Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right

Vera W. S. Soemarwi[1*] W. Susanto[1]

[1]*Faculty of Law, Universitas Tarumanagara, Jalan Letjen S. Parman No 1 Jakarta Barat, Jakarta 11440, Indonesia*
[*]*Corresponding author. Email: veras@fh.untar.ac.id*

ABSTRACT
Digital technology has been quickly developing and has been used in the financial sector, such as banking, but the laws in Indonesia have not provided adequate legal protection for data protection for banking consumers. The Indonesian Government has created various cross-sectoral regulations but they have yet to guarantee legal protection for banking consumers. The abundance of regulations provides leeway for violation of consumer rights. In addition, efforts to implement a new system in law-making process, the omnibus law mechanism, have not been able to improve the personal data protection system for the Indonesian people.

Keywords: *Personal data protection, rights to personal data, digital technology information*

1. INTRODUCTION

The digital era of information technologies in Indonesia began with the online book sales site called http//www.sanur.com in 1996 [1], which became the first e-commerce site in Indonesia. At that time, laws did not regulate consumer protection. The Indonesia Government was also not concerned about personal data protection. The lack of such protection has led to cases like PT Telkom, a major player in data center services in Indonesia, which had utilized data obtained from various industrial sectors, such as agriculture, education, health, finance and banking, hotels, transportation, and mining using cloud computing [2].

Personal data use by state-owned enterprises can occur because Indonesia has yet to have laws and regulations that protect consumers or data owners from having their data processed or digitally obtained. The lack of a regulation that regulates information technology use while simultaneously balancing the interests of business actors and consumers create many legal loopholes for consumer protection violations.

Regulations such as Law No. 19/2016 on Electronic Information and Transactions Law, the Government Regulation No.82/2012 on the Implementation of Electronic Systems and Transactions [3], the Government Regulation No. 18/2012 and the Communication and Information Ministry Regulation No. 20/2016 on Personal Data Protection in Electronic Systems [4] provide more details on how trading in electronic systems and protection of personal data are being regulated. These laws have become the legal basis for business actors, internet service providers and information technology users to uphold their rights and obligations. However, these regulations have not been able to provide legal protection for data owners. Lackluster legal basis and supervision for data processing and use by business players in Indonesia has led to personal data misuse, such as those often complained about by consumers [5] regarding the use of improperly stored identity and personal data. In the credit card industry, for example, consumers' personal data can be accessed, disseminated and shared between banks and other financial institutions without the knowledge of the consumer or the subject of the data owner. Although consumers refuse the use and distribution of their personal data to third parties, banks, credit card companies and the Indonesian government has never paid attention to these objections.

The crux of the matter, according to Dewi (2017), begins with the agreement between the bank and the customer. According to Dewi, the agreement needs to be revised because the agreement's clauses leave no room for the consumer to decide on whether or not they would authorize the bank to use their customer's data for their own benefit or purposes [6]. As a result, customers often get online promotions for credit card offers from other banks and get spammed with online loan offers.

This article will discuss the following questions: to what extent companies comply with the consumer data usage agreement? In addition, to what extent does the Indonesian government protect citizens against personal data violation and misuse by businesses?

1.1. Related Work

Quoting data from the Breach Level Index Gemalto (Beritagar.id, 2019), data abuse in the retail sector made up 8.2% of the total cases in 2018, while the figure stood at 26.4% for the health sector, 10.8% for the financial and financial services sector and 8.97% for the public sector [7].

1.1.1. Data Violation

Overall, there were 5,880,600 cases of data leakage in the financial sector in 2018, which includes bank savings customers, credit card users and customers from other financial service business players. Some of them have even been identified as people who hold important positions in Indonesia. The question arises: how can this happen when the law guarantees protection for users of financial services? One reason relates to the bank's secrecy policy that obliges banks not to provide any information to other parties regarding consumer personal information. However, in reality, thousands of people continue to experience online terrors such as online loan spams, insurance offers and credit card offers, whether it is by telephone or short text messages (SMS) that often mention personal information about the customers or users.

