YURISPRUDEN
Jurnal Fakultas Hukum Universitas Islam Malang
Volume 7, Nomor 2, Juni 2024.

ISSN Online: 2614-3992

Editorial Office : Faculty of Law, Universitas Islam Malang.
Jl. Mayjen Haryono No.193, Dinoyo, Kec. Lowokwaru, Malang, Provinsi Jawa Timur, 65144.
Phone : (0341) 551 932 / 551 822 / (0341) 552 249
E-mail : yurispruden@unisma.ac.id
Website : http://riset.unisma.ac.id/index.php/yur/index

Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins

Diana Setiawati, Tyas Permata Dewi
Law Study Program Faculty of Law Universitas Muhammadiyah Surakarta
Garuda Mas St. No.8, Kartasura, Sukoharjo, Jawa Tengah, 57169, Telp: +62 271-717417
Email: ds170@ums.ac.id

Zulfiani Ayu Astutik
Faculty of Law Ankara University
Emniyet, Dögol Cd., 0600 Yenimahalle/Ankara, Türkiye, Telp: +90 444-5946
Email: astutik@ankara.edu.tr

Article

Article History
Received: Dec 31, 2023;
Reviewed: Feb 15, 2024;
Feb 15, 2024;
Accepted: Feb 29, 2024;
Published: Mar 28, 2024:

DOI:
10.33474/yur.v7i2.20532

Abstract

Di era digital, kejahatan siber, khususnya Sniffing, menjadi ancaman karena pelaku meretas data pribadi nasabah secara tidak sah yang menyebabkan kerugian, sehingga menimbulkan kekhawatiran yang meluas. Tujuan dari penelitian ini untuk memaparkan terkait Pelindungan hukum terhadap korban Sniffing serta menjelaskan bentuk tanggung jawab pihak bank terhadap nasabah yang menjadi korban kejahatan siber Sniffing. Penelitian ini menggunakan pendekatan hukum normatif dengan bahan hukum primer, sekunder dan tersier. Metode analisis menggunakan metode kualitatif untuk menghasilkan informasi yang bersifat deskriptif analisis. Hasil penelitian menunjukkan bahwa berdasarkan UU No. 27 Tahun 2022 dan Peraturan Bank Indonesia No. 3 Tahun 2023 telah mengindikasikan adanya perlindungan hukum terhadap data pribadi nasabah meskipun belum terbentuknya Lembaga khusus yang telah diamanatkan serta belum adanya kejelasan terkait pertanggungjawaban dalam penyelesaian sengketa yang mana dinilai dapat merugikan nasabah. Oleh karena itu nasabah harus lebih berhati-hati untuk menjaga data pribadinya.

Kata Kunci: *Sniffing; Kejahatan Siber; Pelindungan Data Pribadi; Ekonomi Digital; Perbankan.*

Abstract

Cybercrime, particularly Sniffing, poses a hazard in the digital age since attackers illegally breach customers' data, resulting in losses and widespread concern. This study aimed to clarify the legal protections available to victims of sniffing cybercrimes and the banks' obligations to their clientele. This study includes primary, secondary, and tertiary legal materials with a normative legal

approach. The analytical method produced information through descriptive analysis using qualitative methodologies. The research findings demonstrated that, despite the lack of a required special institution and ambiguity surrounding accountability in resolving disputes deemed harmful to customers, Law No. 27 of 2022 and Bank Indonesia Regulation No. 3 of 2023 indicated that there was legal protection for customers' data. As a result, customers must take greater precautions to protect their data.

Keywords: Sniffing; Cyber Crime; Personal Data Protection; Digital Economy; Banking

INTRODUCTION

The progress of the times and technology is accelerating as must be balanced with efforts to protect the data. According to Pancasila, efforts to secure personal data are a form of recognition and safeguarding of human rights.[1] Personal data in the financial sector becomes very important, especially when Indonesia transitions from the traditional to the digital economic era.[2] Sniffing is one type of crime that poses a threat to the financial industry, particularly bank customers, given current technology advancements.[3] Network Sniffing is a network security issue in which a hacker illegally hacks credentials that are not securely encrypted and captures data during transit as a third party.[4] As a bank customer, sniffing has the potential to result in the theft of personal data, which can lead to the compromise of bank account balances. [5]

Based on earlier scientific research into the safety of personal data for clients who experienced account breaches through internet banking. [6] Previous studies solely looked at favourable laws in Indonesia. Our research has been updated with an analysis of Law No. 27 of 2022 concerning Personal Data Protection, which concerns Personal Data Protection. By linking Law No. 8 of 2016

---

1 Lilik Prihatin, Muhammad Achwan, dan Citra Candra Dewi, "Kajian Yuridis Regulasi Perlindungan Hukum Terhadap Penyalahgunaan Data Privasi Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *UNES Law Review* 5, no. 4 (20 Juli 2023): 4128, https://doi.org/10.31933/unesrev.v5i4.731.

2 Sinta Dewi Rosadi dan Garry Gumelar Pratama, "Urgensi Perlindungan Data Privasi Dalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (28 Juni 2018): 91, https://doi.org/10.25123/vej.v4i1.2916.

3 Yesi Febriani dan Vivi Sahfitri, "Monitoring Encegahan Aktivitas Ilegal Dalam Jaringan Pada Kantor Dinas ESDM Provinsi Sumatera Selatan," *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* 4, no. 1 (29 Agustus 2022): 92.

