

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

*by* Yurispruden Journal

---

**Submission date:** 15-Dec-2023 05:42AM (UTC+0530)

**Submission ID:** 2259374963

**File name:** Inerabilities\_In\_Cybercrime\_Sniffing\_Bank\_Account\_Break-Ins.docx (122.61K)

**Word count:** 5258

**Character count:** 30724



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

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

### Article

#### Article History

Received: \_\_\_\_\_  
Reviewed: \_\_\_\_\_  
Accepted: \_\_\_\_\_  
Published: \_\_\_\_\_

#### DOI:

10.33474/yur.v.i.19533

### Abstract (Times New Roman 12, Bold, 1 Spasi)

*In the digital age cybercrime, particularly Sniffing, poses a threat as perpetrators hack personal data for unauthorized access to victims' bank accounts, causing widespread concern. The purpose of this study is to explore legal protection measures for bank customer data to ensure security against Sniffing cybercrime in order to feel safe and protected from the cybercrime. The research uses a normative legal approach with secondary data consisting literature study. Analysis method uses a qualitative method to produce information that is descriptive analysis. the result is, based on Law 27 of 2022, have indicated legal protection for the rights of data subjects. Data protection for Sniffing victims have also been established in accordance with Bank Indonesia Regulation No. 3 of 2023. Additionally, key preventive measures, such as data encryption and user awareness, play a crucial role in safeguarding personal data, so the society become more conscious of the threat posed by Sniffing.*

**Keywords:** Sniffing, Cyber Crime, Personal Data Protection, Digital Economy, Banking

**Abstract (Times New Roman 12, Bold, 1 space)**

Di era digital, kejahatan siber, khususnya Sniffing, menjadi ancaman karena pelaku meretas data pribadi untuk akses tidak sah ke rekening bank korban, sehingga menimbulkan kekhawatiran yang meluas. Tujuan dari penelitian ini adalah untuk mengeksplorasi langkah-langkah perlindungan hukum terhadap data nasabah bank untuk memastikan keamanan terhadap kejahatan siber Sniffing agar merasa aman dan terlindungi dari kejahatan siber tersebut. Penelitian ini menggunakan pendekatan hukum normatif dengan data sekunder berupa studi kepustakaan. Metode analisis menggunakan metode kualitatif untuk menghasilkan informasi yang bersifat deskriptif analisis. Hasil penelitian menunjukkan bahwa berdasarkan UU No. 27 Tahun 2022 telah mengindikasikan adanya perlindungan hukum terhadap hak-hak subjek data. Perlindungan data bagi korban Sniffing juga telah ditetapkan sesuai dengan Peraturan Bank Indonesia No. 3 Tahun 2023. Selain itu, langkah-langkah pencegahan utama, seperti enkripsi data dan kesadaran pengguna, memainkan peran penting dalam melindungi data pribadi, sehingga masyarakat menjadi lebih sadar akan ancaman yang ditimbulkan oleh Sniffing.

**Keywords:** Sniffing, Kejahatan Siber, Pelindungan Data Pribadi, Ekonomi Digital, Perbankan.

## INTRODUCTION

The progress of the times and technology is running faster, the era of digitalization spreads to various sectors such as education, business, banking, government, and many more. These advances are based on efficiency and effectiveness efforts where the source of supporting files is called a database. By using the database, all forms of activities can be easily and can be accessed at any time.<sup>1</sup>

In this technological advancement, there are various kinds of positive and negative impacts. One of the impacts of technological advances that we will discuss is technological advances in the banking sector. Our form of technological advancement in banking is Mobile Banking. The good impact is that customers can easily make transactions more efficiently but the bad impact is the possibility for hackers to hack the bank system.<sup>2</sup> Therefore, a bank security system must be able to protect its customers to avoid losses.

<sup>1</sup> Muhamad Danuri et al., "PERKEMBANGAN DAN TRANSFORMASI TEKNOLOGI DIGITAL," n.d.

<sup>2</sup> Azhari, Lutfu Qolifera Muhammad, and Carolus Gaza Nindra Tama, "Android Mobile Banking

Application Security from Reverse Engineering and Network Sniffing," *International Journal of Computer Science and Information Security* 14, no. 10 (2016): 461–66.

One form of crime that threatens bank customers with today's technological advances is Sniffing. Network Sniffing is a network security problem where a Hacker can hack a password that is not securely encrypted and the Hacker can capture the data during transmission as a third party.<sup>3</sup> With the large number of internet network usage in Indonesia around 54.68% of the total population in Indonesia or 143.26 million in 2017, it is vulnerable to hacking by stealing personal data of the Indonesian people.<sup>4</sup> The impact of Sniffing as a bank customer is the theft of personal data, where the personal data is misused which can lead to the breach of bank account balances.<sup>5</sup>

Quoted from Antaranews.com (2023) said that until June 12, 2023, OJK OJK has received reports of cybercrime which is committed outside the financial services institution with bank account breaches including Fraud, Social Engineering, Skimming, Spam And Also Sniffing as many as 1,931 cases in Central

Java.<sup>6</sup> Sniffing cybercrime in Indonesia has several times victimized bank customers ranging from losses of hundreds of millions to billions of rupiah that have been reported to the Financial Services Authority (OJK). In early September 2023, there was a businessman from Banjar who had been reported to the South Kalimantan Regional Police who was a victim of cybercrime by hacking through the APK like installation which led to the break-in of bank accounts with a total loss of IDR 1.5 billion rupiah.<sup>7</sup> Sniffing cybercrime will continue to grow and it will inconvenience bank customers.

