault) and on the basis of risk or without fault (known as strick liability) (Bambang Poernomo, 1994). Accountability for default claims based on Article 1234 of the KUHPerdata in default, the money borrower will be held accountable if the elements of default are fulfilled, namely: Failure to fulfill his/her obligations at all; performs obligations but is late; performs obligations but is not in accordance with what it should be; doing what shouldn't be done. This means that consumers who borrow money online have an obligation to fulfill their debt payments on time. A delay in repaying a debt loan can be categorized as default, resulting in losses for the company. In P2P Lending transactions, the increase in default by borrowing money is quite large. Therefore P2P lending companies take remedial steps to return the bad loans by using a variety of ways, including using collectors or debt collectors.

Dian Purnama Anugerah in her writing mentioned that the P2P lending is a high risk instrument. In P2P the heaviest burden is to regulate the legal relationship between provider and lender. The worst scenario that can be suffered by lenders is when borrower is default. The lender has no guarantee that their money will return (unsecured creditors). Who has liability in this condition is depend on the agreement, whether the provider is jointly liable or not for the debt incurred. The join liability may arise when the service provider is neglect in performing risk analysis of the borrower. (Anugerah & Indriani, 2018)

High risk in P2P Lending technology is the problem of bad credit. People who make money loans make late installment payments, results in bad credit. Efforts are made to collect bad loans, usually entrepreneurs will hire a third party, namely the debt collector. In the billing process, debt collector behavior is often rude and even threatening. A debt collector in carrying out the collection task obtains using data from financial service businesses that have access to consumer data. The use of personal data of these consumers is illegal and violates the provisions of Article 26 of Law Number 19 Year 2016 concerning Information and Electronic Transactions. Personal data is a person's personal rights (privacy rights) to be able to protect his personal life and free from all kinds of interference. Other than that, a person also has the right to be able to communicate with others without spying and the right to supervise access to information about one's personal life and data. Until now, the fintech industry in Indonesia does not yet have special rules to provide protection for personal data of consumers as conducted by the Banking Law which guarantees the confidentiality of customer data.

In addition to the issue of personal data protection, legal issues related to the implementation of lending money in financial technology through P2P lending is that the company is not registered at the Financial Services Authority (OJK). The public is not aware that the company operating the loan online does not have an OJK permit. Based on reports from OJK, as of 30 November 2019, the total number of registered and licensed P2P lending providers was 144 companies. Meanwhile, from 2018 until November 2019, the FSA has blocked illegal engineering as many as 1898 entities.(OJK, 2019)

Table 2. Comparison of Legal and Illegal Financial Technology until November 2019

Fintech	Total	%
Legal fintech	144	7.05
Illegal fintech blocked by OJK	1898	92.95%
Total	2042	100%

Source: Data Prepared From OJK (2019)

As a result of the non-registered fintech company, OJK cannot supervise the performance of the company. Fintech companies are not allowed to access the contact list on the customer's phone without approval. Contact access made by the company aims to see the validity of consumer data. However, in practice there are a number of fintech organizers who misuse customer personal data where one of them accesses the contact on the customer's cellphone which is then used in billing, when not successful then followed up by accessing

whatsapp contact and spreading it to all contacts on whatsapp so that friends and colleagues and the family knows there are arrears to be paid.

Acts of intimidation and terror in collection of credit or loans in technology companies to customers are serious issues that are in the public spotlight. An increase in complaints is an indication that the practice of intimidating billing and terror in the technology companies is no longer a simple matter. In fact, the Indonesian Consumers Foundation (YLKI) has received complaints from consumers who have been victims of such forms and modes of billing, exceeding 100 reports. From the number of reports dominated by bullying billing cases and strangling loan interest rates. Complaints of consumers who have been victims of the fintech companies in the form of terror, daily fines, and/or sky-high commissions (Dinanti et al., 2020). The terrorist actions of the fintech Company to its customers are carried out by sending text to all consumer contact lists.

Intimidating billing is prohibited and should not be done in a technology company. These provisions are listed in the code of conduct and conduct or the Code of Conduct of the Indonesian Fintech Association (Aftech). The code of conduct requires all fintech companies to prioritize good faith in collecting loans from customers. The code of conduct also requires companies to have and submit settlement and billing procedures to customers, namely borrowers and lenders when loan defaults occur. Then, each organizer is required to convey to the customer the steps to be taken in the event of a loan delay or loan repayment failure.

