

Harmonization of Theft Prevention Regulations Digital Personal Data in Banking Institutions: Perspective Cybercrime Sniffing

Ryska Noviasari, Wardah Yuspin, Arief Budiono
r100220014@student.ums.ac.id, wy204@ums.ac.id, ab368@ums.ac.id

Faculty of Law, Universitas Muhammadiyah Surakarta, Indonesia

Article Info

Received: 2023-08-12

Revised: 2024-02-21

Accepted: 2024-03-31

Keywords:

Cybercrime; Personal Data; Harmonization; Sniffing Protection

Abstract

This research aims to find out how to harmonize relevant applicable laws and regulations in Cybercrime Sniffing and to analyze the protection provided by law to deal with sniffing cases. This research uses normative research methods. The results of this research are: first, crime regulation sniffing in hacking M Banking via the WhatsApp application, which has been regulated in Article 51 paragraph (2) of the ITE Law and its amendments and Article 67 paragraph (1) of the PDP Law has differences in the aspect of criminal sanctions and/or fines, where the sanctions in the ITE Law and its amendments are more the severity of the sanctions contained in the PDP Law. Refers to the principle of preference, namely the principle of a particular law derogating from the general law and based on teleological/sociological interpretation by looking at the purpose of establishing the law, it can be concluded that in cases of criminal acts in the form of sniffing In the hacking of M Banking via the WhatsApp application, because it relates to personal data breaches, what applies is the provisions of Article 67 paragraph (1) of the PDP Law, because the PDP Law is a regulation that more specifically regulates personal data breaches, so the ITE Law and its amendments are as follows: more general settings should be ruled out. The protection provided by the Act to deal with cases of sniffing M-Banking hacking via the WhatsApp application is regulated by criminal sanctions in Article 67 paragraph (1) of the PDP Law, which can be interpreted to mean that the PDP Law provides criminal sanctions and/or fines to all parties, including banks if there is loss resulting from these actions. Sniffing has implications for harming the victim.

I. Introduction

Banks, as institutions that distribute funds and collect funds from the public, require trust from the public. As an institution of public trust, banks are required to always provide the best service and pay attention to the interests of their customers. Considering all money needs, technological advances in this modern era give people convenience.¹

Banks that improve information technology in their customer services indirectly direct banks to a new era, namely the era of digital banking, by opening accounts and executing transactions. Finance refers to closing savings accounts, which are carried out using information technology. One is an electronic transaction (e-banking) via ATM, phone banking, internet banking, etc.

Internet banking and mobile banking are some innovations in the development of Internet media, which continues to increase rapidly. Hence, customers no longer need to come to the bank's branch or head office to carry out banking transactions. Even now, opening an account can be done via internet banking. Likewise, transactions in e-commerce can also be connected via the mobile banking application.² No longer need to open online buying and selling applications. Internet banking facilities provide many benefits for customers, including sending and receiving money just by connecting to the internet by opening the service application mobile banking (e-banking), mutation checks are obtained via the number WhatsApp, which has been registered.

One of the impacts is related to protecting personal data (protecting privacy rights), namely, hacking of personal information stored, disseminated, and even used by others to carry out unlawful acts. This risk is new and a challenge for practitioners and experts in Internet banking services. System failure can also be caused by system damage, such as unstable network problems or not meeting internet usage capacity. There is technological developments are often used for evil purposes.³ Cyber-enabled crimes are becoming increasingly prevalent as the anonymity afforded by the internet and the volume of information shared online allow individuals to engage in such behavior easily. Smartphone users of all ages should be aware that their phones are vulnerable to attack and also know how

¹ Wuryaningsih Dwi Letari, Damatika Purnama Suci, and Muhammad Sholahuddin, "Beberapa Faktor Yang Mempengaruhi Profitabilitas Perbankan Di Indonesia," *Benefit: Jurnal Manajemen Dan Bisnis* 5, no. 1 (2020): 1-19, <https://journals.ums.ac.id/index.php/benefit/index>.

² Delvyan Putri Surya Ningrum and Jamiatur Robekha, "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia," *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora* 2, no. 4 (2023): 765-76, <https://doi.org/10.56799/peshum.v2i4.2115>.

³ Brianna O'Shea, Nicole L. Asquith, and Jeremy Prichard, "Mapping Cyber-Enabled Crime: Understanding Police Investigations and Prosecutions of Cyberstalking," *International Journal for Crime, Justice and Social Democracy* 10, no. 4 (February 21, 2021): 25-39, <https://doi.org/10.5204/IJCJSD.2096>.

to improve device security. Education is the core of security awareness and capability. Cybersecurity education is critical in reaching all communities and all ages.⁴

The digital world is changing very quickly. All modern economies, education systems, and other systems in industrialized countries are built on advanced information technology and digital technology.⁵ Since the internet was created, people have found ways to carry out illegal activities using the internet as a tool.⁶ The internet is a technological product of this century that is developing worldwide, including in Indonesia. With the internet, someone can carry out several activities simultaneously without having to leave the house, for example, discussing, shopping, transferring money, studying, etc. This is the positive side of the internet. However, the internet cannot be separated from the opposing side by its use as a medium for committing crimes, known as cybercrime. Volodymyr Golubev calls it "the new form of anti-social behavior." There are several types of this crime, for example, economic cyber crime, cyber terrorism, cyberstalking, cybersex, and cyberporn. This shows that all forms of crime in the real world have also occurred in cyberspace.⁷ The internet has never been programmed with an internal security system, and it is now known that the digital environment can be easily infiltrated and exposed to cyber-attacks. For decades, cybercriminals have viewed the security industry with skepticism. Attackers are primarily opportunistic, preying on users who have weak protections but don't put up a fight, and if they find a well-secured system, the attackers aren't interested.⁸

According to the Director of Information Application Control, Ministry of Communication and Informatics, the use of the internet by the public in Indonesia has significantly increased since the COVID-19 pandemic, driven by a shift in Internet usage patterns from offices to regional settlements and changes in people's shopping behavior from offline to online. This increasingly rapid

⁴ Isabella M. Venter et al., "Cyber Security Education Is as Essential as 'the Three R's,'" *Heliyon* 5, no. 12 (2019): 0–7, <https://doi.org/10.1016/j.heliyon.2019.e02855>.