The important point in the case is how the banking system security is made strong to be able to secure the personal data of bank customers so that it cannot be hacked which causes losses to bank customers.<sup>8</sup>

Personal data protection in the banking sector is very important because Indonesia itself is in the process of transitioning from the traditional economic era to the digital economic era. Everything

<sup>3</sup> Sara Qaisar and Kausar Fiaz Khawaja, "Cloud Computing : Network / Security Threats and Countermeasures CLOUD COMPUTING : NETWORK / SECURITY THREATS AND," no. January 2012 (2018).

<sup>4</sup> Diana Setiawati, Hary Abdul Hakim, and 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 (2020): 2–9, <https://doi.org/10.18196/iclr.2219>.

<sup>5</sup> Prof. Dr. Ahmad M Ramli, "Sniffing, Peretasan Data Pribadi, Dan Pembobolan Rekening Bank," *Kompas.Com*, 2023, [https://www.kompas.com/tren/read/2023/02/05/](https://www.kompas.com/tren/read/2023/02/05/091134365/sniffing-peretasan-data-pribadi-dan-pembobolan-rekening-bank?page=all)

091134365/sniffing-peretasan-data-pribadi-dan-pembobolan-rekening-bank?page=all.

<sup>6</sup> AntaraNews.com, "OJK: Waspada! Penipuan Dengan Modus 'Sniffing,'" *AntaraNews*, 2023, <https://www.antaranews.com/berita/3608289/ojk-waspada-penipuan-dengan-modus-sniffing>.

<sup>7</sup> JUMARTO YULIANUS, "Jangan Biarkan Korban Kejahatan Digital Berjatuh," *Kompas.id*, 2023.

<sup>8</sup> Cholrul Anam, "OJK Ingatkan Modus Penipuan Sniffing, Bisa Kuras Isi Rekening!," *Bisnis.Com*, 2023, <https://finansial.bisnis.com/read/20230712/90/7673998/ojk-ingatkan-modus-penipuan-sniffing-bisa-kuras-isi-rekening>.



related to the economy of society began to be digitized. Trade and payment transactions began to use information and communication technology following the flow of technological developments.<sup>9</sup> Reflecting on the factors that drive these changes, like a double-edged sword, it becomes an increase in the welfare and progress of human civilization and also becomes a new gap for certain individuals to commit unlawful acts, so new laws arise that confirm the phenomenon of change due to advances in technology.<sup>10</sup>

The regulation and modernization of Law Number 27 Year 2022 on Personal Data Protection has replaced the provisions of Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia which mandates the protection of personal data. Provisions regarding hacking are outlined in Law No. 27 of 2022 on Personal Data Protection. Such acts include the unlawful acquisition or collection of personal data that does not belong to the hacker, for his or her benefit or the benefit of others; doing so may result in monetary

loss to the legal owner of the personal data.<sup>11</sup>

Based on a previous scientific investigation, which examined the safeguarding of personal information for clients who were victims of account theft through Internet Banking (Violina and Zahrani, 2018).<sup>12</sup> Our research has a renewal by using the analysis of Law No.27 of 2022 concerning Personal Data Protection which in previous studies only analyzed based on Positive Law in Indonesia.

How can the legislation contained in Law No.27 of 2022 concerning Personal Data Protection be implemented in a bank policy that can provide security and protection to its customers. The urgency of our research is due to the rise of cybercrime Sniffing following the flow of economic development in the digital era and raising public awareness of their personal data so as not to be misused by individuals and become victims of Sniffing crimes. The legal umbrella with the existence of Law No.27 of 2022 concerning Personal Data Protection of the Public hopes that this can

<sup>9</sup> Sinta Dewi Rosadi and Garry Gumelar Pratama, "Urgensi Perlindungan data Privasi dalam Era Ekonomi Digital Di Indonesia," *Veritas et Justitia* 4, no. 1 (2018): 91, <https://doi.org/10.25123/vej.2916>.

<sup>10</sup> Dewi Ningsih Setia and Rani Permatasari Indah, "PENAGGULANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) YANG MENIMBULKAN KEGADUHAN DAN PERMUSUHAN MELALUI PENDEKATAN PENAL POLICY DI WILAYAH HUKUM POLRESTABES MEDAN," *Ensiklopedia of Journal* 2,

no. 2 (2020): 262-67, <http://jurnal.ensiklopediaiku.org>.

<sup>11</sup> Prof. Dr. Ahmad M Ramli, "Sniffing, Peretasan Data Pribadi, Dan Pembobolan Rekening Bank."