The billing steps include the provision of warning letters, loan scheduling or restructuring requirements, correspondence with the recipient of the loan remotely (desk collection), including via telephone, email, or other forms of conversation. Then, the fintech company must also inform the customer about the schedule of a visit or communication with the billing team, loan write-offs. When using a third party in billing, the fintech company must use a party that is not a blacklisted authority (must be certified) or from the Association. Then, the fintech company is also prohibited from using intimidating, physical and mental violence or other methods that offend SARA or demean the dignity, dignity, and dignity of the recipient of the loan, in the physical world and in cyberspace (cyber bullying) both the recipient of the loan, his property, or relatives and his family.

If the consumer gets the treatment as described above, then the consumer can make criminal complaints against the P2P Lending Provider and third parties. Criminal provisions regarding threats are regulated in Chapter XXIII concerning extortion and threatening of the Criminal Code. Regarding the threat of violence regulated in Article 368 paragraph (1) of the Criminal Code: "Anyone with the intention to benefit themselves or others unlawfully, forcing a person with violence or threat of violence to give something, which is wholly or partly owned by that person or other people, or in order to make debts or write off receivables, are threatened because of extortion, with a maximum imprisonment of nine years ".

R. Soesilo in his KUHP, and his comments complete article by article, named the act in Article 368 paragraph (1) of the Criminal Code as extortion with violence in which the

extortionists: (R. Soesilo, 1991) 1) Forcing others; 2) To provide goods that completely or partially belong to the person himself or someone else's, or make a debt or write off a receivable; 3) With the intention of wanting to benefit oneself or others by opposing rights; 4) Forcing it by using violence or threats of violence.

If the threat fulfills the elements in Article 368 paragraph (1) of the Criminal Code, the perpetrators may be subject to criminal sanctions based on that article. If the threat is carried out through electronic media, then the perpetrators of threats can be subject to criminal sanctions in accordance with Law Number 19 of 2016 concerning Information and Electronic Transactions, namely Article 29 of the ITE Law jo. Article 45B of Law Number 19 Year 2016.

Article 29 of the ITE Law states: "Everyone intentionally and without the right to send electronic information and/or electronic documents that contain threats of violence or intimidation that are intended personally."

Article 45 B of Act 19/2016 states: "Any person who intentionally and without the right to send Electronic Information and/or Electronic Documents containing threats of violence or intimidation addressed personally referred to in Article 29 shall be sentenced to a maximum imprisonment of 4 (four) years and/or a maximum fine a lot of Rp.750,000,000.00 (seven hundred fifty million rupiah)."

In the explanation of Article 45B of Law Number 19 Year 2016 concerning Information and Electronic Transactions, it is explained that the provisions in this Article also include harassment in cyberspace which contains elements of threat of violence or intimidation and result in physical, psychological, and /or violence. material loss. The perpetrators can be criminally processed. The regulation does not state that the act constitutes a complaint offense, so it is understood that the provisions in Article 45B are an ordinary offense, so that everyone can submit a report to the Investigating Officer of the Republic of Indonesia State Police or Civil Servant Investigator for immediate action. Some of the cases above prove that consumers need to get legal protection through regulations, controls and regulatory arrangements related to the implementation of P2P lending technology.

Az. Nasution wrote that consumer protection is part of the law that contains the principles or rules that govern relationships and also contain properties that protect the interests of consumers.(*Departemen Perlindungan Konsumen OJK*, 2017) In borrowing money through P2P lending on technology, a balance is needed between the ease and flexibility of technology offered by fintech with aspects of regulation and consumer protection. Regulator can oversee technology by taking into account factors such as security, consumer protection, services, (especially the risk of information technology and cyber crime) (Az, 2002).

Jeremy Bentham said that the purpose of law is to realize only those that are beneficial (benefits). The law has a goal to provide as much happiness (benefit) as possible to the maximum amount (the greatest happiness for the greatest numbers).(Tolib, 2007) Law aims to perfect life, control excess, advance equality, and maintain certainty. Therefore, to provide legal

certainty for consumers using P2P lending technology, it is necessary to arrange and enforce law so that consumers can obtain their rights and carry out their obligations.

To protect consumers and provide legal certainty, the Government of Indonesia is currently preparing a Bill on the Protection of Personal Data. In the academic text of the Personal Data Protection Bill it is stated in article 18 that the Processing of Personal Data must meet the provisions of the valid approval of the Personal Data Owner for one or several specific purposes that have been submitted to the Personal Data Owner. Consent is not required in terms of processing Personal Data for: fulfillment of agreement obligations in the event that the Owner of the Personal Data is one of the parties or to fulfill the request of the Owner of the Personal Data at the time of entering into an agreement; fulfillment of legal obligations from the Controller of Personal Data in accordance with statutory provisions; fulfillment of protection of the legitimate interests (vital interests) of Personal Data Owners; the exercise of the authority to control Personal Data in accordance with statutory provisions; fulfillment of obligations of Controlling Personal Data in public services for public purposes; and / or fulfillment of other legitimate interests by taking into account the objectives, needs, and balance of interests of the Controller of Personal Data and the rights of the Owner of Personal Data.