4 Sara Qaisar dan Kausar Fiaz Khawaja, "Cloud computing: Network/Security Threats and Counter Measures," *Interdisciplinary Journal of Contemporary Research in Business* 3, no. 9 (1 Januari 2012): 1325.

5 Ahmad M Ramli, "Sniffing, Peretasan Data Pribadi, dan Pembobolan Rekening Bank Halaman all - Kompas.com," Kompas.com, 5 Februari 2023, https://www.kompas.com/tren/read/2023/02/05/091134365/sniffing-peretasan-data-pribadi-dan-pembobolan-rekening-bank?page=all.

6 Delfa Violina dan Hanna Tasya Zahrani, "Perlindungan Data Pribadi Bagi Nasabah Korban Pembobolan Rekening Melalui Internet Banking Ditinjau Dari Hukum Positif Indonesia," *Jurnal Kepastian Hukum Dan Keadilan* 2, no. 1 (13 Januari 2021): 69, https://doi.org/10.32502/khdk.v2i1.3048.

concerning Information Technology and Electronics with previous research, we modified it to reflect the most recent analytical basis and new legislative regulations. In addition, clients will get a form of bank accountability in compliance with the rules of Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection.

With a vast No. of internet network users in Indonesia, around 54.68% of the entire population, or 143.26 million in 2017, the country is vulnerable to hacking and the theft of Indonesian citizens' personal information.[7] According to Antaranews.com (2023), as of June 12, 2023, Financial Services Authority had received reports of cybercrimes committed outside of financial services institutions, such as bank account break-ins, fraud, social engineering, skimming, spam, and sniffing in 1,931 cases in Central Java.[8] This is because sniffing crime has increased due to the economic development of the digital era, as well as boosting public awareness of their data so that individuals do not misuse it and become victims of sniffing crimes. The public hopes that Law No. 27 of 2022 concerning Personal Data Protection will provide legal protection. As a result, this study was conducted to determine the best way to enforce the safety of people's data, specifically bank clients, so that bank customers can feel secure and protected from the threat of sniffing cybercrime.

The following might be used to formulate the key areas of discussion in this research: First, what are the ways that Law No. 27 of 2022 concerning Personal Data Protection is being enforced to protect the personal data of bank customers and second, what obligation does the bank have to sniff victims.

Normative legal research was employed to address the central topic of this study.[9] Primary legal material—Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection and Law No. 27 of 2022 concerning Protection of Personal Data—as well as secondary legal material—books, journals, doctrine, and case laws that can aid in our research—were the sources of the data we used. Legal encyclopedia were the examples of tertiary legal materials that we also used. Through the quotation and analysis of the legal documents we get, we conducted literature research as our method of data collecting. After that, a qualitative

---

7 Diana Setiawati, Hary Abdul Hakim, dan Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (23 Oktober 2020): 99, https://doi.org/10.18196/iclr.2219.

8 Antaranews.com, "OJK: Waspadai penipuan dengan modus 'sniffing,'" Antara News, 27 Juni 2023, https://www.antaranews.com/berita/3608289/ojk-waspadai-penipuan-dengan-modus-sniffing.

9 Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Prenada Media, 2005), 85.

analysis was done on the data we had collected. By creating descriptive presentations based on textual data that has been gathered rather than on numerical data, we employed qualitative analysis.

This research's objective was to clarify the legal protections available to victims of bank account thefts through the implementation of Law No. 27 of 2022 concerning Personal Data Protection. Additionally, this study aimed to clarify the banks' obligations to their customers who fall victim to cybercrimes involving Sniffing.

RESULT AND DISCUSSION

The Protection of Personal Data of Bank Customers Based on Law No. 27 of 2022 concerning Personal Data Protection

Personal data is the right to privacy of an individual, where an individual has the right to protect personal data and determine whether or not his data is given to other parties.[10] Personal data protection includes protection at several stages, such as in the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of personal data.[11] Personal data protection is directly mandated by the Constitution of the Republic of Indonesia as a form of respect for the value of human rights and equal rights.[12] Human Rights contains material with a foundation related to the protection of the most basic rights, which are also the rights of citizens.[13]

This is consistent with Philipus M. Hadjon's theory of legal protection, which holds that legal protection entails both granting recognition of the human rights held by legal subjects and safeguarding their dignity and respect.[14] Based on Law No. 27 of 2022 concerning Personal Data Protection offers dispute resolution mechanisms and means of punishment for violators, in addition to protecting citizens' personal data.

In this case, personal data is the object of protection regulated in Law No. 27 of 2022 concerning Personal Data Protection. Any information that identifies or can be used to identify a person, whether collected directly or indirectly by electronic or non-electronic methods, is considered personal data both

---

[10] Sekaring Ayumeida Kusnadi, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (21 April 2021): 10, https://doi.org/10.47776/alwasath.v2i1.127.

[11] Wardah Yuspin dkk., "Personal Data Protection Law in Digital Banking Governance in Indonesia," *Studia Iuridica Lublinensia* 32, no. 1 (28 Maret 2023): 110, https://doi.org/10.17951/sil.2023.32.1.99-130.

[12] Rina Arum Prastyanti dkk., "Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia," *Jurnal Jurisprudence* 11, no. 1 (14 Januari 2022): 85, https://doi.org/10.23917/jurisprudence.v11i1.14756.