<sup>12</sup> Delfa Violina and 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 (2021): 69, <https://doi.org/10.32502/khdik.v2i1.3048>.

successfully provide legal protection. Therefore, this research is conducted to find out the form of efforts to enforce the Protection of personal data of the community in this case bank customers so that bank customers can feel safe and protected from the threat of cybercrime Sniffing.

Following what has been described above, it can be formulated into the main discussion in this study, namely: First, How is the enforcement of bank customers' personal data protection based on Law No.27 Year 2022 on Personal Data Protection? Second, What is the bank's responsibility towards the victims of sniffing? This research is conducted to explain the legal protection of sniffing victims of bank account breaches based on Law No.27 Year 2022 on Personal Data Protection in addition to explaining how banks bear responsibility for consumers who are victims of sniffing.

Normative legal inquiry is the research method used in this article. Normative legal research, as defined by Peter Mahmud Marzuki (2007), involves the systematic examination of legal principles, legal rules, and legal doctrines to

provide solutions to legal cases under investigation.<sup>13</sup>

We therefore use normative legal research, as we use literature studies to answer our problem formulation. The data we use are primary legal materials, namely Law No.27 of 2022 concerning Personal Data Protection and Bank Indonesia Regulation No. 3 of 2023 concerning Bank Indonesia Consumer Protection, secondary legal materials using books, journals, doctrines, legal cases that can support our research. We also use tertiary legal materials, namely legal encyclopedias.

The data collection technique we use is a literature study by quoting and analyzing the legal materials we obtain. And then the data that we have obtained is then analyzed qualitatively. We use qualitative analysis by producing descriptive explanations based on written data that has been collected and not based on numbers. Qualitative research is naturalistic research which, as defined by Hendryadi et al. (2019: 218), seeks to deeply understand social phenomena in their natural state.<sup>14</sup>

## RESULT AND DISCUSSION

<sup>13</sup> Peter Mahmud Marzuki, *Penelitian Hukum / Prof. Dr. Peter Mahmud Marzuki, S.H., M.S., LL.M.*, Edisi revisi (Jakarta : Kencana, 2019) (2019, n.d.).

<sup>14</sup> A B Ndraha, Y Telaumbanua, and Hasan Toyib, "Kolaborasi Sumber Daya Manusia Dalam Pencapaian Target Dan Sasaran Kinerja Lkpd Pada

Dinas Ketahanan Pangan, Pertanian Dan Perikanan Kabupaten Nias," *Collaborative of Human Resources in Achieving Lkpd Targets and Performance Goals At Dinas Ketahanan Pangan Pertanian Dan Perikanan of Nias Regency* 10, no. 4 (2022): 1508–16.

## Forms of Bank Customer Personal Data Protection Based on the PDP Law

Personal data is the right to privacy of an individual where an individual has the right to be able to protect the personal data and whether or not his personal data is given to other parties.<sup>15</sup> Protection of personal data includes protection at several stages such as in the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of personal data.<sup>16</sup> Protection of personal data 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.<sup>17</sup> In this case, personal data is the object of protection regulated in Law No.27 of 2022 concerning Personal Data Protection. In accordance with the PDP Law (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 individually and personally in conjunction with other information.<sup>18</sup>

As referred to in paragraph (1) of article 4 of the PDP Law, 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.

In contrast, as referred to in paragraph (3) of article 4, personal data generally consists of full name, nationality, gender, marital status, religion, and other personal information that can be used to identify an individual.<sup>19</sup> Regulations related to the scope of personal data as described in Article 4 of the PDP Law have also been regulated in other regulations.

<sup>15</sup> Sekarling Ayumelda Kusnadi, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16, <https://doi.org/10.47776/alwasath.v2i1.127>.

<sup>16</sup> Wardah Yuspin et al., "Personal Data Protection Law in Digital Banking Governance in Indonesia," *Studia Iuridica Lublinska* 32, no. 1 (2023): 99–130, <https://doi.org/10.17951/sil.2023.32.1.99-130>.

<sup>17</sup> Rina Arum Prastyanti et al., "Law And Personal Data : Offering Strategies For Consumer Protection In New Normal Situation In Indonesia," *JURNAL JURISPRUDENCE* 11, no. 1 (2021): 82–99,

<https://doi.org/10.23917/jurisprudence.v11i1.14756>.

<sup>18</sup> Willa Wahyuni, "Dua Jenis Data Pribadi Yang Perlu Dilindungi Menurut UU PDP," *HukumOnline.Com*, 2022, <https://www.hukumonline.com/berita/a/dua-jenis-data-pribadi-yang-perlu-dilindungi-menurut-uu-pdp-lt6349e2932bd09/#!>

<sup>19</sup> Ditama Binbangkum - BPK RI and Bpk.go.id, "Undang-Undang Perlindungan Data Pribadi," *Ditama Binbangkum - BPK RI*, no. 016999 (2022): 1–50, <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>,



With the revocation of Bank Indonesia Regulation No. 7/6/PBI/2005 concerning Transparency of Bank Product Information and Use of Customer Personal Data, POJK No.6 of 2022 discusses consumer and community protection in the financial services sector. Individual personal data and information as referred to in paragraph (2) of article 11 includes: Name, Address, Population Identification Number, Telephone Number, 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 Number (1) POJK Number 6 of 2022 concerning Consumer and Community Protection in the Financial Services Sector.<sup>20</sup> Based on the explanation above, the scope related to Personal Data Information is in line with the scope contained in the PDP Law.