Based on the provisions of Article 18 paragraph (1), the provider of technology must submit the purpose for the use of personal data and must obtain approval from the owner of the personal data. Approval is also carried out in the case of the use of emergency contact or data contact (whether in the form of telephone numbers, e-mail addresses, etc.) contained in the device in the form of cellular telephone, computer or other devices, must be authorized by the owner of the emergency contact or the owner of the contact himself.

Article 20 of the Draft Law on the Protection of Personal Data also states that agreement clauses in which there are requests for Personal Data which do not contain explicit consent from the Owner of Personal Data may be declared null and void. Personal data that must be carried out in accordance with Article 21 confidentiality include processing Personal Data, the Controller of Personal Data must maintain the confidentiality of Personal Data. To control the use of personal data, certain obligations and / or rights are needed from the Controller of Personal Data or from the Owner of Personal Data in the fields of labor, social security, taxation, sector supervision including the financial sector, the administration of population administration, and/or social welfare which provides protection to the basic rights and interests of the Owner of Personal Data; protect the interests of Personal Data Owners who are not capable both physically and legally; and/or necessary for the benefit of the law enforcement process. Safeguards for consumers must also be based on the principle of data protection, especially matters relating to consumer privacy. Entrepreneurs in the technology sector must prioritize overall protection of consumer personal data. The principles of protecting personal data include the principle of collection, the principle of restriction, the principle of data quality, the principle of goal specification, the principle of security measures, the principle of disclosure, individual participation, and the principle of accountability. If the fintech company is not able to

provide protection about the personal data of the consumer, then he will not get the trust of the public. If the company is in violation of the provisions of the principle, the consumer can make a criminal complaint for the legal event that he experienced.

Criminal sanctions related to the protection of personal data are mentioned in Article 61, that if intentionally obtaining or collecting personal data that is not his property with a view to benefiting himself or others unlawfully or could result in losses to the Data Owner being sentenced to a maximum imprisonment of 5 (five) year or a maximum fine of Rp. 50,000,000,000.00 (fifty billion rupiah). If intentionally and unlawfully disclosing Personal Data that does not belong to him shall be punished with a maximum imprisonment of 2 (two) years or a maximum fine of Rp. 20,000,000,000.00 (twenty billion rupiah). Whereas anyone who intentionally and unlawfully uses Personal Data that is not his property can be sentenced to a maximum of 7 (seven) years imprisonment or a maximum fine of Rp.70,000,000,000.00 (seventy billion rupiah).

If the Law on Personal Data Protection is passed, then the criminal sanctions stipulated are expected to be able to discourage entrepreneurs from making intimidation and not illegally accessing consumers' personal data. Based on the principle of The Privity of Contract, every business actor is obliged to provide protection to consumers to protect consumers who have entered into contracts. Violations of personal data of consumers have significantly inconvenience, insecurity and threaten the safety of consumers. Fintech service providers must provide clear information about the terms and conditions of products/services in the agreement, using language that is easy to understand, given the level of financial literacy of the Indonesian people in general is still relatively low. The agreement is also prohibited from stating the transfer of responsibility or liability from the technician to the consumer (exoneration clause). Fintech service providers must also avoid the use of advertisements that have the potential to create misconceptions for consumers and the public.

Legal protection of the borrower's personal data in the application of financial technology money lending (fintech) through P2P lending must also be done repressively by cracking down on technicians who misuse the borrower's personal data as a consumer and to protect the interests of the public. Decisive action that can be imposed on legal fintech providers known to misuse the borrower's personal data as a consumer is regulated in Article 53 of the Financial Services Authority Regulation Number: 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, through administrative sanctions, fines, sanctions limiting business activities, freezing of business activities, and Revocation of license for business activities.

4. Conclusion

The implementation of the P2P lending fintech currently raises many legal issues, including the use of personal data of consumers without permission. The personal data is misused by the fintech company by giving threats via text messages. This intimidating action

threatens the mental health of consumers because it is done by lowering the dignity of the loaner through cyber bullying aimed at the loaner or relatives and family. The action finally enters into the realm of criminal law because it has threatened the security and comfort of consumers' lives.