[13] Nurika Falah Ilmania, Benny Krestian Heriawanto, dan Pinastika Prajna Paramita, "Tanggung Jawab Negara Yang Lahir Dari Kewajiban Atas Kesehatan Masyarakat Di Masa Covid-19 (Perspektif Hak Asasi Manusia)," *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang* 5, no. 1 (20 Januari 2022): 90, https://doi.org/10.33474/yur.v5i1.14078.

[14] Philipus M Hadjon, *Perlindungan Hukum Bagi Rakyat Di Indonesia; Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara* (Surabaya: Bina Ilmu, 1987), 54.

individually and personally in conjunction with other information.[15] As referred to in Article 4 Paragraph (1) of Law No. 27 of 2022 concerning Personal Data Protection, personal data consists of two types, namely specific and general. Article 4 Paragraph (2) defines specific personal data as follows: health information and data, genetic data, biometric data, data regarding children, criminal records, personal financial information, and other data as required by law.

On the contrary, as referred to in Article 4 Paragraph (3) of Law No. 27 of 2022 concerning Personal Data Protection, personal data generally consists of full name, nationality, gender, marital status, religion, and other personal information that can be used to identify a person. Regulations related to the scope of personal data described in Article 4 of Law No. 27 of 2022 concerning Personal Data Protection have also been regulated in other regulations.

With the revocation of Bank Indonesia Regulation No. 7/6/PBI/2005 concerning Transparency of Bank Product Information and Use of Customer Personal Data, Financial Services Authority Regulation No. 6 of 2022 discusses consumer and community protection in the financial services sector. Individual personal data and information as referred to in Article 11 Paragraph (2) includes: Name, Address, Population Identification No. Telephone, No. Mother's Name, Date of Birth and/or Age, and other data owned by consumers. Submitted to financial service business actors or given access. Commercial Banks Registered as Financial Services Business Actors following Article 3 No. (1) Financial Services Authority Regulation No. 6 of 2022 concerning Consumer and Community Protection in the Financial Services Sector. Based on the explanation above, the scope related to Personal Data Information aligns with the scope contained in Law No. 27 of 2022 concerning Personal Data Protection.

The processing of personal data is regulated in Article 16 of Law No. 27 of 2022 concerning Personal Data Protection. In addition, commercial banks must maintain the confidentiality of their customers' personal information in their administration. Protecting customers' data is a form of commitment banks give to their customers to maintain the integrity of the data that customers have provided in financial data.[16] Based on Law No. 27 of 2022 concerning Personal Data

---

[15] Willa Wahyuni, "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi," hukumonline.com, diakses 4 Maret 2024, https://www.hukumonline.com/berita/a/bank-perlu-edukasi-nasabah-terkait-pelindungan-data-pribadi-lt636d737770269/.

[16] Rizky Fahrurrozi, Tarsisius Murwadji, dan Mien Rukmini, "Problematika Pengungkapan Rahasia Bank Antara Kepentingan Negara dan Perlindungan Kepada Nasabah," *Jurnal Esensi Hukum* 2, no. 1 (10 Agustus 2020): 78, https://doi.org/10.35586/esensihukum.v2i1.22.

Protection, financial data is specific personal data.

Public entities, including banks, have an obligation to function both as controllers and processors of personal data.[17] When fulfilling the responsibilities as a Personal Data Controller, the basics of handling personal data include obtaining the valid consent of the personal data subject, complying with contractual and legal obligations, performing duties in the public interest, safeguarding the vital interests of the personal data subject, and exercising the powers of the controller. The rationale for handling personal data is set out Based on Article 20 of Law No. 27 of 2022 concerning Personal Data Protection, to treat personal data by the law and support legitimate interests, this law must be complied with, considering the purposes and requirements and balancing the interests of data controllers and data subjects.

As a customer of a financial institution, you are entitled to information regarding the retention period of documents containing the legality, type, purpose, personal data, and relevance of the personal data processed, details regarding the information collected, the duration of the personal data processing, and the rights of the personal data subject.[18] The bank also has to be able to provide education to its customers, and if there are changes, as expressly stipulated in Article 21 Paragraph (1) and (2) of Law No. 27 of 2022 concerning Personal Data Protection, the bank in its capacity as a personal data manager is obliged to notify in advance the party whose information is found of any changes that may affect the data.

Article 36 of Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection explains that the organizer is obliged to provide access to consumers; in this case, it can be said that customers are related to copies of personal data by Law No. 27 of 2022 concerning Personal Data Protection which authorizes individuals to delete, stop, and eliminate personal information if there are organizers who don't fulfil these obligations, they can be subject to administrative sanctions.

The clauses of the agreement are deemed void and unenforceable under Law No. 27 of 2022 concerning Personal Data Protection. In addition, the processing of personal data that does not include the express and valid consent of the individual whose personal data is being processed is deemed void. If the subject of the personal data is a child, the personal data controller is specifically required to obtain the consent of

---

[17] Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (25 Maret 2021): 41, https://doi.org/10.47268/sasi.v27i1.394.