Commercial Banks as Financial Services Business Actors should provide transparency regarding the processing of customer personal data. The processing of personal data has been regulated in Article 16 of the PDP Law. In addition, commercial banks are required to maintain the

confidentiality of their customers' personal information in their administration. Providing protection to customers' personal data is a form of commitment given by banks to their customers in order to maintain the integrity of the data that has been provided by customers in the form of financial data.<sup>21</sup> Based on the PDP Law, financial data is specific personal data.

Public entities, including banks, have an obligation to function both as controllers and processors of personal data. 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 in Article 20 of the PDP Law. To treat personal data following the law and to support legitimate interests, this law must be complied with, while considering the purposes, and requirements, and balancing the interests of the data controller and the data subject.<sup>22</sup>

As a customer of a financial institution, you are entitled to information

<sup>20</sup> OJK, "Peraturan OJK No. 14/POJK.04/2022 Tahun 2022," no. 99 (2022).

<sup>21</sup> Willa Wahyuni, "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi," *HukumOnline.Com*, 2022,

<https://www.hukumonline.com/berita/a/bank-perlu-edukasi-nasabah-terkait-pelindungan-data-pribadi-tt636d737770269/>.

<sup>22</sup> RI and Bpk.go.id, "Undang-Undang Perlindungan Data Pribadi."



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. The bank also has to be able to provide education to its customers and if there are changes, as expressly stipulated in paragraph (1) and paragraph (2) of Article 21 of the PDP Law, 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.

In Bank Indonesia Regulation Number 3 of 2023 concerning Bank Indonesia Consumer Protection in article 36, it is sufficient to explain that the organizer is obliged to provide access to consumers, in this case, it can be said that the customer is related to a copy of personal data following the PDP Law and authorizes individuals to delete, stop, and/or eliminate personal information following the PDP Law. If there are organizers who do not fulfill these obligations, they can be subject to administrative sanctions.<sup>23</sup>

The agreement clause is considered void and unenforceable under the PDP Law on Personal Data Processing if it does not

include the express and valid consent of the individual whose personal data is being processed. Where the subject of the personal data is a child, the personal data controller is specifically required to obtain the consent of the child's parent or guardian to provide evidence of the consent that has been given. This also applies to persons with disabilities; however, following legal requirements, we only do this with the consent of the person with a disability or their legal guardian through the use of an approved method of communication. So the processing of personal data cannot be done arbitrarily without the consent of the personal data subject.

To maintain security, data controllers must prevent unauthorized individuals from making changes to personal information if doing so would endanger the safety of the data subject or others, jeopardize the disclosure of the data of others, or interfere with national defense and security operations. As per Article 33 of the PDP Law, this is so. In addition, in situations where the processing of personal data poses a significant risk to certain individuals or entities, the Organization responsible for the personal information shall conduct an impact analysis on data protection at least once.

<sup>23</sup> Bank Indonesia, "PERATURAN BANK INDONESIA NOMOR 3 TAHUN 2023," 2023,

[https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI\\_032023.pdf](https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI_032023.pdf).

Article 47 of the Personal Data Protection Law states that the data controller is responsible for the processing of 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.<sup>24</sup> To effectively enforce the protection of personal data, the PDP Law does not only stand alone in providing legal protection, there are other supporting regulations, and bank policies that actively participate in efforts to protect the personal data of their customers following the policies and objectives of the PDP Law.

In ensuring the protection of personal data and information of bank customers, there is a coordinator who is responsible for the protection of data and/or 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/or 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 (SPO A) - Operation Strategy and Development Group (GPOL). This component is important to collect all contributions from collaborating work units, guide them in conducting evaluations and reviews, and ultimately continue business processes that require data and/or information security.<sup>25</sup>

Regarding the protection of personal data in the PDP Law, there is an institution that will be established specifically by the president and is responsible to the president. The institution has the authority to impose administrative sanctions on public bodies, corporations, individuals, and international organizations. In addition, this institution has the jurisdiction to assist law enforcement officials in handling situations involving individuals and companies suspected of committing personal data breaches.<sup>26</sup>

<sup>24</sup> Sagdiyah Fitri Andani Tambunan Agung and 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 (2023): 5–7, <https://doi.org/10.47233/jemb.v2i1.915>.

<sup>25</sup> Bca.co.id, "Kebijakan Perlindungan Data Dan / Atau Informasi Konsumen," 2022, <https://www.bca.co.id/->

[/media/Feature/Report/File/58/Kebijakan-GCG/20230731-kebijakan-perlindungan-data-informasi-konsumen.pdf?funnel\\_source=searchresult](/media/Feature/Report/File/58/Kebijakan-GCG/20230731-kebijakan-perlindungan-data-informasi-konsumen.pdf?funnel_source=searchresult).

