Legal Protection Of Customers Personal Data In Bank Financial Institutions

Dhian Indah Astanti 1, A.Heru Nuswanto2, Sukimin3
1,2,3Semarang University Faculty of Law
Email : dhian.indah@usm.ac.id

Abstract
Since the legal connection between consumers and banks is one built on trust, legal protection for customers is crucial given that banks are financial entities whose operation cannot be divorced from the role of customers. Every individual has personal data, which is something that is intrinsic to them and has to be secured since everyone has the right to privacy, which is guaranteed by the Republic of Indonesia’s 1945 Constitution and is a fundamental citizen right. The goal of this study is to identify the legal safeguards for the confidentiality of consumer information held by Bank Financial Institutions, as well as the legal actions that consumers may take in the event that their privacy is violated. This study employs a normative juridical research design, combining an analytical, historical, and legislative approach. The data type for the research specifications is secondary data, obtained through document/library research (Library Research), and the research standards call for analytical descriptive data. The research’s data is organized logically and methodically, examined using qualitative analytic techniques, and then presented in a qualitative report. The study’s findings indicate that state people have a constitutional right to privacy, which is the cornerstone of the legal protection of personal data. Both government control and self-regulation can be used to legally secure the personal data of customers. As of now, personal data is not legally based in any of Indonesia's laws or regulations. As a result, Indonesia lacks standards for the legal protection of personal data, making it unable to provide its residents with the best possible protection.

I. Introduction
In addition to safeguarding client cash, banks are required under Law Number 10 of 1999's Article 40 (1) to protect customer confidentiality and deposits from third parties who could damage consumers. In addition, those
who trust banks with the management of their money need to be shielded against the arbitrary activities of those institutions that can endanger their clients. Banks and their clients have a different connection than they would with any other contractual party. Nonetheless, unless otherwise mandated by relevant legislation, the bank is likewise required under this arrangement to keep its clients' secrets to itself. A lawyer and his client or a doctor and his patient are comparable to the relationship that exists between a bank and its customers. In other words, they both have a duty to protect patient, client, and consumer information.

Every person is entitled to constitutional rights, which are legal protections. The state is required by the constitution to safeguard all citizens, which includes protecting their fundamental rights. contained in the Preamble to the Fourth Paragraph of the 1945 Republic of Indonesia Constitution (1945 Republic of Indonesia Constitution), which declares that the state has a duty to safeguard the entire Indonesian population by enhancing general welfare, educating the populace, and enforcing a global order founded on social justice, independence, and peace. Article 28 G Paragraph (1) of the 1945 Republic of Indonesia Constitution guarantees citizens the right to personal security, family, honor, dignity, and property under their control. This right to self-defense is one of the rights guaranteed by the constitution. This article makes the assumption that personal rights are property rights. However, as information and communication technologies have advanced, personal rights should also be understood as privacy rights since they are more delicate and can stand in for property rights. To safeguard the right to privacy is to safeguard the right to free expression as well. Accordingly, the right to privacy ensures that one will not be threatened with the dread of acting on a human right or abstaining from it.

Any information that is connected to or has the potential to identify an individual is considered data privacy. A person's right to privacy must be upheld against exploitation of their personal data or the interests of third parties, including exploitation by family members. Banks must consider client protection factors while developing new financial technologies, such as online banking, particularly security that pertains to customer privacy.

Article 26 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions states that, unless otherwise specified by Legislative Regulations, the use of any information via electronic media pertaining to an individual's personal data must be done with that individual's consent. There are regulations that specifically govern the use of personal data, in this case customer personal data, in relation to the explanation of Article 26 paragraph (1) of Law Number 11 of 2008 concerning Information and Electronic Transactions. These regulations are found in Bank Indonesia Regulation Number 7/6/ PBI/2005, which governs provisions regarding Transparency of Bank Product Information and Use of Customer Personal Data. Law Number 11 of 2008's ITE provisions, including Article 26 paragraph (1), are operationalized
based on the BI rules.

The idea of getting to know your consumer is strongly tied to regulations pertaining to personal data of customers. "Principles that are applied bank to find out customer identity, monitor customer transaction activities including reporting suspicious transactions" is what the Know Your Customer Principles (KYCP) refer to, as stated in Article 1 point 2 of Bank Indonesia Regulation Number 3/10/PBI/2001, which was later amended by Bank Indonesia Regulation Number 5/21/PBI/2003. By prohibiting banking from being utilized as a weapon for financial crime, the know-your-customer concept contributes to the preservation of the integrity and reputation of the financial system. The know your customer concept is used with the understanding that it is crucial to safeguard banks from a variety of dangers when working with

The problem of legal protection for consumers' personal data when using online banking services is one that all parties, particularly customers, should be aware of. The goal of this is to safeguard consumers' rights to the personal information they own when managing their online banking. Regulation that employs a self-regulation strategy is insufficient as a tool for actual protection.

complete security of private client information. You should also be aware of the legal safeguards for customers' personal information when it comes to bank secrecy. Weak enforcement results from ignorance of the type of protection offered against violations that take place, particularly when it comes to the legal protection of consumers' personal data.