So far, a number of banks and their employees have been suspected of leaking their customers' data to other parties, either to other banks or third parties. Meanwhile, credit card and bank savings customer's data have been widely circulating on data buying and selling sites on the internet as well as in several social media sites, such as Twitter and Facebook [8]. Such violations raise the question of how perpetrators obtain thousands of data. The emergence of a phenomenon that is often referred to as telemarketing has made some customers suspect that banks have unwisely used their data. Telemarketers generally offer a variety of bank products and services, insurance, credit, and online loans to customers, both credit and depository products [9]. Customers' data are even sold on websites without any obstruction and at low prices. This was experienced by 2 out of 8,626 thousand credit card owners who were found in the credit card customer data sales site temanmarketing.com, which offers sales of credit card customer data at a price of Rp 350,000 for 1,000 customer data. Both credit card owners admitted that they continued to receive insurance offers via text messages, continuous phone calls and other credit card offers. The leaked data included names, cellphone numbers, addresses, date of births and credit card numbers [10].

Furthermore, at the beginning of 2020, Indonesian senior journalist Ilham Bintang had his money from his bank account stolen after a bank employee sold customer's data several times - not just Ilham Bintang - to criminals. The bank employees apparently have access to the Financial Information Service System at the Financial Services Authority ("OJK"). The perpetrator committed the crime for 1 year by selling the data at a price of Rp 100 thousand per data. As a result, Bintang suffered a loss of around Rp 300 million [11]. Another method used by perpetrators begins with a call from someone claiming to be a "bank employee". The "fake bank employee" would then tell customers that they would receive a gift voucher worth Rp 10 million. After that, the "fake bank employee" asks the customer to mention all their data, including their full name, date of birth and mother's name as a way to verify data [12]. After obtaining the data, the "fake bank employee" takes the funds from the customer's personal account.

The banking law in Indonesia requires banks to maintain the confidentiality of their customers [13]. Customer confidentiality constitutes everything that is related to customers' information, such as their personal data, the type of savings they own and the amount of money they have in their accounts. This rule also applies to those who are credit card customers [14].

Furthermore, the Financial Services Authority Regulation No. 1/POJK.07/2013 ("1/POJK.07/2013") requires banks to maintain the confidentiality of consumer data and information. This OJK regulation prohibits banks from using consumer information, except for interests and purposes that have been approved by consumers. If there is a violation of consumer data, this regulation requires banks to provide complaint services and dispute settlement agreements [15]. However, this regulation does not explain what constitutes consumer data and information that must be kept confidential by the bank and may not be disclosed or given to other parties. It also does not entail the types of complaints the consumers can make if something goes wrong at the bank.

OJK's Circular No. 14/SEOJK.07/2014 ("14/SEOJK.07/2014") on Confidentiality and Security of Data and/or Consumer Personal Information elaborates that consumer personal data and information includes the name, address, place of birth, date of birth, age, telephone number, name of the individual's biological mother, information of directors or commissioners in a company - including their identity documents - and composition of a company's shareholders [16]. This circular also clarifies the previous OJK regulations. It now requires financial sector business players ("PUJK"), including banks, to explain to consumers the objectives and consequences should the consumers agree on giving their written consent to the use of consumer personal data and/or information either to banks, third parties, or affiliated parties [17].

The laws and regulations in the banking and financial services sector have yet to regulate how banks and other financial services must process, store and use customer data. Existing laws and regulations have so far provided an "advantage" for banks to use consumer data and personal information for the internal interests of PUJK. They also give no limits to the extent of these internal interests. With the absence of regulations that entail procedures or details on data processing and storage, it can be said that banks have no transparency that can be supervised by a certain authorized institution, which would have been able to guarantee the protection of the customer's personal data. The Banking Law and Financial Services Authority Regulations are unable to affect the practice of disclosing personal data of bank customers because the existing regulations tend to regulate large-scale violations that can be directly monitored, both internally and by customers who own the accounts. They also have to touch on the disclosure of bank secrets, which have been done without the knowledge of the account owner or OJK's permission. This makes the consumers vulnerable to such crimes amid the gray area since the law has not clearly regulated practices that are carried out outside the scope of supervision of

account holders or institutions that supervise banking activities [18].