<sup>26</sup> Engelbertus Wendratama, "UU PDP Sah, Ini 3 Syarat Lembaga Perlindungan Data Pribadi," *Magdalene.Com*, 2023, <https://magdalene.co/story/apa-itu-lembaga-perlindungan-data-pribadi/#:~:text=Lembaga pelindung data pribadi ini akan dibentuk oleh,dan>

As a form of protection of customers' personal data based on the PDP Law, it can be said that it is sufficient as an initial form of government sensitivity to the urgency of legal protection of personal data, although until the time this article was made, there has not been the formation of a special institution in charge of organizing personal data protection whose roles, duties, and authorities have been written in the PDP Law Article 58 to Article 60 of the PDP Law, which has the importance of protecting personal data in today's digital era.

#### Forms of Bank Responsibility for Sniffing Victims

Sniffing is a form of cybercrime that is carried out by a malicious program commonly called (malware). The action is clearly very detrimental to the victim. By unlawfully obtaining confidential information and data through the internet network.<sup>27</sup> With the insecurity of technology networks, lack of understanding of digital security, use of unsecured Wi-Fi networks, and sharing of personal information, there is an opportunity to become a victim of Sniffing cybercrime.<sup>28</sup> Important personal

information, including credit card details, emails, and 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 installed, damages or steals important personal data on the phone.

In the PDP Law, the unlawful act of stealing other people's personal data has been regulated specifically in Article 67 paragraph (1) The regulation in question regulates the actions of parties who intentionally access or collect personal data that does not belong to them, with the intention of utilizing it for personal gain or causing harm to the data subject, can face imprisonment of up to five years in prison or a maximum fine of five billion rupiah. Additional safeguards are stipulated in Article 48 of the ITE Law in conjunction with Article 32. These safeguards carry a maximum penalty of five billion rupiah plus a ten-year prison sentence.<sup>29</sup>

In studying the concept of responsibility linguistically, responsibility has various meanings. There are two terms, namely Responsibility which has a social

Pusat Pelaporan dan Analisis Transaksi Keuangan %28PPATK%29.

<sup>27</sup> Mulki Indana Zulfa, Silvester Tena, and Sampurna Dadi Rizkiono, "Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android," *RENATA: Jurnal Pengabdian Masyarakat Kita*

*Semua* 1, no. 1 (2023): 7–16,

<https://doi.org/10.61124/1.renata.4>.

<sup>28</sup> YULIANUS, "Jangan Biarkan Korban Kejahatan Digital Berjatuh.".

<sup>29</sup> "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," 2008, 1–19.



orientation and liability which is a form of juridical responsibility.<sup>30</sup>

Looking at the concept of sniffing cybercrime, which is tapping with the aim of stealing personal data in the form of important information that even involves the victim's banking information.<sup>31</sup> If the cyber attack is centered on attacking the bank system which aims to steal the personal data of its customers, the bank as the controller of personal data should be juridically responsible for the losses received by the customer. The loss suffered by the customer is guaranteed by the bank. 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.<sup>32</sup> 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 the PDP Law.

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.<sup>33</sup> 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 financial management activities of the customer following the agreed guidelines. In the case of i-banking, this authority is derived from the instructions given by the original customer through the use of User ID and PIN, unless denied through judgment or evidence to the contrary.<sup>34</sup>

As a personal administrator, the bank is responsible for preventing unauthorized access to personal information that is not accessed by the authorized subject of the information. By utilizing electronic security systems in a reliable, secure, and accountable manner, this prevention can be achieved. Personal data controllers are obliged to fulfill these duties following Article 39 of the PDP Law.

Following the obligations of the personal data controller contained in Article 39 of the PDP Law, if the electronic security system owned by the bank fails to protect

<sup>30</sup> Dewoto Kusumo and Rifki Afandi, "Vicarious Liability in Personal Data Protection," *Indonesian Journal of Innovation Studies* 13, no. 2 (2020): 1–12.

<sup>31</sup> Eril Obelt Choiri, "Sniffing Adalah Tindakan Pencurian, Ini Cara Menghindarinya!," *GudangSSL*, 2023, <https://gudangssl.id/blog/apa-itu-sniffing/>.

<sup>32</sup> Willa Wahyuni, "Bentuk Pertanggungjawaban Bank Kepada Nasabah Saat Serangan Siber," *HukumOnline.com*, 2023,

<https://www.hukumonline.com/benta/a/bentuk-pertanggungjawaban-bank-kepada-nasabah-saat-serangan-siber-ht64997b3673273/?page=all>.

<sup>33</sup> Danang Kurniawan, "Initiating the Establishment of Digital Banks in Indonesia: A Juridical Study," *Journal of Transcendental Law* 4, no. 1 (2022): 1–15, <https://doi.org/10.23917/jtl.v4i1.17311>.

<sup>34</sup> Tan Henry Tanuwidjaja, "Tanggung Gugat Dalam Transaksi Melalui Internet Banking," *Universitas Narotama Surabaya* 3, no. April (2019): 21–34.



the personal data of its customers, it is the responsibility of the bank to be responsible for the losses suffered by customers.

In organizing an electronic system, in Article 16 letter b of the ITE Law, business actors are required to maintain the confidentiality and integrity of the electronic system in its implementation.