[18] Taufik Hidayat Telaumbanua, "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif," *LEX PRIVATUM* 13, no. 1 (4 Januari 2024): 12, https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/53779.

the child's parent or guardian to provide evidence of the consent given; this also applies to persons with disabilities; however, it is subject to legal requirements. We only do this with the consent of the person with a disability or their legal guardian through approved communication methods. Thus, the processing of personal data cannot be carried out arbitrarily without the personal data subject's consent.

To maintain security, data controllers must prevent unauthorised individuals from changing personal information. If there is someone who makes changes if it will endanger the safety of the data subject or another person, endanger the disclosure of the data of another person, or interfere with the country's defence and security operations, as Article 33 of Law No. 27 of 2022 concerning Personal Data Protection, accordingly.

In addition, in situations where the processing of personal data poses a significant risk to specific individuals or entities, the organization responsible for the personal information shall conduct an impact analysis on data protection at least once.

Article 47 Law No. 27 of 2022 concerning Personal Data Protection states that the data controller is responsible for processing personal data and shall demonstrate responsibility by performing its duties in line with the management principles of personal data protection.

Indeed, in the process of protecting personal data, there are two methods commonly used, namely, implementing regulations that can guarantee privacy in its use and securing the physical aspects of personal data itself.[19] To streamline personal data protection, Law No. 22 of 2007 concerning Personal Data Protection doesn't only stand alone in providing legal protection; there are other supporting regulations and bank policies that actively participate in efforts to protect their customers' data by the policies and objectives of the Law.

In ensuring the protection of personal data and information of bank customers, there is a coordinator responsible for protecting the data and information of its customers. For example, in the policy of one of the banks, PT Bank Central Asia, Tbk, which is contained in the document "Policy on the Protection of Consumer Data and Information" PT Bank Central Asia, Tbk has a coordinator who is responsible for protecting the personal data of its customers called the Bureau of Service Operation Support A (SOS A) - Operation Strategy and Development Group (OSDG). This component is essential to collect all contributions from collaborating work units, guide them in conducting evaluations and

[19] Sagdiyah Fitri Andani Tambunan Agung dan Muhammad Irwan Padli Nasution, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Di E-Commerce," *Jurnal Ekonomi Manajemen Dan Bisnis (JEMB)* 2, no. 1 (1 Juli 2023): 6, https://doi.org/10.47233/jemb.v2i1.915.

reviews, and ultimately continue business processes that require data and information security.[20]

Based on Law No. 22 of 2007 concerning Personal Data Protection, an agency will be expressly established by the president and is responsible to the president. It can impose administrative sanctions on public bodies, corporations, individuals, and international organizations. In addition, it has the jurisdiction to assist law enforcement officials in handling situations involving individuals and companies suspected of committing personal data breaches.[21]

As a form of preventing cybercrime from accessing confidential consumer data, although there is no specialized institution at the time of writing this article, the roles, responsibilities and authorities of this institution have been outlined in articles 58 to 60 of Law No. 22 of 2007 concerning Personal Data Protection. It is stated that the jurisdiction of legal protection has been expanded to include legal consequences to protect the data of Indonesian citizens abroad by applying extradition and Mutual Legal Assistance efforts and synchronizing mechanisms with international cooperation.[22]

Responsibility of Banks to Victims of Money Laundering

Sniffing is considered a type of cybercrime because it uses malicious programs, often malware, to perform hijacking and unlawfully obtain the victim's personal information to benefit the perpetrator. This, of course, has a negative impact on the victim. Unlawfully obtaining confidential information and data through the internet network. [23] The insecurity of technology networks, lack of understanding of digital security, use of unsecured Wi-Fi networks, and sharing of personal information open up opportunities to become a victim of Sniffing cybercrime. [24] Important personal information, including credit card details, emails, i-banking and m-banking credentials, are usually among the compromised data and information. Usually, the act is done by installing an Android application, which once

---

[2020] Herdi Setiawan, Mohammad Ghufron, dan Dewi Astutty Mochtar, "Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Transaksi e-Commerce," *MLJ Merdeka Law Journal* 1, no. 2 (9 November 2020): 105, https://doi.org/10.26905/mlj.v2i1.5496.

[21] Siti Yuniarti, "Petugas/Pejabat Pelindungan Data Pribadi Dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura," *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 4, no. 2 (4 Juni 2022): 114, https://doi.org/10.21512/becossjournal.v4i2.8377.

[22] Raden Romdhon Natakusuma, *Optimalisasi Penegakan Hukum Terhadap Kejahatan Siber Guna Mewujudkan Keamanan Data Pribadi Dalam Rangka Ketahanan Nasional* (Jakarta: Lembaga Ketahanan Nasional Republik Indonesia, 2023), 35.

[23] Mulki Indana Zulfa, Silvester Tena, dan Sampurna Dadi Rizkiono, "Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android," *RENATA: Jurnal Pengabdian Masyarakat Kita Semua* 1, no. 1 (10 April 2023): 8, https://doi.org/10.61124/1.renata.4.

[24] Jumarto Yulianus, "Jangan Biarkan Korban Kejahatan Digital Berjatuhan," kompas.id, 17 September 2023, https://www.kompas.id/baca/nusantara/2023/09/16/jangan-biarkan-korban-kejahatan-digital-berjatuhan.

installed damages or steals important personal data on the phone..

