VARIA JUSTICIA

Varia Justicia
Vol. 16 No. 1 (2020) pp. 39-47
pISSN: 1907-3216 | eISSN: 2579-5198

A Shift in The Principle of Bank Secrecy due to Advancement in Information Technology

Budi Agus Riswandi
Faculty of Law, Universitas Islam Indonesia, Yogyakarta, Indonesia
*email: budiagusr@uii.ac.id

DOI: https://doi.org/10.31603/variajusticia.v16i1.3336

Submitted: February 2020 *Revised: March 2020* *Accepted: April 2020*

Keywords:
Bank Secrecy, Advancement in IT, Bank Principle

ABSTRACT

Bank secrecy is a conditional legal agreement used by a bank to guarantee the confidentiality of customers' dealing and financial affairs. However, the advancement in information technology, especially in the implementation of electronic systems and transactions across banks, has introduced tremendous changes in the ability of financial institutions to efficiently secure customers' data. This study provides a detailed explanation of the transformation process using the normative method. The result showed a shift in the principle of bank secrecy to data security in the event of a violation.

1. INTRODUCTION

The banking sector is devoted to the holding of financial assets for its customers. In addition, the core objective of banks, is to build trust with its customers, therefore, a variety of strict legal rules are put in place to ensure adequate implementation and adherence. The legal rules are made both by the government as well as between banks and their customers. According to Julapa Jagtiani, the relationship between banks and customers is bound by rules made to protect consumers' information and regulated by the government.[1]

Muhammad Djumhana stated that bank secrecy is the security, confidentiality, and privacy of a client's foregoing financial activities. In this case, all data and information related to finance, and other commodities need to be kept confidential.[2] The prevailing principle of bank secrecy is currently undergoing a shift in meaning with different legal consequences, due to the expansion from conventional methods to electronic system-based patterns. Therefore, the laws guiding the protection of customer's

[1] Julapa Jagtiani, "Fintech: The Impact on Consumers and Regulatory Responses," *Journal of Economics and Business* 100 (2018).

[2] Muhamad Djumuhana, *Hukum Perbankan Di Indonesia* (Bandung: Citra Adya, 1993).

personal data are amended. The Indonesian banking sector also practices this principle, as stated in Article 1, number 28 of Law No. 7 of 1992 and Law No. 10 of 1998. According to these laws, bank secrecy is related to the various information regarding the deposits and withdrawal activities carried out by customers. This is further explained in Article 40 paragraph (1) and (2) of Law no. 7 of 1992 and Law No. 10 of 1998, which stated the following: (1). banks need to keep customers deposit information except in rare cases, as referred to in Article 41, 41A, 42, 44, and 44A. (2) The provisions referred to in paragraph (1) is also applicable to affiliated parties. This principle was also strengthened with the issuance of Financial Services Authority Regulation No. 1/POJK.07/2013 concerning Consumer Protection and Bank Indonesia Regulation No. 16/1/PBI/2014. In these two regulations, it is stated that banks need to apply the consumer protection with the principle of confidentiality and security of personal data.

The application of these rules liquefies the strict provisions on bank secrecy, which focuses on the principle with more attention to the confidentiality and security of customers' data. Furthermore, provisions that expand the principle of bank secrecy regarding the confidentiality and security of personal data have deviated from conventional to electronic systems bound by the provisions of Law No. 11 of 2008 concerning Electronic Information and Transactions. According to Article 26, paragraph (1) and (2) of Law no. 11 of 2008, (1) Unless determined by legislation, the use of any private related a customer's personal data need to be conducted with the approval of the person concerned, (2) Any person whose rights are violated as referred to in paragraph (1) has every right to file a claim for losses incurred under this Law. In addition, Article 26 paragraph (1) and (2) of Law no. 11 of 2008 emphasizes that approval need to be obtained from customers regarding the provision of their personal data to a third party. Therefore, in terms of violation of the confidentiality and security of personal data in relation to electronic system-based bank activities, the perpetrator is subject to sanctions as stipulated in Law No. 7, 10, and 11 of 1992, 1998, and 2008, respectively. Based on the description, it is therefore, necessary to study and explore the shift in the meaning of bank secrecy and the legal consequences in electronic system-based banking activities in Indonesia.