If the bank fails to protect the personal data of its customers, within three days, after realizing a data breach, 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 the PDP Law contain provisions regarding notification of personal data protection breaches. Violation of the PDP Law, particularly Article 57, may result in administrative sanctions for not safeguarding the personal information of bank customers.

Based on paragraphs (1) and (2) of article 42 of Bank Indonesia Regulation Number 3 of 2023 concerning Bank Indonesia Consumer Protection, the organizer is responsible for any losses suffered by customers due to errors, omissions, or actions that violate regulatory provisions. The implementation of laws

and regulations is the responsibility of various entities, including the directors, board of commissioners, management, employees of the organization, and third parties who represent or work for the benefit of the organization. The organization is not liable for any loss that can be proven to be caused by the customer's carelessness or fault.

In the process of compensating for the losses suffered by customers, there is a first proof related to the cause of customer losses. The proof is carried out by the bank by bringing transaction data to the customer.<sup>36</sup>

Article 12 of the PDP Law describes the rights of personal data subjects, including the ability to initiate legal proceedings and request compensation. However, the specific procedure to be followed when filing a compensation claim remains unclear.

But in the positive legal system in Indonesia, a consumer, in this case, a customer of a bank, can sue someone for allegedly damaging his or her goods or services; often, breach of contract or illegal behavior is the basis for such cases.<sup>37</sup>

<sup>36</sup> Kadek Doni Wiguna and Nyoman Satyayudha Dananjaya, "Pertanggungjawaban Bank Atas Kerugian Nasabah Yang Menggunakan Electronic Banking," *Jurnal Kertha Desa* 9, no. 12 (2021): 23–35.

<sup>37</sup> Wiguna and Dananjaya.

<sup>37</sup> Joice Irma Runtu Thomas, "PERTANGGUNGJAWABAN BANK TERHADAP HAK NASABAH YANG DIRUGIKAN DALAM PEMBOBOLAN REKENING NASABAH," *Lex et Societatis* 1, no. 1 (2013): 116–21, <https://ejournal.unsrat.ac.id/index.php/lexetsocietatis/article/viewFile/1320/1071>.

If in a case the customer has suffered losses as a result of sniffing. The bank must provide accountability efforts to its customers in terms of handling and resolving the losses suffered by customers. The bank must swiftly respond and convey several stages as a form of accountability to customers, some forms of bank accountability efforts are as follows; Complain Handling; Peaceful Efforts, Banking Mediation, and Court Lines.<sup>38</sup>

Although all forms of personal data protection and their responsibilities have been legally regulated in the PDP Law 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 provides confusion in protecting victims.

Therefore, we as the general public and also as users of electronic banking services 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. In addition, unsolicited calls containing questionable files should be avoided.<sup>39</sup>

## CONCLUSION

Law No. 27 of 2022 on Personal Data Protection, in this case called the PDP Law, can be said to be sufficient as a 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 the processing of personal data. Although there is a special institution that has been mandated in Articles 58 to 60 of the PDP Law, which until this research was made, there has not been the formation of a special 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 personal data.

<sup>38</sup> Tanuwidjaja, "Tanggung Gugat Dalam Transaksi Melalui Internet Banking."

<sup>39</sup> Alicia Diahwahyuningtyas and Rizal Setyo Nugroho, "Ramai Soal Sniffing, Modus Penipuan Resi Hingga Undangan Yang Bisa Curi Saldo

Rekening," *Kompas.Com*, 2023, <https://www.kompas.com/tren/read/2023/01/29/183000165/ramai-soal-sniffing-modus-penipuan-resi-hingga-undangan-yang-bisa-curi?page=all>.

As a form of responsibility for the losses suffered by customers, the PDP Law has not yet regulated exactly who can be said to be responsible for the act of cybercrime Sniffing. Although in Article 47 of the PDP Law, the personal data controller is said to be responsible, 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, we feel that these efforts are not sufficient 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 the conceptual liability and dispute resolution in the PDP Law which cannot provide legal certainty for victims of cybercrime sniffing.

## REFERENCES

- Agung, Sagdiyah Fitri Andani Tambunan, and 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 (2023): 5–7. <https://doi.org/10.47233/jemb.v2i1.915>.
- Alicia Diahwahyuningtyas, and Rizal Setyo Nugroho. "Ramai Soal Sniffing , Modus Penipuan Resi Hingga Undangan Yang Bisa Curi Saldo Rekening." *Kompas.Com*, 2023. <https://www.kompas.com/tren/read/2023/01/29/183000165/ramai-soal-sniffing-modus-penipuan-resi-hingga-undangan-yang-bisa-curi?page=all>.
- AntaraNews.com. "OJK: Waspada Penipuan Dengan Modus 'Sniffing.'" *AntaraNews*, 2023. <https://www.antarane.ws.com/berita/3608289/ojk-waspada-penipuan-dengan-modus-sniffing>.
- Azhari, Lucgu Qolfiera Muhammad, and Carolus Gaza Nindra Tama. "Android Mobile Banking Application Security from Reverse Engineering and Network Sniffing." *International Journal of Computer Science and Information Security* 14, no. 10 (2016): 461–66.
- Bca.co.id. "Kebijakan Perlindungan Data Dan / Atau Informasi Konsumen," 2022. [https://www.bca.co.id/-/media/Feature/Report/File/S8/Kebijakan-GCG/20230731-kebijakan-perlindungan-data-informasi-konsumen.pdf?funnel\\_source=searchresult](https://www.bca.co.id/-/media/Feature/Report/File/S8/Kebijakan-GCG/20230731-kebijakan-perlindungan-data-informasi-konsumen.pdf?funnel_source=searchresult).
- Choirul Anam. "OJK. Ingatkan Modus Penipuan Sniffing. Bisa Kuras Isi Rekening!" *Bisnis.Com*, 2023. <https://finansial.bisnis.com/read/20230712/901673998/ojk-ingatkan-modus-penipuan-sniffing-bisa-kuras-isi-rekening>.
- Danuri, Muhamad, Manajemen Informatika, Jakarta Teknologi, and Cipta Semarang. "PERKEMBANGAN DAN TRANSFORMASI TEKNOLOGI