⁵ Rana Saifullah and Sayeda Sassi Roshan Shah, "Transnational Law and Criminal Justice System: Highlighting Legislative and Procedural Challenges to Combat Cyber Crime in the Wake of CPEC," *JISR Management and Social Sciences & Economics* 21, no. 4 (December 30, 2023): 73–92, <https://doi.org/10.31384/jisrmsse/2023.21.4.5>.

⁶ Cecelia Horan and Hossein Saiedian, "Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions," *Journal of Cybersecurity and Privacy* 1, no. 4 (September 30, 2021): 580–96, <https://doi.org/10.3390/jcp1040029>.

⁷ Bambang Sukoco, "Pendekatan Restoratif Justice Sebagai Upaya Penyelesaian Cybercrime Dengan Pelaku Anak (Studi Kasus Penyelesaian Tindak Pidana Anak Usia Sekolah)," *Jurnal Law and Justice* 1, no. 1 (2016): 54–64, <https://doi.org/https://doi.org/10.23917/laj.v1i1.2859>.

⁸ A Pântea, "Cyber Security and Impact on Computer Crimes," *Acta Universitatis Danubius. Juridica* 12, no. 1 (2023): 348–57, <https://www.ceeol.com/search/article-detail?id=1180778>.

digital acceleration must, of course, be accompanied by vigilance. Various modes of cybercrime will continue to develop.⁹

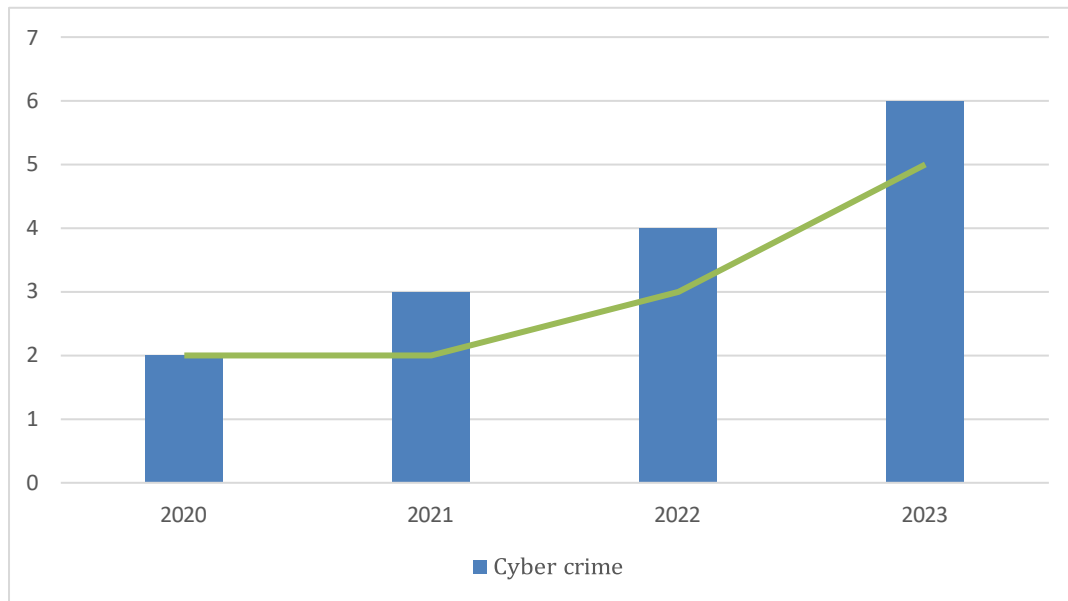


Figure 1. Data Increased cybercrime

Since March 2020, the total number of complaints received has been almost 200,000 report fraud, with the most used media being WhatsApp and Instagram, which will increase yearly until 2023.¹⁰ There are 5,000 reports of complaints about fraudulent activities (fraud) who enter the Ministry of Communication and Information website every week. Since March 2020, the total number of complaints we have received is almost 200,000 fraud reports, with the most used media being WhatsApp and Instagram. These statistics show that Indonesia is already in an emergency cybercrime situation. One of the efforts made by the Ministry of Communication and Information to support transactions online safely for consumers and financial services players is the launch of the Cek Rekening.id site. This site functions as a portal for collecting a database of bank accounts suspected of being suspected of criminal activity.

Enhancement of online traffic transactions of e-commerce, which is driving the increase in cybercrime in the banking sector, is also a concern for the Indonesian Police. From 2017 to 2020, 16,845 reports of criminal acts of cyber fraud were

⁹ David Buil-Gil, Yongyu Zeng, and Steven Kemp, "Offline Crime Bounces Back to Pre-COVID Levels, Cyber Stays High: Interrupted Time-Series Analysis in Northern Ireland," *Crime Science* 10, no. 1 (2021): 1–16, <https://doi.org/10.1186/s40163-021-00162-9>.