2. RESEARCH METHODS

This is a normative juridical research, which focused on the rule of law. The normative legal research is carried out by studying the meaning of bank secrecy, and its regulations related to the implementation of electronic systems and transactions. This study aims to determine the legal consequences associated with the implementation of electronic systems and transactions in accordance with the laws and regulations in Indonesia. Data were obtained from secondary sources in the form of primary legal materials, such as Law No. 7, 10, and 11 of 1992 1998 and 2008 on Financial Services

Authority Regulation. In addition to law No.1/POJK.07/2013, No. 16/1/PBI/2014, and No 82 of 2012 on Government Regulation. Data were also obtained from Regulation of the Minister of Communication and Information Technology Number 20 of 2016, legal materials in the form of books, research results, scientific journals, and dictionaries. The obtained data were descriptively and qualitatively analyzed.

3. RESULTS AND DISCUSSION

3.1. The Shift associated with the Principle of Bank Secrecy due to the implementation of Electronic Transactions

Initially, banks were concerned with the principle of secrecy, however, the development of privacy concept, led to the concern with the principle of confidentiality and security of personal data. Werner De Capitani stated that this technique existed during the time of the Hamurabi Code, some 4000 years ago, with financial privacy associated with personal data.[3] This time, the shift was felt faster due to the strong influence of information technology advancement. Moor stated that privacy is a difficult concept to understand because it changes periodically and is often influenced by the political and technological features of the society.[4]

David Banisar defined privacy as a broad concept relating to the protection of individual autonomy and society.[5] Floridi stated that there are two theories of information privacy, namely reductionist and ownership-based interpretations. According to reductionist interpretations, the privacy of information is valuable because it preserves unintended consequences due to violation. Meanwhile, ownership-based interpretation views that everyone has the information.[6] Privacy is considered important in protecting the ability of individuals to develop ideas and personal relationships. Personal experiences and cultures strongly influence their notion in some countries. For example, European countries are susceptible to privacy due to the several violations experienced during the Second World War.[7] Samuel Warren and Louis Brandeis, which stated a person's rights are irrevocably protected from intrusion or unwanted disclosure. This term

[3] Werner De Capitani, "Banking Secrecy Today," *U. Pa. Journal Int'ernational Bussines Law* 10, no. 1 (1988).

[4] Jacques Pelteret, Marc and Ophof, "A Review of Information Privacy and Its Importance to Consumers and Organizations," *The International Journal of an Emerging Transdiscipline* 19 (2016): 23-35.

[5] David Banisar, "The Right to Information and Privacy: Balancing Rights and Managing Conflicts, Washington DC: The International Bank for Reconstruction and Development /TheWorld Bank," *Sabaragamuwa University Journal* 15, no. 1 (2011): 1–7.

[6] Pelteret, Marc and Ophof, "A Review of Information Privacy and Its Importance to Consumers and Organizations."

[7] Banisar, "The Right to Information and Privacy: Balancing Rights and Managing Conflicts, Washington DC: The International Bank for Reconstruction and Development /TheWorld Bank."

is called the "right to be alone," and it was accepted in the Bill of Rights of the United States constitution.[8]

Due to the advancement in the use of information technology, the concept of privacy which initially focused on caring for customers data shifted to protecting the personal interests by providing banks with the right to control data, reject certain types of processing, right to claim/forget the its portability. [9]

This led to a shift in the principle of bank secrecy to confidentiality and data security in Indonesia, as stated in Law No. 7 and 10 of 1992 and 1998. According to Adrian Sutedi, Article 40 paragraph (1) of these laws stated that banks are required to keep information on their customers' deposits.[10] Rachmadi Usman reported that all data information related to finance and other matters need to be kept confidential. This article also emphasized several interests exempted from the bank's secrecy obligations, as discussed in subsequent chapters. Firstly, managers of Indonesian Banks, has the authority to issue written instructions to banks to provide information, show written evidence and letters regarding the financial condition of certain customers' financial statement to tax officials, upon request by the Minister of Finance in accordance with Article 41. Secondly, the Chairperson of Indonesian banks grants permission to officials of the State Receivables and Auction Agency to obtain information regarding a customer debtor, as stated in Article 41A. Thirdly, the Chairperson of Bank Indonesia grants permission to the police, prosecutors, or judges to obtain information from banks regarding the depositor for the judiciary in criminal cases, as stated in Article 42. Fourthly, in the context of exchanging information between banks, the directors have the ability to notify the customers' financial condition to other banks, as reported in Article 44). Finally, based on the request, approval, or authority of the customer made in writing, the bank is obliged to provide the information their personal information as reported in Article 44A.[11]