Law Number 8 of 1999 concerning Consumer Protection and Law Number 10 of 1998 about Amendments to Law Number 7 of 1992 concerning Banking ensure protection for all banking business operations in compliance with relevant standards and give logical outcomes for bank services.

Problems that will subsequently be used as material for study can be recognized based on the context that has been given. The research's characterization of the issue is how bank financial organizations' legal protection of their customers' personal data?

2. Research Method

In this research, the type of research used is normative legal research. Normative legal research attempts to find legal rules, legal principles, and legal doctrines to answer the legal issues faced. This research uses a statutory approach and an analytical approach. In essence, normative legal research is research that examines and analyzes legal norms that have been established by authorized officials for this purpose. The legal norms referred to here are

---

1Munir Fuady, *Hukum Perbankan Modern*, Bandung : PT.Citra Aditya Bakti,hlm 101
3Arie, *Perlindungan Hukum Privacy Data Nasabah dalam Penyelelanggaran Internet Banking*, 2015, hlm.2
Normative legal research is the sort of research that was employed in this study. In order to address the legal questions raised, normative legal study looks for legal theories, norms, and principles. Both an analytical and legislative approach are used in this study. Normative legal research, to put it simply, is the study of legal standards that have been developed for this reason by authorized officials. The legal standards being discussed here are those pertaining to Bank Financial Institutions' legal protection of their clients' personal information.

Analytical descriptive research, or research that completely and methodically explains the subject of the primary problem, is the type of research definition that will be applied. In order to make conclusions and produce a study about the legal protection of client personal data at Bank Financial Institutions, researchers examine and aggregate the data that has been gathered. According to Soerjono Soekanto, descriptive research aims to offer as much accurate information as possible on individuals, illnesses, or other symptoms. The findings of the analysis on the legal protection of bank financial institutions' consumers' personal data will be presented in this study.

Secondary data are required in order to gather objective data, as per the research methodology employed in normative legal research. This information was obtained through library research, or document/document analysis. Document/library study, according to Syamsudin, is the process of gathering, reviewing, or tracking down papers or other material that may contain information or information that researchers may need.

The research's data analysis approach is logically and methodically organized, examined utilizing qualitative analysis techniques, and then presented in a qualitative manner.

3. Results and Discussion

1. Legal Protection for Customers Regarding the Security of Personal Data at Bank Financial Institutions

Law Number 8 of 1999 concerning Consumer Protection provides legal protection for customers regarding the security of their personal data. It outlines their rights to comfort, security, and safety when consuming goods and/or services, as well as their right to compensation. Article 4 letter an of the law expresses these rights. Furthermore, "the right to have opinions and complaints regarding the goods and/or services used" is stated in Article 4 Letter D. This regulation gives customers the chance to report issues with the bank's online banking services. In exchange, the bank owes it to its customers to hear their concerns or comments.

One of the factors influencing a client's trust in a bank is personal information or the privacy of their customer data. The following justifies the protection of the right to privacy: In order to keep his status at a particular
level, a person must first conceal some aspects of his personal life while forming interactions with others. Second, in order for someone to truly require privacy, they must have some alone time in their lives. Third, although privacy is an unalienable right, it can be violated if a person discloses personal information to the public. Fourth, the freedom to have domestic relations—including how one constructs a marriage or other relationship—is equally covered by privacy. Builds a family and other people must not know about these personal relationships, so Warren calls it the right against the word.

Fifth, the incalculability of the damages incurred is another reason why privacy should be protected by the law. Since it has interfered with their personal life, the loss is believed to be far more significant than the actual loss, and if any loss occurs, the sufferer is entitled to compensation. The idea of data protection suggests that people should have the freedom to choose whether or not to share their personal information. In addition, people are entitled to choose the terms under which personal data may be transferred. Increased security for privacy. In order to create the right to protect personal data, the right to privacy has evolved.

Banks are required to maintain the confidentiality of personal data. A basic examination of the protection of personal data may be found in Article 26 paragraph (1) of Law Number 11 of 2008 respecting Electronic Information and Transactions. In this context, the security of personal data—particularly with regard to bank secrets—is briefly discussed in Law Number 10 of 1998 about Amendments to Law Number 7 of 1992 concerning Banking, namely in Article 40 paragraphs (1) and (2). Law Number 10 of 1998 about Amendments to Law Number 7 of 1992 concerning Banking defines bank secrecy as "anything related to information regarding depositors." This term is included in Article 1 number 28 of that law.