- DIGITAL," n.d.
- Dewi Rosadi, Sinta, and Garry Gumelar Pratama. "Urgensi Perlindungan data Privasi dalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4, no. 1 (2018): 91. <https://doi.org/10.25123/vej.2916>.
- Indonesia, Bank. "PERATURAN BANK INDONESIA NOMOR 3 TAHUN 2023," 2023. [https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI\\_032023.pdf](https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI_032023.pdf).
- Kurniawan, Danang. "Initiating the Establishment of Digital Banks in Indonesia: A Juridical Study." *Journal of Transcendental Law* 4, no. 1 (2022): 1–15. <https://doi.org/10.23917/jtl.v4i1.1731>.
- Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>.
- Kusumo, Dewoto, and Rifki Afandi. "Vicarious Liability in Personal Data Protection." *Indonesian Journal of Innovation Studies* 13, no. 2 (2020): 1–12.
- Marzuki, Peter Mahmud. *Penelitian Hukum / Prof. Dr. Peter Mahmud Marzuki, S.H., M.S., LL.M.* Edisi rev. Jakarta: Kencana, 2019 © 2019, n.d.
- Ndraha, A B, Y Telaumbanua, and Hasan Toyib. "Kolaborasi Sumber Daya Manusia Dalam Pencapaian Target Dan Sasaran Kinerja Lkpj Pada Dinas Ketahanan Pangan, Pertanian Dan Perikanan Kabupaten Nias." *Collaborative of Human Resources in Achieving Lkpj Targets and Performance Goals At Dinas Ketahanan Pangan Pertanian Dan Perikanan of Nias Regency* 10, no. 4 (2022): 1508–16.
- Ningsih Setia, Dewi, and Rani Permatasari Indah. "PENAGGULANGAN KEJAHATAN TEKNOLOGI INFORMASI (CYBER CRIME) YANG MENIMBULKAN KEGADUHAN DAN PERMUSUHAN MELALUI PENDEKATAN PENAL POLICY DI WILAYAH HUKUM POLRESTABES MEDAN." *Ensiklopedia of Journal* 2, no. 2 (2020): 262–67. <http://jurnal.ensiklopediaiku.org>.
- Obelt Choiri, Eri. "Sniffing Adalah Tindakan Pencurian, Ini Cara Menghindarinya!" *GudangSSL*. 2023. <https://gudangssl.id/blog/apa-itu-sniffing/>.
- OJK. "Peraturan OJK No. 14/POJK.04/2022 Tahun 2022," no. 99 (2022).
- Prastyanti, Rina Arum, Istiyawati Rahayu, Eiad Yafi, Kelik Wardiono, and Arief Budiono. "Law And Personal Data : Offering Strategies For Consumer Protection In New Normal Situation In Indonesia." *JURNAL JURISPRUDENCE* 11, no. 1 (2021): 82–99. <https://doi.org/10.23917/jurisprudence.v11i1.14756>.
- Prof. Dr. Ahmad M Ramli. "Sniffing, Peretasan Data Pribadi, Dan Pembobolan Rekening Bank." *Kompas.Com*, 2023. <https://www.kompas.com/tren/read/2023/02/05/091134365/sniffing-peretasan-data-pribadi-dan-pembobolan-rekening-bank?page=all>.
- Qaisar, Sara, and Kausar Fiaz Khawaja. "Cloud Computing: Network / Security Threats and Countermeasures CLOUD COMPUTING : NETWORK / SECURITY THREATS AND," no. January 2012 (2018).