In line with the legal facts presented by Dewi (2017), the legal relationship between customers and banks, including debtors and creditors, is based on an agreement. The agreement is a reciprocal agreement between parties that are exercising their rights and obligations. The parties have a balanced and equal legal position. In reality, however, for practical and time-saving reasons, the bank changes the legal position of the parties in the agreement so that the customer is in a weak bargaining position while the bank has strong control over the customer's bargaining position unless the customer accept this weak position or rejects the agreement offered by the bank [19]. Even though parties have made and agreed upon the agreement, customers do not know how their personal data and information will be used by the bank. Many PUJK use the excuse of using customer personal data without the customer's permission "to improve product quality" but there is no explanation of how the “product improvement” in question will be carried out by the bank. Such a situation places the customer as a “personal data” exploitation victim, with the customer often being at a disadvantage.

Alongside the continuous development of the globalization era, banks also follow IT developments by trying to provide the best service to customers, including through e-banking or mobile banking facilities. These facilities require customers to provide their personal data and information. In the case of violations, the bank would distort the series of customer activities on the electronic system. The Banking Law does not regulate customer protection in the electronic or online form so in the case of electronic banking services, customers and PUJK must refer to the Electronic Information and Transaction Law (“ITE Law”). Article 15 of the ITE Law requires banks to operate their electronic systems reliably and safely. Government Regulation No. 71/2019 on Electronic System Operators (“PP 71/2019”) clarifies electronic system user protection by stipulating that in processing personal data, PSE is obliged to implement personal data protection principles. In addition, the regulation also obliges PSE to inform both relevant supervisors and customers of any data leakage.

1.1.2. Privacy as a human rights in the digital world

The Human Rights Declaration recognizes that every individual has the right to have their privacy protected and unrestricted by anyone. The International Covenant on Civil and Political Rights asserts and protects the right to privacy. The European Union views the right to privacy as a fundamental right and thus it is important to further stipulate it in regional and national regulations [20]. In Europe, the protection of the right to privacy is an important issue [21]. The General Data Protection Regulation (“GDPR”) is one of the European Union’s instruments for privacy protection. The GDPR regulates international rules that emphasize the principles of personal data protection, which were later adopted by several countries. The GDPR is the world's most ambitious and comprehensive data protection regulation [22]. This regulation serves as a way to harmonize data privacy laws in Europe and restructure the way companies approach data privacy while empowering and protecting the data privacy of all European Union citizens[23].

The difference in policies between countries in Europe and Asia, such as Indonesia, is that the protection of the right to privacy has not been adequately guaranteed. In today's digital era, the lack of protection towards the use of personal data will weaken the public’s legal position. Information technology system users, particularly in Asian countries like Indonesia, do not know where their personal data is stored and distributed and do not know what their personal data is being used for. Various examples of cases in Indonesia where banks use customer data without the customer's permission illustrate the customer’s weak position. Tan (2019) found that at least 3 to 5 Southeast Asian countries have specific laws and regulations for personal data protection. Indonesia is not one of them, despite having at least 32 laws that regulate personal data. To date, Singapore, Malaysia, and the Philippines are countries that have data protection laws, followed by Thailand that had just passed the personal data protection law in early 2019 [25].

Article 28G of Indonesia’s constitution, namely the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), does not explicitly mention the protection of personal data or privacy [24]. However, the author of this study interprets that the 1945 Constitution guarantees the right to privacy as a human right since it also guarantees the protection of oneself and their family, honor, dignity and property. The author of this study concludes that Article 28 G of the NRI Constitution guarantees the protection of privacy and personal data.