One of the regulations issued by Bank Indonesia is Number 7/6/PBI/2005 Concerning Transparency of Bank Product Information and Use of Customer Personal Data. This regulation was made in light of the fact that, in order to increase protection against customers' personal rights when dealing with the bank and to provide protection against the use of customers' personal data, internet banking transparency regarding the use of personal data submitted by customers to the bank is necessary. The restrictions that are now in place deal with concerns about client personal data, which may contain bank secrets.

Both government control and self-regulation can be used to legally secure the personal data of customers. The internal legal regulation approach of the service delivery itself is essentially where preventive legal protection of client personal data with a self-regulation approach is evident. When employing a government regulatory strategy to deploy internet banking, the legal protection of client personal data is centered on a set of regulations issued
by the government, which has the jurisdiction to impose these restrictions. The responsibility and power to establish and oversee banks has been delegated to Bank Indonesia. It will achieve this by implementing preventative measures, such as guidelines, advice, instructions, and direction, as well as repressive actions, such as inspections and subsequent action, an act of correction.

Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking (UU Banking) is the law that, in this case, is the instrument for protecting customer personal data when internet banking is implemented. These provisions must be closely related to the issue of legal protection for customer personal data.

Two provisions in the Banking Law, specifically Article 29 paragraph (4), which states that banks "are obliged to provide information regarding the possible risk of loss arising in connection with customer transactions carried out through the bank for the interests of customers," may be used to determine and provide legal protection for customers' personal data when providing internet banking services. Then, according to Article 40, paragraphs (1) and (2), "(1) banks must maintain the confidentiality of information pertaining to depositors and their deposits, with the exception of situations covered by Articles 41, 41A, 42, 43, 44, and 44A.

The clauses in paragraph (1) as intended also apply to parties that are linked. Article 29 paragraph (4) explanation of provisions states that the purpose of disclosing information about potential customer loss is to increase transparency in the banking industry by making information about business operations and bank conditions more accessible. Regarding bank secrecy, Article 40 paragraph (1) states that banks are required to maintain the confidentiality of all information pertaining to finance as well as other information from individuals and organizations that the bank knows about due to its business operations. Filing a complaint in line with applicable laws provides effective legal protection if the personal data of online banking users is not secured in compliance with Bank Indonesia Regulation (PBI) Number 10/10/PBI/2008 Regarding Resolving Customer Complaints, as well as Bank Indonesia Regulation (PBI) Number 7/7/PBI/2005. Customer representatives, in writing, or orally, may handle complaints through the complaint system (Bank Indonesia: 2005).

In addition, it may be accomplished by joint agreement-based mediation between the client and the banking party, as outlined in Bank Indonesia Regulation (PBI) Number 8/5/PBI/2006 and PBI Number 10/1/PBI/2008 about Banking Mediation. Customer personal data is governed by Law Number 11 of 2008 concerning Information and Electronic Transactions, namely Article 21 paragraph (2) A, (2) B, (2) C, (3), (4), and (5), as well as Article 26 paragraph (1) and (2). These regulations apply to online banking transactions.

Customers in particular need to be aware of their legal protection for the
personal data they own. Bank Indonesia Regulation Number 9/15/PBI/2007 concerning the Implementation of Risk Management in the Use of Information Technology in Commercial Banks was issued by Bank Indonesia, the regulatory body and supervisor of banking activities in Indonesia, to help all banks that use information technology reduce the risks associated with their operations. Because there is now no law in Indonesia that expressly governs online banking, this rule is applied. However, online banking employs information technology to carry out its operations, and this utilization of technology necessitates the control of potential dangers, leading to the creation of management dangers that are controlled by Bank Indonesia.

Article 25 of Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector outlines additional provisions pertaining to the protection of customers in the financial services sector. Specifically, Article 25 requires financial services business actors to uphold the security of customer savings, funds, or assets that they are responsible for. Financial Services Business Actors are forbidden from giving their customer data and/or information to other parties in any manner, according to Article 31 Paragraph 1. According to paragraph (2) of Article 31, if the customer provides written authorization or if it is mandated by statutory requirements, the ban as stated in paragraph (1) is not applicable. According to Article 31 Paragraph (3), if a Financial Services Business Actor receives personal information about an individual or group of individuals from another party and plans to use that information for its operations, the Financial Services Business Actor must have written confirmation that the other party has received written consent from the individual or group to disclose the personal information to any party, including Financial Services Business Actors. Customers are protected by these provisions in the event that abuse of their personal information connected to bank secrets is brought to light.