¹⁰ Yuslia Naili Rahmah, "Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah 'Istimewa Yogyakarta,'" *Jurnal Pendidikan Ekonomi* 7, no. 6 (2018): 579–88, <https://proxsisgroup.com/articles/waspadailah-hantaman-serangan-cyber-terhadap->

submitted to the National Police's Directorate of Cyber Crime (Ditipidsiber). Cybercrime can be categorized into 2 (two) areas, namely: 1) Computer-related crime, where the computer is targeted by the perpetrator for any illegal and criminal behavior by processing computer system data in an unauthorized way to commit computer crimes, and 2) Computer-generated crime, where the computer becomes a tool/weapon used by perpetrators for illegal behavior to damage or steal some privacy and system data.¹¹

Sniffing is sniffing data packets on a computer network system, which can monitor and capture all network traffic passing through which the packet is sent. There have been many cases of sniffing by fraudsters making applications in the form of online invitations, which are APK extensions.¹² In their action, the fraudster sends the invitation via WhatsApp, a digital wedding invitation, and directs the victim to attend, so indirectly, the victim opens the application. However, when the victim opened the file, the victim's data, including mobile banking, was successfully retrieved, so the victim lost money in the ATM by sniffing, committing data theft/breaches. Theft of personal data is not something anyone can take lightly. The theft of personal data can cause significant losses to a person or a company. For individuals, losses resulting from theft of personal data, namely the crime of stealing accounts (phishing) targeted or social engineering type of attack.

They are related to criminal acts through sniffing who hacked M Banking via the application Whatsapp, juridically regulated in Law of the Republic of Indonesia Number 1 of 2024 concerning Information and Electronic Transactions (UU ITE) Article 31 paragraph (2), which explains the prohibition on anyone who intentionally intercepts a document or electronic information which results in it being lost, change, and cessation of a document or electronic information. Further provisions, Article 36 of the ITE Law, stipulate that every person is prohibited from intentionally and without rights carrying out acts as referred to in Articles 30 to Article 34, which could result in material loss to other people. If the substance of Article 31 paragraph (2) Amendment to the ITE Law in juncto

Article 36: The Second Amendment to the ITE Law results in material losses for other parties so that they will be punished with a maximum prison sentence of 12 (twelve) years in prison and/or a maximum fine of IDR 12,000,000,000 (twelve billion rupiah); this is regulated in the provisions of Article 51 paragraph (2) of the ITE Law.

¹¹ Arpita Singh et al., "An Algorithm for Crime Detection in Digital Forensics Lakshmaiah Education Foundation," *Journal of Survey in Fisheries Sciences* 10, no. 35 (2023): 2023.

¹² Diana Setiawati, Tyas Permata Dewi, and Zulfiana Ayu Astutik, "Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins," *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang* 7, no. 2 (March 28, 2024): 184–99, <https://doi.org/10.33474/yur.v7i2.21184>.

Law of the Republic of Indonesia Number 27 of 2022 concerning the Protection of Personal Data (from now on referred to as the PDP Law) also regulates criminal acts sniffing, namely Article 65 paragraph (1), which governs that every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him to benefit himself or another person which could result in loss to the Personal Data Subject. Further provisions in Article 67 paragraph (1) of the PDP Law emphasize that every person who intentionally and unlawfully obtains or collects personal data that can harm other parties to benefit themselves or others as intended in Article 65 paragraph (1) of the PDP Law, then he will be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of IDR 5,000,000,000 (five billion rupiah).

If you look carefully, the specific settings are most appropriate for criminal acts, such as sniffing those who hacked M-Banking via the WhatsApp application. There have yet to be any proper comprehensive regulations. However, it is a criminal act if you look at personal data being hacked and causing losses to other parties. Sniffing has relevance to the provisions of Article 31 paragraph (2) Amendment to the ITE Law in conjunction with Article 36 Second Amendment to the ITE Law in conjunction with a criminal penalty under Article 51 paragraph (2) of the ITE Law. Apart from that, it is also relevant to the provisions of Article 65 paragraph (1) of the PDP Law and is punishable by crime under Article 67 paragraph (1) of the PDP Law.

The following legal problem is that the sanctions provisions in Article 51, paragraph (2) of the ITE Law differ from those in Article 67, paragraph (1) of the PDP Law. Article 51, paragraph (2) of the ITE Law confirms a maximum criminal sanction of 12 (twelve) years in prison and/or a maximum fine of IDR 12,000,000,000 (twelve billion rupiah). In comparison, Article 67 paragraph (1) of the PDP Law confirms criminal sanctions imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000 (five billion rupiah). At the same time, in the Criminal Code, several criminal acts of theft of personal data are charged under Article 363 paragraph (1) of the Criminal Code, which is punishable by criminal imprisonment for a maximum of 7 (seven) years.

Differences in sanctions cause overlapping regulations among related legal regulations. Therefore, there is a need for harmony or harmonization between these regulations to overcome and prevent their occurrence.