Lending (2018) defines data breach as a compromise of security that leads to damage, loss, alteration, unauthorized disclosure or access to protected data that is sent, stored, or processed accidentally or intentionally in a way that is violating the law [27]. Data breaches include various actions that can lead to data leaks, whether it is done through hacking by individuals or groups of people, due to negligence, viruses, or inadequate information systems. Internal and external information breaches can cause data leaks, whether they are on purpose (for example, data theft by an intruder or sabotage by insiders) or by accident (for example, by employees and partners who unintentionally disclose sensitive information). The motivation for insider attacks may include corporate espionage, complaints against their superiors, or financial rewards. Accidental leaks mainly occur from unintentional activities due to poor business processes, such as failure to implement appropriate preventive technology, security policies or employee surveillance [28]. Under the GDPR, personal data breach means that there is a security breach that causes damage, loss, alteration, unauthorized disclosure of, or access to personal data that are transmitted, stored, or processed [29].

Meanwhile, Article 26 of the ITE Law stipulates that the use of any information through electronic media that concerns a person's personal data must be carried out with the consent of the person concerned. If their rights are violated, they can

file a lawsuit for losses incurred under the ITE Law.

Comparison of consent for personal data use in Europe

In the context of information technology, an agreement between service users and information technology service providers provides a foundation for a legal relationship between the two parties. The data owners' consent is one of the main keys of being able to store, process and use data. GDPR experts recognize that low voluntary approval can justify data processing activities [30]. The GDPR explains that the data subject must give consent in a way that is free, specific, informed and unambiguous in order for the data to be processed. The subject may either give their consent through a written statement, including electronic means, or through an oral statement. Without a concrete and clear agreement, the electronic system may not process the subject's data. Moreover, data subjects should be clearly informed of the specific data processing. Vague and abstract goals, such as promoting customer satisfaction, product development or optimizing services, are prohibited [31].

If the data processing is carried out to improve service satisfaction to consumers, just like how many banks are informing their customers, the GDPR requires banks to tell what kind of improvement they want to implement.

With this approach, data subjects will clearly know the purpose of the data use, whether it is for themselves or for other parties. As such, this will not interfere with the basic rights of the individual because the subjects give consent after they clearly know the purpose.

In Indonesia, law enforcers can impose criminal penalties and fines as stipulated by the Banking Law if an internal bank party commits a personal data breach. However, the law does not provide protection for customers, whether that constitutes notifying customers that there has been a personal data breach or informing them on what the bank should do to fix the situation after the data leak occurred. The customers can file a civil lawsuit in accordance with Law Number 8 of 1999 concerning Consumer Protection (UUPK) as a form of protection. In addition, based on 1/POJK.07/2013, consumers can submit complaints that indicates the disputes between PUJK and consumers to the Financial Services Authority. Consumers can also submit complaints that indicate personal data and information violations to the Financial Services Authority [32].

In addition, law enforcers may use the ITE Law for data breach cases if the electronic system, such as e-banking or computer, carries out the personal data violation, regardless of whether parties inside or outside the banking sector had committed them. If the violation of personal data occurs due to the failure of PSE's operation in the financial sector, then PP 71/2019 obliges PSE to notify the owner of the data in writing that there has been a failure in protecting the confidentiality of personal data [33]. Furthermore, the Indonesian Ministry of Communication and Information Technology ("Kemenkominfo") Regulation No. 20/2016 on Personal Data Protection in Electronic Systems ("Permen Kominfo 20/2016") stipulates that if the violation occurs, the perpetrators must also provide a reason or cause of the data protection failure. They must ensure that the notification has been received by the data owner if the failure contains potential losses to the person concerned. Any written notification sent to the owner of the data should be no later than 14 days after the failure was discovered [34].