In Article 67 Paragraph (1) of Law No. 22 of 2007 concerning Personal Data Protection, stealing another person's data is the act of a party who intentionally accesses or collects personal data that does not belong to him/her, to utilise it for personal interests or cause harm to the data subject, may be subject to criminal sanctions of imprisonment for a maximum of five years or a maximum fine of five billion rupiah. Additional protection is regulated in Article 32 *jo.* 48 of Law No. 11 of 2006 concerning Information Technology and Electronics, the penalty is a maximum fine of five billion rupiah plus ten years imprisonment.

In studying the concept of Responsibility in language, I found that Responsibility has various meanings. There are two terms, namely Responsibility, which has a social orientation and liability, which is a form of juridical Responsibility. [25] This obligation is created once personal data is processed and managed by Law No. 22 concerning 2007 on Personal Data Protection. Law No. 11 of 2008 concerning Information Technology and Electronic Liability has also existed since the beginning of the implementation because the organizer is responsible for safely, responsibly and reliably operating the electronic system.

The concept of sniffing cybercrime is tapping with the aim of stealing personal data illegally in the form of important information that even involves the victim's banking information. [26] Two distinct conceptions emerge when determining who is liable for failing to protect consumer data. According to Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection, the form of responsibility must be demonstrated by determining whose negligence failed to secure personal data.

In the event that the cyberattack is focused on breaching the bank's system in order to obtain the personal information of its clients, the bank, acting as the controller of the personal data, will be held legally liable for any losses incurred by the clients in line with Financial Services Authority Regulation No. 6 of 2022 and article 42 of the Bank Regulations Indonesia No. 3 of 2023. However, the Bank has a social duty to provide customers with steps to take when they become victims of personal data theft if the failure to protect personal data results from the customer's negligence in securing their personal data. Customers may be spied on by the bank, but the bank is not liable for paying out damages; in contrast, the bank guarantees

---

[25] Zulian Claudia dan Ariawan Gunadi, "Vicarious Liability in Personal Data Protection:," *Rechtsidee* 12, no. 2 (22 Desember 2023): 6, https://doi.org/10.21070/jihr.v12i2.995.

[26] Eril Obeit Choiri, "Sniffing Adalah Tindakan Pencurian, Ini Cara Menghindarinya!," 5 Mei 2023, https://gudangssl.id/blog/apa-itu-sniffing/.

that personal information lost due to carelessness in the banking system will not be compromised. In this case, it concerns the customer's rights if in using the services of the bank and there are problems related to the bank, then the bank must be responsible for the consumer protection of its customers.[27] The bank's obligation as the controller of personal data to be responsible for the losses suffered by its customers is clearly stated in Article 47 of Law No. 22 of 2007 concerning Personal Data Protection.

Banks, in providing services, realize relationships with customers must be from start to finish, such as in the process of opening an account to closing a bank account.[28] In every transaction in the banking system, it will always begin with a contract/agreement. The agreement between the bank and the customer stipulates that the bank has the authority to accept and carry out all customer financial management activities following the agreed guidelines. In the case of i-banking, this authority is derived from the instructions given by the original customer through user ID and password unless denied through judgment or evidence.[29]

As a personal administrator, the bank is responsible for preventing unauthorized access to personal information not accessed by the authorized subject of the information. This prevention can be achieved by utilizing electronic security systems in a reliable, secure, and accountable manner. Personal data controllers must fulfill these duties following Article 39 of Law No. 22 of 2007 concerning Personal Data Protection.

Following the obligations of the personal data controller contained in Article 39 of Law No. 22 of 2007 concerning Personal Data Protection, if the electronic security system owned by the bank fails to protect the personal data of its customers, it is the responsibility of the bank to be responsible for the losses suffered by customers.

In organizing electronic systems, Article 16 letter b of Law No. 11 of 2008 concerning Information Technology and Electronics states that business actors must maintain electronic systems' confidentiality and integrity in their implementation.[30]

Suppose the bank fails to protect the personal data of its customers within three days after realizing a data breach. In that case, financial institutions are required by law to notify the affected individuals and other relevant entities in writing. Paragraphs (1), (2), and (3) of Article 46 of Law No. 22 of

---

[27] Wahyuni, "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi."

[28] Danang Kurniawan, "Initiating the Establishment of Digital Banks in Indonesia: A Juridical Study," *Journal of Transcendental Law* 4, no. 1 (18 Desember 2022): 7, https://doi.org/10.23917/jtl.v4i1.17311.

[29] Tan Henny Tanuwidjaja, "Tanggung Gugat Dalam Transaksi Melalui Internet Banking," *Universitas Narotama Surabaya* 3 (2019): 30.

[30] Kadek Doni Wiguna dan Nyoman Satyayudha Dananjaya, "Pertanggungjawaban Bank Atas Kerugian Nasabah yang Menggunakan Electronic Banking," *Jurnal Kertha Desa* 9, no. 12 (2021): 30.

2007 concerning Personal Data Protection includes clauses addressing notification of personal data breaches. The Bank may face administrative consequences under Article 57 of Law No. 22 of 2007 concerning Personal Data Protection if it fails to fulfil its duties as the controller of personal data under Article 46 of Law No. 22 of 2007 concerning Personal Data Protection, which requires notification to the relevant subject.

Based on Article 42 of Paragraphs (1) and (2) of Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection, the organizer is responsible for any losses customers suffer due to errors, omissions, or actions violating regulatory provisions. Implementing laws and regulations is the responsibility of various entities, including the directors, board of commissioners, management, employees, and third parties representing or working for the organization's benefit.[31] The organization is not liable for any loss that can be proven to be caused by the customer's carelessness or fault.