According to Article 40, paragraphs (2) of Law no. 7 of 1992 Jo and Law No. 10 of 1998, affiliated parties are excluded from the bank's confidential obligations. This is explained in details as follows:

1. Members of the Commissioner Boards, supervisors, directors, officers, or bank employees,

[8] Will Thomas De Vries, "Protecting Privacy in The Digital Age," *Berkeley Technology Law Journal* 18 (2003): 283.

[9] Bart van der Sloot, "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data,'" *Utrecht Journal of International and European Law 25* 31, no. 80 (2015).

[10] Adrian Sutedi, *Hukum Perbankan Suatu Tinjauan Pencucian Uang, Merger, Likuidasi, Dan Kepailitan* (Jakarta: Sinar Grafika, 2008).

[11] Rachmadi Usman, *Hukum Perbankan* (Jakarta: Sinar Grafika, 2001).

2. Members of the management, supervisors, managers, officials, or employees of banks in the form of cooperative law and accordance with regulations,
3. Parties that provide services to banks, such as public accountants, appraisers, and legal consultants,
4. The various parties that have influenced the management of banks, such as shareholders, Commissioners, supervisors, directors, and the manager's families.

In line with the provisions of bank secrecy, business activities are also provided with the obligation to implement consumer protection with the principle of confidentiality and security of personal data. This is observed in the provisions of Financial Services Authority Regulation No. 1/POJK.07/2013 on Consumer Protection in accordance with Bank of Indonesia Regulation No. 16/1/PBI/2014 on Consumer Protection in Payment System Services, where bank obligations guarantee the principle of bank secrecy, confidentiality, and security of data.

The obligations regarding the confidentiality and security of personal data regarding electronic systems implementation, used by banks are also bound by the provisions of Article 26 paragraph (1) of Law no. 11 of 2008 on Electronic Information and Transactions. This law stated that "Unless determined by the legislation, the use of customers' personal information through electronic media needs the consent of the person concerned." This provision emphasizes the importance of protecting the personal data of electronic media users. According to Article 26, paragraph (1) of Law no. 11 of 2008, personal rights is a customer’s right to achieve the following: (1). enjoy private life and free from all kinds of distractions, (2). communicate with others without spying, (3). monitor access to information regarding one's personal life and data. Furthermore, it is the obligation to maintain confidentiality and personal protection to further strengthen the provisions of Article 15 Government Regulation Number 82 of 2012 on the Implementation of Electronic Transactions and Systems.

This shift, due to technological advancement, is obliged to maintain the confidentiality, integrity, and availability of personal data. It also guarantees the acquisition, disclosure, and utilization of personal data based on the owner's approval and in accordance with the objectives. According to article 1 paragraph (1) in the Regulation of the Minister of Communication and Informatics Technology Number 20 of 2016, personal data that is stored, maintained, and protected for confidentiality. Meanwhile, Article 1 paragraph (2) on the Regulation of the Minister of Communication and Informatics Technology Number 20 of 2016 stated that a customer's data is identified both directly and indirectly to each individual in accordance with statutory provisions. The protection of personal data in the form of confidentiality is also contained in Articles 26, 27, and 28 of the Ministerial Regulation of Communication and Informatics Number 20 of 2016.

The various laws and regulations regarding bank secrecy led to the following conclusions (1). A bank in carrying out its business activities is bound by the principle of bank secrecy as regulated in Article 40 of Law No. 7, and 10 of 1992 and 1998 Jo, respectively. It is also in accordance with the Financial Services Authority Regulation No. 1/POJK.07/2013 on Consumer Protection and No. 16/1/PBI/2014 on Payment System Service. (2). Banks that carry out their business activities by utilizing electronic systems and transactions are also bound by the provisions of Law No. 11 of 2008 on Information and Electronic Transactions Jo, Government Regulation Number 82 of 2012 on Implementation of the System and Electronic Transactions Jo, and Regulation of the Minister of Communication and Informatics Number 20 of 2016 on Protection of Personal Data in Electronic Systems.