2. Research Method

This writing uses normative legal research methods, using a conceptual approach (conceptual approach)¹³ and a legislative approach (statute approach)

¹³ Wardah Yuspin and Bima Artha Wijaya, "Legal Protection On Bitcoin Price Manipulation," *RJOAS* 2,

on the issues discussed,¹⁴ namely related to how to harmonize relevant applicable laws and regulations for cybercrime sniffing and what legal protection is provided for by law for customers regarding personal data. The primary legal materials used are the ITE Law and the Personal Data Protection Law, which are secondary legal materials in journals and related articles.¹⁵

3. Results and Discussion

Sniffing

Sniffing is one form of cybercrime that is carried out using the internet network to collect user data illegally.¹⁶ This crime can occur when you are connected to a malicious public network and then carry out the data transfer process from client to user and vice versa. The data transfer process has a back-and-forth data flow from clients and users. That's where sniffing works; they will capture data packets sent using help tools, and after that, sniffing will catch and get stuck on the victim's computer. Then, malicious programs will be inserted to obtain the victim's data. Next, sniffing works on the data segment in layer transport by inserting a malicious program on the victim's computer, where the program will then conduct the sniffing process. As a result, sensitive data on the victim's computer can be read by sniffer.

The way of work is sniffing by tapping into the victim's device via the internet network and then accessing applications that store critical user data, such as username, password mobile banking, information credit card, password e-mail, and other important information. The APK application will automatically be installed on the victim's cellphone after the victim clicks on the digital wedding invitation in APK format. After installation, the APK application will request access to phone data such as SMS, media, etc. In addition, the APK will be able to access SMS and read the OTP code from the bank, which is usually sent via SMS, if this access is ignored. Data such as user ID, approval PIN, password mobile banking, and other transaction information can be accessed by perpetrators. What will happen is that apart from the victim's data potentially

no. 122 (2022): 47–54, <https://doi.org/10.18551/rjoas.2022-02.06>.

¹⁴ Wardah Yuspin et al., *Menggagas Pembentukan Bank Digital Di Indonesia* (Surakarta: Muhammadiyah University Press, 2022).

¹⁵ Heppy Purbasari and Dewita Puspawati, "Exploration Study of Sharia Corporate Exploration Study of Sharia Corporate Governance Disclosure on Bank Annual Governance Disclosure on Bank Annual Report of Sharia Business Unit Report of Sharia Business Unit," *Riset Akuntansi Dan Keuangan Indonesia* 6, no. 1 (2021): 50–61, <http://journals.ums.ac.id/index.php/reaksi/index>.

¹⁶ Hanna Maria Ritonga, Delvi Natalia Br. Ginting, and Anggun Kireina Pandiangan, "Tanggung Jawab Perbankan Terhadap Pembobolan M-Banking Nasabah Akibat Kejahatan Sniffing," *Jurnal Profile Hukum* 2, no. 2 (2024): 194–204.

being stolen, the victim's mobile banking will also be hacked, and can even make separate transfers to unknown parties. The impact of cybercrime is 1) loss of revenue, 2) reputational damage, 3) loss of customers, and 4) regulatory sanctions.¹⁷

Harmonize relevant applicable laws and regulations Cybercrime Sniffing

Regulations regarding customer personal data are closely related to the principle of getting to know your customer. According to Article 1 number 2 of Bank Indonesia Regulation Number 3/10/PBI/2001, which was later amended by Bank Indonesia Regulation Number 5/21/PBI/2003, Principles of Knowing Your Customer, better known as Know Your Customer Principles (KYCP) is a principle applied by banks to find out customer identity, monitor customer transaction activities including transaction reporting which has the principle of getting to know your customer to help protect the reputation and integrity of the banking system by preventing banking from being used as a tool for financial crime. Applying the principle of knowing nasabah (Know Your Customer Principle) is based on the consideration that this principle is essential to protect banks from various risks in dealing with customers.

Based on the provisions and legal basis, namely the ITE Law, several forms of cybercrime exist. The forms of cybercrime are cyber crimes that use information from technology, such as computers, as the primary tool in crime. Such as the spread of pornography, gambling, and pollution via social media and fraud. Likewise, with forgery, extortion, and threats.¹⁸ Don't forget either hoaxes, which are spread through social media, or Cybercrime, which is related to the world of electronic information and is related to computers and networks as the primary target, such as accessing illegal data, disrupting computer systems and their data, and eavesdropping. This usually happens in Indonesia's banking and cyber security systems. All digital technology users have the potential to become victims of cyber attacks.¹⁹

Criminal acts of sniffing by hacking M-Banking have three main characteristics: first, sniffing by committing burglary, and second, M-Banking is done deliberately and planned. This can be proven by the application format (APK)

¹⁷ Victoria Wang, Harrison Nnaji, and Jeyong Jung, "Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability," *International Journal of Law, Crime and Justice* 62, no. September 2018 (2020): 100415, <https://doi.org/10.1016/j.ijlcj.2020.100415>.

¹⁸ Delvyan Putri Surya Ningrum and Jamiatur Robekha, "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia."

¹⁹ Steve Schlackman, "WHO HOLDS THE COPYRIGHT IN AI CREATED ART," *Art Journal*, 2020, <https://artpreneur.com/journal/the-next-rembrandt-who-holds-the-copyright-in-computer-generated-art/>.

used to hack M-banking.²⁰ By preparing to use the application format (APK), which is used as a means of hacking into M-Banking, it can be ensured that the action sniffing by hacking M-Banking is a deliberate and planned act. Hence, it is impossible to act sniffing carried out due to negligence or carelessness. Second, criminal acts in the form of sniffing by committing burglary M-Banking. It may not be possible to determine the target victims precisely. Still, it is also possible that there may be targets for specific victims. This is possible because the main orientation of criminal acts is sniffing on the victim's data, which is then used to break into M-Banking balances.²¹ This means a criminal act in the form of sniffing can be planned to target certain victims or imposed on victims randomly. Third, criminals act in the form of sniffing Substantially; this is an action whose orientation is on "utilizing the victim's data" so that the personal data is followed by hacking into M-Banking. This also shows that criminal acts include sniffing, a criminal offense related to personal data. Of the three characteristics of criminal acts, they are sniffing by committing burglary, M-Banking above, it can be concluded that substantively a criminal act takes the form of sniffing is a criminal offense with the main focus being.²²