- RI, Ditama Binbangkum - BPK, and Bpk.go.id. "Undang-Undang Perlindungan Data Pribadi." *Ditama Binbangkum - BPK RI*, no. 016999 (2022): 1-50. <https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022>.
- Setiawati, Diana, Hary Abdul Hakim, and 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 (2020): 2-9. <https://doi.org/10.18196/iclr.2219>.
- Tamwidjaja, Tan Henny. "Tanggung Gugat Dalam Transaksi Melalui Internet Banking." *Universitas Narotama Surabaya* 3, no. April (2019): 21-34.
- Thomas, Joice Irma Runtu. "PERTANGGUNGJAWABAN BANK TERHADAP HAK NASABAH YANG DIRUGIKAN DALAM PEMBOBOLAN REKENING NASABAH." *Lex et Societatis* 1, no. 1 (2013): 116-21. <https://ejournal.unsrat.ac.id/index.php/lexetsocietatis/article/viewFile/1320/1071>.
- "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," 2008, 1-19.
- Violina, Delfa, and 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 (2021): 69. <https://doi.org/10.32502/khdk.v2i1.3048>.
- Wahyuni, Willa. "Bank Perlu Edukasi Nasabah Terkait Pelindungan Data Pribadi." *HukumOnline.Com*, 2022. <https://www.hukumonline.com/berita/a/bank-perlu-edukasi-nasabah-terkait-pelindungan-data-pribadi-lt636d737770269/>.
- . "Bentuk Pertanggungjawaban Bank Kepada Nasabah Saat Serangan Siber." *HukumOnline.com*, 2023. <https://www.hukumonline.com/berita/a/bentuk-pertanggungjawaban-bank-kepada-nasabah-saat-serangan-siber-lt64997b3673273/?page=all>.
- . "Dua Jenis Data Pribadi Yang Perlu Dilindungi Menurut UU PDP." *HukumOnline.Com*, 2022. <https://www.hukumonline.com/berita/a/dua-jenis-data-pribadi-yang-perlu-dilindungi-menurut-uu-pdp-lt6349e2932bd09/#!>
- Wendratama, Engelbertus. "UU PDP Sah , Ini 3 Syarat Lembaga Perlindungan Data Pribadi." *Magdalene.Com*, 2023. <https://magdalene.co/story/apa-itu-lembaga-perlindungan-data-pribadi/#:-:text=Lembaga pelindung data pribadi ini akan dibentuk oleh,dan Pusat Pelaporan dan Analisis Transaksi Keuangan%28PPATK%29>.
- Wiguna, Kadek Doni, and 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 Berjatuh." *Kompas Id*, 2023.
- Yuspin, Wardah, Kelik Wardiono, Aditya Nurrahman, and Arief Budiono. "Personal Data Protection Law in Digital Banking Governance in Indonesia." *Studia Iuridica Lublinsia* 32, no. 1 (2023): 99-130. <https://doi.org/10.17951/sil.2023.32.1.99-130>.
- Zulfa, Mulki Indana, Silvester Tena, and Sampurna Dadi Rizkiono. "Aktivitas

Sniffing Pada Malware Pencuri Uang  
Di Smartphone Android.” *RENATA:  
Jurnal Pengabdian Masyarakat Kita*  
*Semua* 1, no. 1 (2023): 7–10.  
<https://doi.org/10.61124/1.renata.4>.

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

ORIGINALITY REPORT

2%

SIMILARITY INDEX

0%

INTERNET SOURCES

3%

PUBLICATIONS

0%

STUDENT PAPERS

PRIMARY SOURCES

1

Robert Walters, Leon Trakman, Bruno Zeller.  
"Data Protection Law", Springer Science and  
Business Media LLC, 2019

Publication

2%

Exclude quotes On  
Exclude bibliography On

Exclude matches < 2%

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

---

PAGE 1

---



**Article Error** You may need to use an article before this word.



**S/V** This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 2

---

PAGE 3

---



**Prep.** You may be using the wrong preposition.



**Run-on** This sentence may be a run-on sentence.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Verb** This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.



**Missing ","** Review the rules for using punctuation marks.

PAGE 4

---



**Run-on** This sentence may be a run-on sentence.



**Article Error** You may need to use an article before this word.

PAGE 5

---



**Missing ","** Review the rules for using punctuation marks.

PAGE 6

---



**Missing ","** Review the rules for using punctuation marks.



**Article Error** You may need to remove this article.





**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.

PAGE 7

---



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.



**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

PAGE 8

---



**Article Error** You may need to remove this article.



**Missing ", "** Review the rules for using punctuation marks.



**Article Error** You may need to remove this article.



**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.



**Run-on** This sentence may be a run-on sentence.



**Prep.** You may be using the wrong preposition.

PAGE 9

---



**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.



**Prep.** You may be using the wrong preposition.



**Run-on** This sentence may be a run-on sentence.



**Proper Nouns** You may need to use a capital letter for this proper noun.

PAGE 10

---



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**S/V** This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Article Error** You may need to remove this article.



**Proper Nouns** You may need to use a capital letter for this proper noun.

PAGE 11

---



**Prep.** You may be using the wrong preposition.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Article Error** You may need to remove this article.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

PAGE 12

---



**S/V** This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.



**Prep.** You may be using the wrong preposition.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Article Error** You may need to use an article before this word.

PAGE 13

---



**Run-on** This sentence may be a run-on sentence.



**P/V** You have used the passive voice in this sentence. You may want to revise it using the active voice.



**Article Error** You may need to remove this article.

PAGE 14

---



**Wrong Article** You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.



**Prep.** You may be using the wrong preposition.

PAGE 15

---

PAGE 16

---

PAGE 17

---