In general, unless the bank acknowledges that it was negligent in safeguarding the customer's personal information, clients will have a hard time establishing the existence of a bank negligence element when bringing an action for culpability for losses resulting from personal data leaks. [32] Customers may be deemed careless in protecting their personal information if they downloaded a file device that turned out to be infected with malware, which allowed personal financial information to be stolen, or if they knowingly gave personal financial details to unofficial websites or websites belonging to the relevant bank. In compensating for the losses customers suffer, there is a first proof related to the cause of customer losses. The bank carries out the proof by bringing transaction data to the customer.[33]

Article 12 of Law No. 22 of 2007 concerning Personal Data Protection describes the rights of personal data subjects, including the ability to initiate legal proceedings and request compensation. However, the specific procedure for filing a compensation claim remains unclear.

There are multiple steps in the dispute resolution process for customers' data that have been compromised by the bank's carelessness in protecting it. These steps include filing complaints, receiving

---

[31] Irwan Saleh Indrapradja, "Kajian Yuridis Terhadap Tanggung Jawab Direksi Dan Dewan Komisaris Pada Struktur Organisasi Perseroan Terbatas Yang Bersifat Kolegialitas Menurut Undang-Undang Nomor 40 Tahun 2007 Tentang Perseroan Terbatas," *Jurnal Ilmiah Magister Ilmu Administrasi* 13, no. 1 (2019): 126, https://jurnal.unnur.ac.id/index.php/jimia/article/view/272.

[32] Joice Irma Runtu Thomas, "Pertanggungjawaban Bank Terhadap Hak Nasabah Yang Dirugikan Dalam Pembobolan Rekening Nasabah," *Lex et Societatis* 1, no. 1 (2013): 118.

[33] Wiguna dan Dananjaya, "Pertanggungjawaban Bank Atas Kerugian Nasabah Yang Menggunakan Electronic Banking," 30.

complaints, mediating disputes, and reaching a settlement.[34] Customers can file a complaint by following Bank Indonesia Regulation No. 3 of 2023 as the initial course of action. However, in the positive legal system in Indonesia, a consumer, in this case, a bank customer, can sue someone for allegedly damaging their goods or services; often, breach of contract or illegal behaviour is the basis for such cases.[35]

If in a case, the customer has suffered losses from sniffing. The bank must provide accountability efforts to its customers in handling and resolving the losses sustained by customers. The bank must swiftly respond and convey several stages as a form of accountability to customers; some accountability efforts are complaint handling, Peaceful Efforts, Banking Mediation, and Court Lines.[36]

Although all forms of personal data protection and their responsibilities have been legally regulated in Law No. 22 of 2007 concerning Personal Data Protection and supported by Bank Indonesia Regulation No. 3 of 2023 concerning Consumer Protection, Bank Indonesia has not been able to provide a clear conceptualization regarding how the form of responsibility to victims and the procedures for filing a lawsuit for losses suffered by victims. The unclear concept of liability creates confusion about protecting victims.

Therefore, as the general public and as users of electronic banking services, we must understand the modes of sniffing cybercrime that can target us directly without us realizing it. Some tips for us as users of electronic banking services to avoid Sniffing mode are: Do not be easily fooled by messages containing links without directly confirming the authenticity of the sender of the message, Do not download unapproved applications, be careful when conducting financial transactions on public Wi-Fi networks, and ensure account transaction notifications are consistently enabled.[37] In addition, unsolicited calls containing questionable files should be avoided.[38]

CONCLUSION

Law No. 27 of 2022 concerning Personal Data Protection is sufficient as a

---

[34] Aminah Bambang Eko Turisno, "Perlindungan Hukum Bagi Konsumen Perbankan dalam Penggunaan Data Pribadi Nasabah (Studi pada PT Bri Kantor Wilayah Semarang)," *Diponegoro Law Review* 5, no. 3 (2016): 10, https://www.neliti.com/id/publications/19263/.

[35] Thomas, "Pertanggungjawaban Bank Terhadap Hak Nasabah Yang Dirugikan Dalam Pembobolan Rekening Nasabah," 120.

[36] Tanuwidjaja, "Tanggung Gugat Dalam Transaksi Melalui Internet Banking," 30.

[37] Erlina Permata Sari, Deyana Annisa Febrianti, dan Riska Hikmah Fauziah, "Fenomena Penipuan Transaksi Jual Beli Online Melalui Media Baru Berdasarkan Kajian Space Transition Theory," *Deviance Jurnal Kriminologi* 6, no. 2 (31 Desember 2022): 159, https://doi.org/10.36080/djk.1882.

[38] Alicia Diahwahyuningtyas dan Rizal Setyo Nugroho, "Ramai soal Sniffing, Modus Penipuan Resi hingga Undangan yang Bisa Curi Saldo Rekening Halaman all. - Kompas.com," 29 Januari 2023, https://www.kompas.com/tren/read/2023/01/29/183000165/ramai-soal-sniffing-modus-penipuan-resi-hingga-undangan-yang-bisa-curi?page=all.

form of government sensitivity to the urgency of protecting personal data from cybercrime sniffing. The protection of personal data has also been structurally regulated, including in processing personal data. Although there is a unique institution that has been mandated in Articles 58 to 60 of Law No. 27 of 2022 concerning Personal Data Protection until this research was done, there has not been the formation of a particular institution responsible for protecting personal data, efforts to protect personal data must continue to be improved, because it is a form of enforcement of human rights in Indonesia, which as a society has the right to get protection for its data.