2. FINDINGS AND DISCUSSIONS

2.1. Parties that have the authority and responsibility for data breaches

The last part of this analysis discusses the Data Protection Authority (DPA). In Europe, each EU member state should provide one or more independent public authorities that are responsible for monitoring the GDPR implementation in order to protect the basic individual rights and freedom related to how their data is being processed as well as facilitating the free flow of personal data within the European Union [35]. The DPA is responsible for overseeing the implementation of data protection laws through investigations within its authority. DPA also provides expert advice on data protection issues and addresses complaints on violations of the GDPR and relevant national laws [36].

It can be concluded from the Banking Law that perpetrators who commit the personal data violation are the ones that is responsible for their actions. As a body that supervise the matter, OJK can provide external bank protection for consumers. OJK's supervision is only effective if there is a complaint from the victim. OJK's spokesperson said in an interview that "as long as there is no report, there can be no action [37]." Meanwhile, in cases where electronic systems in the banking sector are involved, the law does not explicitly explain who is authorized and responsible if a violation occurs. As a

3. CONCLUSIONS

The absence of a monitoring system for data uses as well as the lack of laws and information transparency regarding personal data processing, use and storage allows personal data breaches to occur in Indonesia. Banisar (2018) divides the right to privacy into four, namely information privacy, body privacy, territorial privacy and communication privacy [38]. Furthermore, Banisar conveyed the need for restrictions on each privacy so that individuals can freely enjoy their rights. To reinforce the idea conveyed by Banisar, Indonesia needs to divide the right to privacy into four parts, with each classification being further defined and clarified in terms of the limitations of each of these classifications. The ITE Law also needs to be revised by.

ACKNOWLEDGMENT

Tarumanagara University has supported the research and publication as well as the Faculty of Law Tarumanagara University.

REFERENCES

[1] Mansur D M A and Gultom E 2005. Cyberlaw Aspek Hukum Teknologi Informasi, PT. Refika Aditama.

[2] Dewi S 2006, 'Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia' (2016) 5 *Yustitia* 22.

[3] Anjani M R and Santoso B, 'Urgensi Rekonstruksi Hukum E-Commerce di Indonesia' (2018) 14, *Jurnal Law Reform* 89.

[4] Yuniarti S, 'Perlindungan Hukum Data Pribadi di Indonesia' (2019) 1 *Jurnal BECOSS (Business Economic, Communication, and Social Sciences)* 147.

[5] Rosadi S D, 'Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework In Indonesia' (2018) 5 Brawijaya Law Journal 143.

[6] Dewi S, 'Prisip-prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya' (2017) 19 *Sosiohumaniora* 206.

[7] Adzkia A, Maraknya kebocoran data akun jual beli, 2019, https://lokadata.id/artikel/maraknya-kebocoran-data-akun-jual-beli.

[8] Laucereno S F, Data Nasabah Bank Juga Dijual Lewat Online Shop, (Detik, 25Agustus 2017) https://finance.detik.com/moneter/d-3615147/data-nasabah-bank-juga-dijual-lewat-online-shop.

[9] Rani M, 'Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank' (2014) 2 Jurnal Selat 168.

[10] Kresna M, 'Bagaimana Data Nasabah Kartu Kredit Diperjualbelikan' (Tirto, 20 Maret 2019) https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv#top.

[11] Wildansyah S, Polisi: Tersangka Pekerja Bank Tak Hanya Jual Data Ilham Bintang (Detik, 5 Febuari 2020) https://news.detik.com/berita/d-4886814/polisi-tersangka-pekerja-bank-tak-hanya-jual-data-ilham-bintang/2.

[12] Yoliawan H, Data Nasabah Bank Rawan Bocor (Kontan, 7 Maret 2018) https://keuangan.kontan.co.id/news/data-nasabah-bank-rawan-bocor.

[13] Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan ("UU Perbankan") (Indonesia) Pasal 40 ayat 1.

[14] Penjelasan Pasal 40 ayat 1 UU Perbankan.