Using the victim's data to hack the victim's M Banking further results in profits for the perpetrator. In general, illegality is an action carried out by someone intentionally and without authorization to access all or part of a computer system. Arrangement of illegal access includes violations of computer systems and data security (integrity, availability, and confidentiality), such as hacking, cracking, or computer trespass. The legislators divided the regulation of illegal access into three parts. The acts regulated are intentional and without authority or against the law, such as Accessing a computer or electronic system in any way, accessing a computer or electronic system in any way to obtain electronic information and/or electronic documents, and accessing a computer or electronic system in any way by violating, by passing, or breaching security systems.²³

Legal problems regarding criminal acts in the form of sniffing regulated in the ITE Law and its amendments and the PDP Law, namely that there are differences in the sanctions provisions in Article 51 paragraph (2) of the ITE Law, which are

²⁰ Benjamin A. Morrison, Lynne Coventry, and Pam Briggs, "Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults," *Frontiers in Psychology* 11, no. April (2020): 1–13, <https://doi.org/10.3389/fpsyg.2020.00623>.

²¹ Jerico Mathias and Rosamine Blessica, "Hate Speech and the Freedom Discourse," *Indonesia Media Law Review* 1, no. 1 (January 31, 2022): 1–22, <https://doi.org/10.15294/imrev.v1i1.56673>.

²² Tsania Aziziyah, Purwoleksono Didik Endro, and Taufik Rachman, "Sniffing Cybercrime Di M-Banking via WhatsApp: Kerangka Hukum Komparatif Dan Implikasinya," *Indonesian Journal of Innovation Studies* 13, no. 2 (2023): 1–12.

²³ Purnomo, "Kebijakan Hukum Terhadap Kejahatan Cybercrime Di Era Informasi Dan Masyarakat Virtual," *Palimpsest* 9, no. 2 (2002): 77–83.

different from the sanctions provisions in Article 67 paragraph (1) of the PDP Law. Article 51, paragraph (2) of the ITE Law confirms a maximum criminal sanction of 12 (twelve) years in prison and/or a maximum fine of IDR 12,000,000,000 (twelve billion rupiah). In comparison, Article 67 paragraph (1) of the PDP Law confirms criminal sanctions maximum imprisonment of 5 (five) years and/or a maximum fine of IDR 5,000,000,000 (five billion rupiah).

Legal problems regarding differences in sanctions in the ITE Law and its amendments and the PDP Law can be resolved juridically in two ways, namely through the principle of preference and through teleological/sociological interpretation. Refers to the principle of preference, namely the principle of a special law derogating from a general law, which emphasizes that a specific law can override a general law. In this case, Article 67 paragraph (1) of the PDP Law applies to criminal acts such as sniffing and hacking M-Banking via WhatsApp. This is because the PDP Law regulates criminal acts relating to personal data, which can expressly exclude cyber crimes in general as regulated by the ITE Law and its amendments.

Referring to the teleological/sociological interpretation by looking at the purpose of the law, it can be seen that the PDP Law was designed to enforce the law for criminal acts related to personal data. This differs from the provisions in the ITE Law and its amendments, which generally focus on regulating cyber crimes. Therefore, because it refers to the principle of preference, namely the principle of *lex specialis derogate legigeneralis*, and based on teleological/sociological interpretation by looking at the purpose of establishing the law, it can be concluded that in cases of criminal acts in the form of sniffing. In hacking M-Banking via the Whatsapp application, what applies is the provisions of Article 67 paragraph (1) of the PDP Law.

Crime setting sniffing in hacking M-Banking via the Whatsapp application, which has been regulated in the ITE Law and its amendments, and the PDP Law has differences in the aspect of sanctions where the sanctions in the ITE Law and its amendments are more severe than the sanctions contained in the PDP Law. Refers to the principle of preference, namely the principle a special law derogating from the general law and based on teleological/sociological interpretation by looking at the purpose of establishing the law, it can be concluded that in cases of criminal acts in the form of sniffing In hacking M-Banking via the WhatsApp application, what applies is the provisions of Article 67 paragraph (1) of the PDP Law, with the threat of imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000 (five billion rupiah), because the PDP Law regulates personal data violations, which can eliminate or exclude cyber violations regulated by the ITE Law and its amendments.

Protection provided by law to deal with cases of sniffing

Sniffing In fact, it is a form of a criminal act that is categorized as cybercrime in the form of wiretapping and taking information or data carried out against the law by utilizing the internet network.²⁴ The main characteristics of sniffing passively are not having sure signs, so often there is no suspicion, or the victim becomes unaware of the action of sniffing the passivity he experienced. Action sniffing passively utilizes a hub device that primarily spreads signals to all clients. Of the two types of action, sniffing generally harms the victim. These losses can be in the form of financial or non-financial losses. One of the massive acts of sniffing that occur in society is through specific application files (APK format), which are opened via WhatsApp, automatically steal personal data, and even hack, depleting the M-Banking balance.²⁵ Sniffing Active is an action aiming to change the substance of existing data. Sniffing Actively runs on the network switch and not on the device itself. Sniffing Passive is an action in the form of intercepting data that utilizes data transfer between the server and client back and forth, where the result of this action is that the substance of the existing data does not change.²⁶

Personal data is any information related to an identifiable person, in English, known as personally identifiable information or abbreviated as PII. The abbreviation is widely known in the United States. According to the National Institute of Standards and Technology, personal data is any information about an individual maintained by an institution, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date, and place of birth, mother's maiden name, or biometric records.²⁷ Personal data is other information related to individuals, such as medical, educational, financial, and employment. Meanwhile, according to the European Union Data Protection Regulation or GDPR, personal data is any information that is connected or can be connected to a person.²⁸

²⁴ Steven Kemp et al., "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19," *Journal of Contemporary Criminal Justice* 37, no. 4 (November 18, 2021): 480–501, <https://doi.org/10.1177/10439862211027986>.