The implementation of electronic transactions and systems shows that bank secrecy broadly shifted to the protection of personal data with a very broad scope, in accordance with the banking sector. In line with this understanding, banks are obligated to guarantee the customer's personal data are protected by providing the right to control, reject, process, and carry out claims.

3.2. Legal Consequences of Violation and Shifts in Principles of Bank Secrecy in implementing Electronic Systems and Transactions in the Banking Sector

This section analyzes the various consequences of violating bank secrecy principles in line with the provisions of Law No. 7 and 10 of 1992 and 1998 Jo, respectively, which stated that, assuming there is a violation of bank secrecy, the violator is held liable in accordance with criminal, civil and administrative laws.

The violation of bank secrecy is an act of crime, as shown in Article 51 of Law No. 10 of 1998. According to this law, which stated that criminal acts in Articles 46, 47, 47A, 48 (paragraph 1), 49, 50, and 50A are crimes minimum sanctions of IDR. 4,000,000,000 (four billion) to IDR. 200,000,000 (two hundred billion).

In addition, the violations of bank secrecy are for administrative responsibility, carried out by Bank Indonesia (BI). These responsibilities are as follows:

1. Money fines,
2. Written warning,
3. Decreasing bank reputation,
4. A prohibition from participating in clearing activities,
5. Suspension of certain business activities in all branch offices,
6. Dismissal of a bank manager and subsequently hire temporary substitute till a general meeting of shareholders is conducted with the approval of Bank of Indonesia,
7. Inclusion of members, managers, bank employees, shareholders in the list of disgraced people in the banking sector.

For civil liability, these laws are not regulated in specific articles, regarding the material of the lawsuit and the legal remedies. However, this matter is regulated based on civil provisions, and this is subject to compensation claims based in accordance with Article 1365 of the Civil Code.

The violation of bank secrecy relating to the obligations contained in the Financial Services Authority Regulation Number 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector, is related to administrative sanctions. This is found in Article 53 of the Financial Services Authority Regulation No.1/POJK.07/2013 on Consumer Protection in the form of the following:

1. Written warning,
2. Fines or obligations to pay a certain amount of money,
3. Limitation of business activities,
4. Suspension of business activities, and
5. Revocation of business license

However, the Imposition of administrative sanctions can be imposed either individually or in groups. During violation of bank secrecy, the sanctions set out in Bank of Indonesia Regulation No. 16/1/PBI/2014 on Consumer Protection of Payment System Services may be subject to administrative sanctions. This is stated in Article 29 paragraph (1) and (2). These sanctions are imposed as follows:

1. Written warning,
2. Fines,
3. Temporary suspension, in part or all payment system service activities,
4. Revocation of license for payment system service activities.

From these descriptions, it is clear that violations of the principle of bank secrecy have consequences for bank liability on both criminals, civil, and administrative law. However, criminal liability is only contained in the provisions of Law No. 7 and 10 of 1992 and 1998 Jo, respectively, while civil liability is contained in Financial Services Authority Regulation No.1/POJK.07/2013 Jo, and Bank of Indonesia Regulation No. 16/1/PBI/2014. Furthermore, administrative responsibilities have been regulated in Law No. 7 of 1992 Jo, UU no. 10 of 1998 Jo, Financial Services Authority Regulation No.1/POJK.07/2013 Jo, and Bank of Indonesia Regulation No. 16/1/PBI/2014. The above listed administrative sanctions are regulated in a variety of ways, with different models of sanctions imposed. The various responsibilities outlined in this study can be requested from the banking sector when conducting businesses assuming its services do not utilize the electronic systems and transactions.

However, when the reverse is the case, then the legal responsibility is need to be based on the provisions of Law No. 11 of 2008 on Information and Electronic Transactions Jo, Government Regulation Number 82 of 2012 on Implementation of Electronic Systems and Transactions Jo, and Regulation of the Minister of

Communication and Informatics Number 20 of 2016 on Protection of Personal Data in Electronic Systems.

The administrative responsibilities of these laws have been regulated in Article 84 paragraph (1), (2), (3) and (4) Government Regulation Number 82 of 2012 on the Implementation of Electronic Transactions and Systems. The violations of data protection, its secrecy or confidentiality, is subjected to administrative sanctions in the form of the following:

1. Written warning,
2. Administrative fines,
3. Temporary suspension, and
4. Removal from the list referred in article 5 paragraph (4), article 37 paragraphs (2), article 62 paragraphs (1), and article 65 paragraphs (4).