[15] 1/POJK.07/2013 Pasal 32 ayat 1.

[16] Surat Edaran OJK Nomor 14/SEOJK.07/2014 ("14/SEOJK.07/2014") (Indonesia) Pasal 1 ayat 1.

[17] 14/SEOJK.07/2014 Pasal 2 ayat 6 huruf a.

[18] Sutiawan H A, Etty Mulyati & Ijud Tajudin, 'Perlindungan Nasabah Terkait Praktik Pembukaan Rahasia Bank Oleh Pegawai Bank Dalam Proses Penegakan Hukum Tindak Pidana Pencucian Uang Dihubungkan Dengan Asas Kepastian Hukum' (2018) 48(3) *Jurnal Hukum dan Pembangunan* 630.

[19] Bahagia, Sri Walny Rahayu and Mansur T M, 'Perlindungan Data Pribadi Nasabah Dalam Penawaran Transaksi Asuransi oleh PT Bank Negara Indonesia (Persero)' (2019) 3(1) *Syiah Kuala Law Journal* 18.

[20] Brkan M, 'Data Protection and European Private International Law: observing a bull in a China Shop' (2015) 5 *International Data Privacy Law* 257.

[21] Acquisti A, Gritzalis S, Lambrinoudakis C & Capitani S De di Vimercati (ed), Digital Privacy: Theory, Technologies, and Practices, *Auerbach Publications: Taylor & Francis Group*, New York London 2008, page ix.

[22] Bennett C J, 'The European General Data Protection Regulation: An instrument for the globalization of privacy standards?' (2018) 23 *Information Policy* 239.

[23] Wong K Li Xan and Dobson A S, 'We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in Westernised democracies' (2019) 4 *Global Media and China* 220.

[24] Hanara D, 'Mainstreaming Human Rights in the Asian Judiciary' (2018) 4 *Constitutional Review* 78.

[25] Tan S and Azman N S, The EU GDPR's impact on ASEAN data protection law (Financier Worldwid, September 2019) https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law.

[26] Priscyllia F, 'Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum' (2019) 34 *Jatiswara* 239.

[27] Lending C, Minnick K, Schorno P J, 'Corporate Governance, Social Responsibility, and Data Breaches' (2018) 53 *The Financial Review* 413.

[28] Cheng L, Liu F and Yao D (Daphne), 'Enterprise data breach: causes, challenges, prevention, and future directions' (2017) 7 *WIREs Data Mining and Knowledge Discovery* 1.

[29] The General Data Protection [2016] OJ L. 119/1 Pasal 4 ayat 12.

[30] Hoofnagle C J, Sloot B v d, Borgesius F Z, The European Union general data protection regulation: what it is and what it means (2019) 28 *Information & Communication Technology Law* 65-98.

[31] Hoofnagle C J, Sloot B v d, Borgesius F Z, The European Union general data protection regulation: what it is and what it means (2019) 28 *Information & Communication Technology Law* 65-98.

[32] Pasal 40 (1) and (2) 1/POJK.07/2013.

[33] Pasal 14 (5) PP 71/2019 (Indonesia).

[34] Pasal 28c Permen Kominfo 20/2016.

[35] Pasal 51 ayat 1 GDPR.

[36] European Commission, 'What are Data Protection Authorities (DPAs)' https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en#:~:text=DPAs%20are%20independent%20public%20authorities,and%20the%20relevant%20national%20laws.

[37] Oktarina Paramitha Sandy, OJK Akui tak Bisa Tindak Langsung Penjual Data Nasabah, (cyberthreat.id, 13 Mei 2019) https://cyberthreat.id/read/447/OJK-Akui-tak-Bisa-Tindak-Langsung-Penjual-Data-Nasabah.

[38] David Banisar and Simon Davies, 'Global Trends In Privacy Protection: An International Survey Of Privacy, Data Protection, And Surveillance Laws And Developments' (2018) XVIII *John Marshall Journal of Computer and Information Law*.