As a form of responsibility for losses suffered by customers, Law No. 27 of 2007 concerning Personal Data Protection has yet to regulate precisely who can be responsible for cybercrime sniffing. Although in Article 47, the personal data controller is said to be accountable, in Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection, who can be considered responsible is not based on the personal data controller, which in this study is the Bank, but who is proven negligent in maintaining personal data. Although banks must educate their customers about efforts to prevent losses from leaking customer personal data, these efforts are insufficient to protect the public from the theft of personal data, which in this study is in the form of financial data. There is a lack of clarity on conceptual liability and dispute resolution, which cannot provide legal certainty for victims of cybercrime sniffing.

REFERENCES

Agung, Sagdiyah Fitri Andani Tambunan, dan Muhammad Irwan Padli Nasution. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Di E-Commerce." *Jurnal Ekonomi Manajemen Dan Bisnis (JEMB)* 2, no. 1 (1 Juli 2023): 5–7. https://doi.org/10.47233/jemb.v2i1.915.

antaranews.com. "OJK: Waspadai penipuan dengan modus 'sniffing.'" Antara News, 27 Juni 2023. https://www.antaranews.com/berita/3608289/ojk-waspadai-penipuan-dengan-modus-sniffing.

Bambang Eko Turisno, Aminah. "Perlindungan Hukum Bagi Konsumen Perbankan dalam Penggunaan Data Pribadi Nasabah (Studi pada PT Bri Kantor Wilayah Semarang)." *Diponegoro Law Review* 5, no. 3 (2016): 1–14. https://www.neliti.com/id/publications/19263/.

Choiri, Eril Obeit. "Sniffing Adalah Tindakan Pencurian, Ini Cara Menghindarinya!," 5 Mei 2023. https://gudangssl.id/blog/apa-itu-sniffing/.

Claudia, Zulian, dan Ariawan Gunadi. "Vicarious Liability in Personal Data Protection:" *Rechtsidee* 12, no. 2 (22 Desember 2023): 2–7. https://doi.org/10.21070/jihr.v12i2.995.

Diahwahyuningtyas, Alicia, dan Rizal Setyo Nugroho. "Ramai soal Sniffing, Modus Penipuan Resi hingga Undangan yang Bisa Curi Saldo Rekening Halaman all. - Kompas.com," 29 Januari 2023. https://www.kompas.com/tren/read/2023/01/29/183000165/ramai-soal-

sniffing-modus-penipuan-resi-hingga-undangan-yang-bisa-curi?page=all.

Fahrurrozi, Rizky, Tarsisius Murwadji, dan Mien Rukmini. "Problematika Pengungkapan Rahasia Bank Antara Kepentingan Negara Dan Perlindungan Kepada Nasabah." *Jurnal Esensi Hukum* 2, no. 1 (10 Agustus 2020): 77–96. https://doi.org/10.35586/esensihukum.v2i1.22.

Febriani, Yesi, dan Vivi Sahfitri. "Monitoring Encegahan Aktivitas Ilegal Dalam Jaringan Pada Kantor Dinas ESDM Provinsi Sumatera Selatan." *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)* 4, no. 1 (29 Agustus 2022): 92–99.

Hadjon, Philipus M. *Perlindungan Hukum Bagi Rakyat Di Indonesia; Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum dan Pembentukan Peradilan Administrasi Negara*. Surabaya: Bina Ilmu, 1987.

Ilmania, Nurika Falah, Benny Krestian Heriawanto, dan Pinastika Prajna Paramita. "Tanggung Jawab Negara Yang Lahir Dari Kewajiban Atas Kesehatan Masyarakat Di Masa Covid-19 (Perspektif Hak Asasi Manusia)." *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang* 5, no. 1 (20 Januari 2022): 89–106. https://doi.org/10.33474/yur.v5i1.14078.

Indrapradja, Irwan Saleh. "Kajian Yuridis Terhadap Tanggung Jawab Direksi Dan Dewan Komisaris Pada Struktur Organisasi Perseroan Terbatas Yang Bersifat Kolegialitas Menurut Undang-Undang Nomor 40 Tahun 2007 Tentang Perseroan Terbatas." *Jurnal Ilmiah Magister Ilmu Administrasi* 13, no. 1 (2019): 123–49. https://jurnal.unnur.ac.id/index.php/jimia/article/view/272.

Kurniawan, Danang. "Initiating the Establishment of Digital Banks in Indonesia: A Juridical Study." *Journal of Transcendental Law* 4, no. 1 (18 Desember 2022): 1–15. https://doi.org/10.23917/jtl.v4i1.17311.

Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (21 April 2021): 9–16. https://doi.org/10.47776/alwasath.v2i1.127.

Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Prenada Media, 2005.

Natakusuma, Raden Romdhon. *Optimalisasi Penegakan Hukum Terhadap Kejahatan Siber Guna Mewujudkan Keamanan Data Pribadi Dalam Rangka Ketahanan Nasional*. Jakarta: Lembaga Ketahanan Nasional Republik Indonesia, 2023.