To provide consumer protection to P2P Lending fintech users in Indonesia, today's society must be able to more carefully choose a company that can be trusted. The issue of several crimes experienced by P2P Lending fintech consumers currently makes consumers helpless because the access of personal data to be used as a threat if there is a breakdown of instalment payments. On the basis of this, consumers can make efforts to protect themselves through criminal charges for defamation, criminal use of personal data, regulations on consumer protection, and Financial Services Authority Regulation Number: 1/POJK.07/2013.

The government is also expected to ratify the Draft of Personal Data Protection Act. Ratification of the Draft Bill on Protection of personal data is expected to provide learning to P2P fintech companies. Apart from the government, the community must also protect themselves by understanding the concept of borrowing money through financial technology with P2P lending. The public must be aware of the law and educate themselves about the great value of personal data in this digital age. The public must understand that the impact of exploitation of personal data can be carried out by other parties and will be detrimental to them. Business in the digital era must be understood in detail by the public. People as consumers, on the one hand, will enjoy digital products or services that make it easier for them to work and in everyday life. However, the public must also understand that the use of online loans without knowledge of the development of Big Data, Blockchain and Cloud Computing will be very detrimental when their personal data is used by other parties.

Big Data is a technology in which the way it works relies on the personal data of individual individuals which is processed by certain algorithms which in turn can be used as a tool for business actors to make business expansion and strategies. Likewise with Blockchain, it is not uncommon for the resulting algorithm to spit out consumer personal data. Cloud computing as a means of storing data for consumers who rely on the internet network is very vulnerable to being exposed to cyber attacks which have an impact on the vulnerability of data leakage. The public must also be able to know and understand the agreement made between the lender and the loan recipient as outlined in electronic documents, one of which is the interests of the identity of the parties or personal data. Personal data is certain personal data that is stored and maintained for the truth and its confidentiality is protected.

The form of legal protection for the borrower's personal data in the financial technology loan application through P2P lending in a repressive way is to take firm action against legal financial technology actors and illegal financial technology actors who misuse the borrower's personal data as consumers and to protect the interests of the community.

Firm actions that can be imposed on legal fintech operators who are found to have misused the personal data of borrowers as consumers are regulated in Article 53 of the

Financial Services Authority Regulation Number: 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, which states: **1)** Financial Services Business Actors and/or parties violating the provisions of this Financial Services Authority Regulation shall be subject to administrative sanctions, among others in the form of: a. Written warning; b. Fines, namely the obligation to pay a certain amount of money; c. Restrictions on business activities; d. Suspension of business; and e. Revocation of business activity license. **2)** The sanctions as referred to in paragraph (1) letter b, letter c, letter d, or letter e may be imposed with or without the imposition of written warning sanctions as referred to in paragraph (1) letter a. **3)** The fine as referred to in paragraph (1) letter b may be imposed separately or jointly with the imposition of sanctions as referred to in paragraph (1) letter c, letter d, or letter e. **4)** The amount of the fine as referred to in paragraph (1) letter b shall be determined by the Financial Services Authority based on the provisions concerning administrative sanctions in the form of fines that apply to each financial service sector. **5)** The Financial Services Authority can announce the imposition of administrative sanctions as referred to in paragraph (1) to the public.

Daftar Pustaka

Anagnostopoulos, I. (2017). *FinTech and RegTech: Impact on Regulators and Banks*.

Anugerah, D. P., & Indriani, M. (2018). Data Protection in Financial Technology Services: Indonesian Legal Perspective. *IOP Conference Series: Earth and Environmental Science*, *175*(1), 12188. https://doi.org/10.1088/1755-1315/175/1/012188

Az, N. (2002). *Hukum Perlindungan Konsumen Suatu Pengantar*. Diadit Media.

Bambang Poernomo. (1994). *Asas-asas Hukum Pidana*. Ghalia Indonesia.

Dehghan, F., & Haghighi, A. (2015). E-money regulation for consumer protection. *International Journal of Law and Management*, *57*(6), 610–620.

Departemen Perlindungan Konsumen OJK. (2017).

Dinanti, D., Sakti, M., Irfani, I. ., & Pramita, S. . (2020). Politics of Law for the Protection of Debtors as Consumer in Fintech based Loaning Services. *UNNES LAW JOURNAL*, *6*(2), 427–444.

Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Dalam Sistem Elektronika, Pub. L. No. 20 (2016).

OJK. (2019). *Data Otoritas Jasa Keuangan Per Tanggal 30 November 2019*.

R. Soesilo. (1991). *Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal. Politeia – Bogor.* Politeia – Bogor.

Sari, A. . (2018). Perlindungan Hukum Bagi Pemberi Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending Di Indonesia. *Jurnal Uajy*.

Tolib, S. (2007). *Pokok-pokok Filsafat Hukum dalam Penelusuran Kepustakaan*. Penerbit Dewa Ruchi.