²⁵ Muhammad Isnaeni Puspito Adhi and Eko Soponyono, "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law," *Law Reform: Jurnal Pembaharuan Hukum* 17, no. 2 (September 30, 2021): 135–44, <https://doi.org/10.14710/lr.v17i2.41736>.

²⁶ Aryono and Jaco Barkhuizen, "Criminal Law Enforcement of Phishing Attacks on Online Banking Services," in *International Conference Health, Science And Technology (ICOHETECH)*, 2021, 360–63, <http://ojs.uib.ac.id/index.php/icohetech/article/view/1160>.

²⁷ Amelia Mays, "Protection of Personal Data in the Care Application," *Journal of International Trade, Logistics and Law* 8, no. 1 (2022): 23–27.

²⁸ Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer, and Mulatu Fekadu Zerihun, "Analysis of Cyber-Crime Effects on the Banking Sector Using the Balanced Score Card: A Survey of Literature," *Journal of Financial Crime* 27, no. 3 (June 16, 2020): 945–58, <https://doi.org/10.1108/JFC-03-2020-0037>.

Everyone has the right to privacy regarding their data, and all countries have regulations regarding personal data protection, including Indonesia. The primary purpose of the mode sniffing is to steal data and information from the cellphone he hacked. The stolen data is in the form of username, password, email, and other data. According to Article 3 of the Personal Data Protection Bill, the types of personal data include Personal Data of a general nature and specific Personal Data. Meanwhile, general Personal Data as intended in paragraph (1) letter a includes:

- a. full name;
- b. gender;
- c. citizenship;
- d. religion; and/or
- e. personal data combined to identify an individual. Specific Personal Data as intended in paragraph (1) letter b includes:

- a. health data and information;
- b. biometric data;
- c. data genetics;
- d. sexual life/orientation;
- e. political views;criminal record;
- f. child data;
- g. personal financial data; and/or

h. Other data follows the provisions of statutory regulations. The Indonesian government has implemented the PDP Law to protect the personal data of Indonesian citizens. Article 1 Paragraph 1 of the PDP Law defines personal data as data about natural persons who are identified or can be identified individually or in combination with other information directly or indirectly through electronic systems or non-electronic.

Efforts to protect personal data generally are separate from how the principles of personal data protection are fulfilled and implemented in processing personal data. Personal data processing consists of collecting, processing, and deleting personal data. Referring to the provisions of Article 67 paragraph (1) of the PDP

Law, the bank must also provide true legal responsibility if there is a loss resulting from action and sniffing in the M-Banking hack, which had implications for harming the victim. However, the provisions in Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking (from now on referred to as the Banking Amendment Law), especially in Article 37 B paragraph (1), which confirms that the bank must guarantee and protect It is felt that the funds that the public has deposited are not sufficient to ensure legal accountability by the bank if a criminal act occurs sniffing who carried out the M-Banking hack.

The provisions of Article 37B paragraph (1) of the Banking Amendment Law only emphasize banks' obligation to safeguard funds from the public without any legal consequences.

What if the bank needs to be more optimal or make mistakes in safeguarding funds from the public? Accountability carried out by banks is mandatory for Sharia banks. This is confirmed in Article 39 of Law Number 21 of 2008 concerning Sharia Banking (after this referred to as the Sharia Banking Law), which is substantively similar to the formulation of Article 29 paragraph (4) of the Banking Amendment Law, which states that Sharia banks are obliged to provide information on potential losses and experienced by customers. Similar to banking practices in general, in Sharia banking, the banks also often miss out and do not provide information regarding criminal acts in the form of sniffing who carried out the M Banking burglary and its countermeasures.

In cases involving criminal acts in the form of sniffing who committed the M-Banking hack, it is clear that the fault is not with the customer, so the argument, on the contrary, is used that Islamic banks must be legally responsible for losses to victims as a result of criminal acts in the form of sniffing who committed the burglary M-Banking. Therefore, both conventional and Islamic banks must be responsible for victims due to losses caused by victims of criminal acts in the form of sniffing who committed the burglary. M-Banking is a form of liability that can be reimbursed for all or part of the nominal balance of M-Banking or other forms of liability.²⁹

Looking at the definition of personal data protection in the PDP Law, according to Philipus M Hadjon, we can see whether the implementation of the PDP Law has provided legal protection to personal data owners, especially banking customers. According to Philipus, the theory of legal protection is divided into two parts: preventive legal protection and repressive legal protection. Preventive protection is regulated in Article 65, paragraph (3) of the PDP Law. This means

²⁹ Dewoto Kusumo and Rifki Afandi, "Sniffing Cybercrimes in M-Banking via WhatsApp: Comparative Legal Framework and Implications," *Indonesian Journal of Innovation Studies* 13, no. 2 (2020): 1–12.

that the provisions regarding personal data protection are also ultimately binding to any trade that utilizes an electronic system. Administrative sanctions are sanctioned against violating the obligation to provide complete and correct information. According to the author, the government gives preventive legal protection to prevent breaches. This preventive guarantee is contained in the law. Security premise individual information as one type of security for personal information is regulated in Article 28 G paragraph (1) of the Constitution of the Republic of Indonesia 1945, which the PDP Law also regulates.³⁰

Repressive legal protection is legal protection to resolve things disputes. Repressive protection in case sniffing this doesn't seem right One effort that can be made to strengthen the legal framework for personal data protection is to create a protection system that applies principles that uphold the protection of user privacy at both regulatory and technical levels. This principle is used in building every online service system and will prevent the possibility of transferring control of personal data to the system. This principle has been implemented in European Union countries in their personal data protection regulations known as GDPR (General Data Protection Regulation).