Prastyanti, Rina Arum, Istiyawati Rahayu, Eiad Yafi, Kelik Wardiono, dan Arief Budiono. "Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia." *Jurnal Jurisprudence* 11, no. 1 (14 Januari 2022): 82–99. https://doi.org/10.23917/jurisprudence.v11i1.14756.

Prihatin, Lilik, Muhammad Achwan, dan Citra Candra Dewi. "Kajian Yuridis Regulasi Perlindungan Hukum Terhadap Penyalahgunaan Data Privasi Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *UNES Law Review* 5, no. 4 (20 Juli 2023): 4126–39. https://doi.org/10.31933/unesrev.v5i4.731.

Qaisar, Sara, dan Kausar Fiaz Khawaja. "Cloud computing: Network/Security Threats and Counter Measures." *Interdisciplinary Journal of Contemporary Research in Business* 3, no. 9 (1 Januari 2012): 1323–29.

Ramli, Ahmad M. "Sniffing, Peretasan Data Pribadi, dan Pembobolan Rekening

Bank Halaman all - Kompas.com." Kompas.com, 5 Februari 2023. https://www.kompas.com/tren/read/2023/02/05/091134365/sniffing-peretasan-data-pribadi-dan-pembobolan-rekening-bank?page=all.

Rosadi, Sinta Dewi, dan Garry Gumelar Pratama. "Urgensi Perlindungan Data Privasi Dalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4, no. 1 (28 Juni 2018): 88–110. https://doi.org/10.25123/vej.v4i1.2916.

Sari, Erlina Permata, Deyana Annisa Febrianti, dan Riska Hikmah Fauziah. "Fenomena Penipuan Transaksi Jual Beli Online Melalui Media Baru Berdasarkan Kajian Space Transition Theory." *Deviance Jurnal Kriminologi* 6, no. 2 (31 Desember 2022): 153–68. https://doi.org/10.36080/djk.1882.

Setiawan, Herdi, Mohammad Ghufron, dan Dewi Astutty Mochtar. "Perlindungan Hukum terhadap Data Pribadi Konsumen dalam Transaksi e-Commerce." *MLJ Merdeka Law Journal* 1, no. 2 (9 November 2020): 102–11. https://doi.org/10.26905/mlj.v2i1.5496.

Setiawati, Diana, Hary Abdul Hakim, dan Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (23 Oktober 2020): 95–109. https://doi.org/10.18196/iclr.2219.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (25 Maret 2021): 38–52. https://doi.org/10.47268/sasi.v27i1.394.

Tanuwidjaja, Tan Henny. "Tanggung Gugat Dalam Transaksi Melalui Internet Banking." *Universitas Narotama Surabaya* 3 (2019): 21–34.

Telaumbanua, Taufik Hidayat. "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif." *LEX PRIVATUM* 13, no. 1 (4 Januari 2024): 1–24. https://ejournal.unsrat.ac.id/v3/index.php/lexprivatum/article/view/53779.

Thomas, Joice Irma Runtu. "Pertanggungjawaban Bank Terhadap Hak Nasabah Yang Dirugikan Dalam Pembobolan Rekening Nasabah." *Lex et Societatis* 1, no. 1 (2013): 116–21.

VioIina, Delfa, dan Hanna Tasya Zahrani. "Perlindungan Data Pribadi Bagi Nasabah Korban Pembobolan Rekening Melalui Internet Banking Ditinjau Dari Hukum Positif Indonesia." *Jurnal Kepastian Hukum Dan Keadilan* 2, no. 1 (13 Januari 2021): 69–79. https://doi.org/10.32502/khdk.v2i1.3048.

Wahyuni, Willa. "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi." hukumonline.com. Diakses 4 Maret 2024. https://www.hukumonline.com/berita/a/bank-perlu-edukasi-nasabah-terkait-pelindungan-data-pribadi-lt636d737770269/.

Wiguna, Kadek Doni, dan Nyoman Satyayudha Dananjaya. "Pertanggungjawaban Bank Atas Kerugian Nasabah yang Menggunakan Electronic Banking." *Jurnal Kertha Desa* 9, no. 12 (2021): 23–35.

Yulianus, Jumarto. "Jangan Biarkan Korban Kejahatan Digital Berjatuhan." kompas.id, 17 September 2023. https://www.kompas.id/baca/nusantara/2023/09/16/jangan-biarkan-korban-kejahatan-digital-berjatuhan.

Yuniarti, Siti. "Petugas/Pejabat Pelindungan Data Pribadi Dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura." *Business Economic, Communication, and Social Sciences Journal (BECOSS)* 4,

no. 2 (4 Juni 2022): 111–20. https://doi.org/10.21512/becossjournal.v4i2.8377.

Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, dan Arief Budiono. "Personal Data Protection Law in Digital Banking Governance in Indonesia." *Studia Iuridica Lublinensia* 32, no. 1 (28 Maret 2023): 99–130. https://doi.org/10.17951/sil.2023.32.1.99-130.

Zulfa, Mulki Indana, Silvester Tena, dan Sampurna Dadi Rizkiono. "Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android." *RENATA: Jurnal Pengabdian Masyarakat Kita Semua* 1, no. 1 (10 April 2023): 7–10. https://doi.org/10.61124/1.renata.4.