Sanctions, according to this provision, are also carried out by the Minister or the head of the supervisory agency and regulator of the relevant sector in accordance with statutory provisions. In the context of violations committed by the banking sector, then it may be imposed by the Financial Services Authority or Bank Indonesia.

The administrative sanctions in Government Regulation Number 82 of 2012 on the Implementation of Electronic Transactions and Systems do not eliminate criminal and civil liability. It means that the violation of data protection, including those qualified by bank secrecy, is not subjected to administrative sanctions. The criminal sanctions refer to Law No. 7 of 1992 Jo Law No. 10 of 1998, while civil refer to the Civil Code. Civil sanctions are in the form of cancellation of the agreement, or compensation.

Furthermore, for legal responsibilities contained in the Minister of Communication and Informatics Regulation Number 20 of 2016 on Protection of Personal Data in the Electronic System only regulates administrative responsibility. This is as stated in the provisions of Article 36 paragraph (1) Number 20 of 2016 in the form of the following sanctions:

1. Verbal warning,
2. Written warning,
3. Temporary activity suspension,
4. Announcement on online sites such as websites.

Administrative sanctions are provided by the head of the supervisory agency and regulator of the relevant sector following statutory provisions. In the context of a violation of data protection related to bank secrecy, the Financial Services Authority, or Bank Indonesia are responsible for imposing sanctions.

Based on understanding the various violations consequences of data protection, the following needs to be considered in terms of legislation as follows. First, for the consequences associated with violations of bank secrecy, such as protected data protection, the results are criminal liability based on the provisions of Law No. 7 and 10

of 1992 and 1998 Jo, respectively. Secondly, the form of administrative liability refers to Law No. 7 and 10 of 1992 and 1998 Jo, Financial Services Authority Regulation No.1/POJK.07/2013 Jo, Bank of Indonesia Regulation No. 16/1/PBI/2014 Jo, Government Regulation Number 82 of 2012 Jo, as well as Minister of Communication and Informatics Regulation No. 20 of 2016. The form and imposition of administrative sanctions vary greatly and do not eliminate criminal and civil liability. Thirdly, the form of civil liability refers to the cancellation of the agreement, compensation, and claim.

4. CONCLUSION

The advancement in information technology has led to a shift from the principle of bank secrecy to confidentiality and security of personal data. Due to this shift, banks are no longer limited to the principle of data secrecy. They are also obligated to protecting customer's personal interests, deposits, control data, reject certain types of processing, and claim forgotten information. Therefore, the consequences of violating the shifting principle of bank secrecy to confidentiality and security of data are in the form of administrative, civil, or criminal sanctions.

REFERENCES

Banisar, David. "The Right to Information and Privacy: Balancing Rights and Managing Conflicts, Washington DC: The International Bank for Reconstruction and Development /TheWorld Bank." *Sabaragamuwa University Journal* 15, no. 1 (2011): 1–7.

Capitani, Werner De. "Banking Secrecy Today." *U. Pa. Journal Int'ernational Bussines Law* 10, no. 1 (1988).

Djumuhana, Muhamad. *Hukum Perbankan Di Indonesia*. Bandung: Citra Adya, 1993.

Jagtiani, Julapa. "Fintech: The Impact on Consumers and Regulatory Responses." *Journal of Economics and Business* 100 (2018).

Pelteret, Marc and Ophof, Jacques. "A Review of Information Privacy and Its Importance to Consumers and Organizations." *The International Journal of an Emerging Transdiscipline* 19 (2016).

Sloot, Bart van der. "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of 'Big Data.'" *Utrecht Journal of International and European Law 25* 31, no. 80 (2015).

Sutedi, Adrian. *Hukum Perbankan Suatu Tinjauan Pencucian Uang, Merger, Likuidasi, Dan Kepailitan*. Jakarta: Sinar Grafika, 2008.

Usman, Rachmadi. *Hukum Perbankan*. Jakarta: Sinar Grafika, 2001.

Vries, Will Thomas De. "Protecting Privacy in The Digital Age." *Berkeley Technology Law Journal* 18 (2003): 283.

This work is licensed under a Creative Commons Attribution 4.0 International License