4. Conclusion

Based on the results and discussion described by the author, it can be concluded that Sniffing is one form of cybercrime that uses the internet network to collect user data illegally. Legal problems regarding differences in sanctions in the ITE Law and its amendments and the PDP Law can be resolved juridically in two ways, namely through the principle of preference and through teleological/sociological interpretation. To achieve harmonization in regulations, crime regulation sniffing in hacking M-Banking via the WhatsApp application, which has been regulated in Article 51 paragraph (2) of the ITE Law and its amendments and Article 67 paragraph (1) of the PDP Law has differences in the aspect of criminal sanctions and/or fines, which are the sanctions in the ITE Law and its amendments heavier than the sanctions contained in the PDP Law. Refers to the principle of preference, namely the principle a special law derogating from the general law and based on teleological/sociological interpretation by looking at the purpose of establishing the law, it can be concluded that in cases of criminal acts in the form of sniffing In the M-Banking hack via the Whatsapp application, because it relates to personal data breaches, what applies is the provisions of Article 67 paragraph (1) of the PDP Law, because the PDP Law is a regulation that more specifically regulates personal

³⁰ Mirnayanti Mirna, Judhariksawan, and Maskum, "Analisis Pengaturan Keamanan Data Pribadi Di Indonesia," *Jurnal Ilmiah Living Law* 15, no. 1 (January 31, 2023): 16–30, <https://doi.org/10.30997/jill.v15i1.4726>.

data breaches, so the ITE Law and its amendments as a more general arrangement should be ruled out. The protection provided by law for handling cases sniffing M-Banking hacking via the WhatsApp application is regulated by criminal sanctions in Article 67 paragraph (1) of the PDP Law, which can be interpreted to mean that the PDP Law provides criminal sanctions and/or fines to all parties, including banks if there is loss resulting from these actions. Sniffing has implications for harming the victim.

References

- Adhi, Muhammad Isnaeni Puspito, and Eko Soponyono. "Crime Combating Policy of Carding in Indonesia in the Political Perspective of Criminal Law." *Law Reform: Jurnal Pembaharuan Hukum* 17, no. 2 (September 30, 2021): 135–44. <https://doi.org/10.14710/lr.v17i2.41736>.
- Akinbowale, Oluwatoyin Esther, Heinz Eckart Klingelhöfer, and Mulatu Fekadu Zerihun. "Analysis of Cyber-Crime Effects on the Banking Sector Using the Balanced Score Card: A Survey of Literature." *Journal of Financial Crime* 27, no. 3 (June 16, 2020): 945–58. <https://doi.org/10.1108/JFC-03-2020-0037>.
- Aryono, and Jaco Barkhuizen. "Criminal Law Enforcement of Phising Attacks on Online Banking Services." In *International Conference Health, Science And Technology (ICOHETECH)*, 360–63, 2021. <http://ojs.udb.ac.id/index.php/icohetech/article/view/1160>.
- Aziziyah, Tsania, Purwoleksono Didik Endro, and Taufik Rachman. "Sniffing Cybercrime Di M-Banking via WhatsApp: Kerangka Hukum Komparatif Dan Implikasinya." *Indonesian Journal of Innovation Studies* 13, no. 2 (2023): 1–12.
- Buil-Gil, David, Yongyu Zeng, and Steven Kemp. "Offline Crime Bounces Back to Pre-COVID Levels, Cyber Stays High: Interrupted Time-Series Analysis in Northern Ireland." *Crime Science* 10, no. 1 (2021): 1–16. <https://doi.org/10.1186/s40163-021-00162-9>.
- Delvyan Putri Surya Ningrum, and Jamiatur Robekha. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia." *PESHUM : Jurnal Pendidikan, Sosial Dan Humaniora* 2, no. 4 (2023): 765–76. <https://doi.org/10.56799/peshum.v2i4.2115>.
- Dwi Letari, Wuryaningsih, Damatika Purnama Suci, and Muhammad Sholahuddin. "Beberapa Faktor Yang Mempengaruhi Profitabilitas Perbankan Di Indonesia." *Benefit: Jurnal Manajemen Dan Bisnis* 5, no. 1 (2020): 1–19. <https://journals.ums.ac.id/index.php/benefit/index>.
- Horan, Cecelia, and Hossein Saiedian. "Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions." *Journal of Cybersecurity and Privacy* 1, no. 4 (September 30, 2021): 580–96. <https://doi.org/10.3390/jcp1040029>.
- Kemp, Steven, David Buil-Gil, Asier Moneva, Fernando Miró-Llinares, and Nacho Díaz-Castaño. "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19." *Journal of Contemporary Criminal Justice* 37, no. 4 (November 18, 2021): 480–501. <https://doi.org/10.1177/10439862211027986>.
- Kusumo, Dewoto, and Rifki Afandi. "Sniffing Cybercrimes in M-Banking via WhatsApp: Comparative Legal Framework and Implications." *Indonesian Journal of Innovation Studies* 13, no. 2 (2020): 1–12.
- Mathias, Jerico, and Rosamine Blessica. "Hate Speech and the Freedom Discourse." *Indonesia Media Law Review* 1, no. 1 (January 31, 2022): 1–22. <https://doi.org/10.15294/imrev.v1i1.56673>.