2. Protection of Personal Data in Legislation in the Financial Services Sector

Financial Services Authority Regulation Number 13/POJK.02/2018 concerning Digital Financial Innovation in the Financial Services Sector

The norms regarding personal data protection in POJK No 13/2018 are:

1. 1. The principle of independent monitoring: OJK mandates that organizers implement the principle of independent monitoring, which includes the following at minimum: a. principles of information and communication technology governance in compliance with statutory regulations; b. consumer protection in compliance with this Financial Services Authority Regulation; c. consumer education and outreach; d. confidentiality of consumer data and/or information, including transaction data and/or information; e. principles of risk management and prudence; f. principles of anti-money laundering and prevention of terrorism financing in accordance with statutory provisions; and g. inclusivity and the principle of information...
transparency.

2. Data centers in Indonesia: OJK mandates that coordinators find disaster recovery and data centers inside Indonesian borders.

3. Obligation to preserve data confidentiality: From the moment that data is acquired until it is deleted, the organizer is required to preserve the confidentiality, integrity, and accessibility of the transactional, financial, and personal data that it handles. The following conditions must be satisfied in any provisions for the use of user data and information that the organizer obtains: Users’ consent must be obtained in the following ways: a. by communication of usage restrictions and information; b. through communication of any changes in the purpose of utilizing data and information to users; and the media and methods used to obtain data and information guarantee confidentiality, security and integrity.

4. Protection of Consumers Organizers are required to adhere to the fundamental principles of consumer protection, which include: a. handling complaints and resolving consumer disputes in a straightforward, timely, and cost-effective manner; b. handling fair treatment; c. being dependable; d. maintaining the confidentiality and security of consumer data and information. It is mandatory for organizers to offer technology-driven customer support centers. At the very least, technology-based customer care centers offer customer service centers that may be operated on their own or in collaboration with third parties.

5. Financial literacy: Activities aimed at promoting financial inclusion and literacy must be carried out by organizers.

6. The Ban. First, it is against the law for organizers to give third parties data or information about their patrons. The ban as stated in paragraph (1) is excluded, with the following exception the prohibition as intended in paragraph (1) is excluded if: a. the consumer gives consent electronically; and/or b. the organizer is required by statutory provisions to provide data and/or information regarding the consumer to a third party. Cancellation or change of part of the approval for disclosure of data and/or information as intended in paragraph (2) letter a is carried out electronically by the consumer in the form of an electronic document.²

²Pasal 18 ayat (1)
³Pasal 29
⁴Pasal 30 ayat (1)
⁵Pasal 30 ayat (2)
⁶Pasal 31 ayat (1)
⁷Pasal 31 ayat (2)
⁸Pasal 6 ayat (3)
Financial Services Authority Regulation Number 77/POJK.01/2016 concerning Information Technology-Based Money Lending and Borrowing Services

The following are the guidelines for managing personal data that are included in POJK 77/2016:

1. Fundamentals of User Protection. In accordance with Article 29 POJK 77/2016, organizers are required to put into practice the following fundamental user protection principles: a. transparency; b. fair treatment; c. dependability; d. data confidentiality and security; and e. easily, swiftly, and reasonably addressing user complaints.

2. The Maximum Loan Amount. The maximum amount of IDR 2,000,000,000.00 (two billion rupiah) that can be granted as loan money under the terms mentioned in paragraph (1).

3. Licensing and registration requirements

4. Incapacity to operate;

5. Dependent on agreement. The organizer-lender agreement and the loan recipient-lender agreement are both included in the Agreement for the Implementation of Information Technology-Based Money Lending and Borrowing Services.

4. Conclusion

1. The personal data of bank clients is still not completely protected by a number of bank confidentiality rules that have not been adequately enforced. This is evident from the fact that a lot of consumers are still uneasy about third parties using their personal information to present them with offers of other items.

2. Because there are still issues that customers face as a result of customer data being leaked to third parties and because the bank is still not fully attending to customer complaints about leaked personal data to the authorities, the bank's obligation to maintain the confidentiality of customer personal data cannot yet be implemented as stipulated in the customer data protection legislation.

3. Bank clients who report to the bank the use of their data without consent may pursue legal action if they feel disadvantaged as a result of third parties distributing and using their information.
References

a. Book


b. Legal regulations:

Sekretariat Negara RI. *Undang-Undang No. 7 Tahun 1992 tentang Perbankan*. Jakarta, 1992


c. Journals:


Sekaring Ayumeida Kusnadi. “Perlindungan Hukum Data Pribadi Sebagai Hak Privasi”. Al Wasath Jurnal Ilmu Hukum, Volume 2, Nomor 1, April 2021: 9-16

Parida Angriani. “Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce”
Perspektif Hukum Islam dan Hukum Positif. Jurnal Syariah dan Hukum, Volume 19 Nomor 2, Desember 2021: 149-165