- Mays, Amelia. "Protection of Personal Data in the Care Application." *Journal of International Trade, Logistics and Law* 8, no. 1 (2022): 23–27.
- Mirna, Mirnayanti, Judhariksawan, and Maskum. "Analisis Pengaturan Keamanan Data Pribadi Di Indonesia." *Jurnal Ilmiah Living Law* 15, no. 1 (January 31, 2023): 16–30. <https://doi.org/10.30997/jill.v15i1.4726>.
- Morrison, Benjamin A., Lynne Coventry, and Pam Briggs. "Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults." *Frontiers in Psychology* 11, no. April (2020): 1–13. <https://doi.org/10.3389/fpsyg.2020.00623>.
- O'Shea, Brianna, Nicole L. Asquith, and Jeremy Prichard. "Mapping Cyber-Enabled Crime: Understanding Police Investigations and Prosecutions of Cyberstalking." *International Journal for Crime, Justice and Social Democracy* 10, no. 4 (February 21, 2021): 25–39. <https://doi.org/10.5204/IJCJSD.2096>.
- Pântea, A. "Cyber Security and Impact on Computer Crimes." *Acta Universitatis Danubius. Juridica* 12, no. 1 (2023): 348–57. <https://www.ceeol.com/search/article-detail?id=1180778>.
- Purbasari, Heppy, and Dewita Puspawati. "Exploration Study of Sharia Corporate Governance Disclosure on Bank Annual Report of Sharia Business Unit Report of Sharia Business Unit." *Riset Akuntansi Dan Keuangan Indonesia* 6, no. 1 (2021): 50–61. <http://journals.ums.ac.id/index.php/reaksi/index>.
- Purnomo. "Kebijakan Hukum Terhadap Kejahatan Cybercrime Di Era Informasi Dan Masyarakat Virtual." *Palimpsest* 9, no. 2 (2002): 77–83.
- Rahmah, Yuslia Naili. "Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah 'Istimewa Yogyakarta.'" *Jurnal Pendidikan Ekonomi* 7, no. 6 (2018): 579–88. <https://proxsisgroup.com/articles/waspadailah-hantaman-serangan-cyber-terhadap->
- Ritonga, Hanna Maria, Delvi Natalia Br. Ginting, and Anggun Kireina Pandiangan. "Tanggung Jawab Perbankan Terhadap Pembobolan M-Banking Nasabah Akibat Kejahatan Sniffing." *Jurnal Profile Hukum* 2, no. 2 (2024): 194–204.
- Saifullah, Rana, and Sayeda Sassi Roshan Shah. "Transnational Law and Criminal Justice System: Highlighting Legislative and Procedural Challenges to Combat Cyber Crime in the Wake of CPEC." *JISR Management and Social Sciences & Economics* 21, no. 4 (December 30, 2023): 73–92. <https://doi.org/10.31384/jisrmse/2023.21.4.5>.
- Schlackman, Steve. "WHO HOLDS THE COPYRIGHT IN AI CREATED ART." *Art Journal*, 2020. <https://artpreneur.com/journal/the-next-rembrandt-who-holds-the-copyright-in-computer-generated-art/>.
- Setiawati, Diana, Tyas Permata Dewi, and Zulfiana Ayu Astutik. "Personal Data Protection Vulnerabilities In Cybercrime Sniffing Bank Account Break-Ins." *Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang* 7, no. 2 (March 28, 2024): 184–99. <https://doi.org/10.33474/yur.v7i2.21184>.
- Singh, Arpita, S K Singh, Nilu Singh, and Sandeep K Nayak. "An Algorithm for Crime Detection in Digital Forensics Lakshmaiah Education Foundation." *Journal of Survey in Fisheries Sciences* 10, no. 3S (2023): 2023.
- Sukoco, Bambang. "Pendekatan Restoratif Justice Sebagai Upaya Penyelesaian Cybercrime Dengan Pelaku Anak (Studi Kasus Penyelesaian Tindak Pidana Anak Usia Sekolah)." *Jurnal Law and Justice* 1, no. 1 (2016): 54–64. <https://doi.org/https://doi.org/10.23917/laj.v1i1.2859>.
- Venter, Isabella M., Rénette J. Blignaut, Karen Renaud, and M. Anja Venter. "Cyber Security Education Is as Essential as 'the Three R's.'" *Heliyon* 5, no. 12 (2019): 0–7. <https://doi.org/10.1016/j.heliyon.2019.e02855>.

- Wang, Victoria, Harrison Nnaji, and Jeyong Jung. "Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability." *International Journal of Law, Crime and Justice* 62, no. September 2018 (2020): 100415.
<https://doi.org/10.1016/j.ijlcj.2020.100415>.
- Yuspin, Wardah, Kelik Wardiono, Anindhita Nurfaatin Sukirman, and Aditya Nurrahman. *Menggagas Pembentukan Bank Digital Di Indonesia*. Surakarta: Muhammadiyah Universty Press, 2022.
- Yuspin, Wardah, and Bima Artha Wijaya. "Legal Protection On Bitcoin Price Manipulation." *RJOAS* 2, no. 122 (2022): 47-54.
<https://doi.org/10.18551/rjoas.2022-02.06>.