Identity Theft and Personal Data Protection in Indonesian Criminal Law

Said Noor Prasetyo [1*] Cindy Monique [2]

[1] *Faculty of Law, Universitas Muhammadiyah Malang, Malang, Indonesia*
[2] *Master of Law, Universitas Brawijaya, Malang, Indonesia*
[*] *Corresponding author. Email: saidnoor@umm.ac.id*

ABSTRACT
In the digital era, identity is very important to protect because it is a representation of a person in an electronic system. Along with the development of information technology, this type of crime is also developing along with the emergence of cybercrime. One type of cybercrime that threatens a person's identity is identity theft. Identity theft is a new type of crime. However, the impact of this crime has had a massive impact, especially in the banking sector. Basically, Identity Theft does not have a direct impact, because the victim does not lose anything. New losses will be felt when personal data is used to commit crimes. This crime always haunts us when surfing in cyberspace. Many criminals target identity as the key to accessing someone's accounts such as bank accounts, credit cards, and other accounts. This crime is a serious threat in the digital era, especially in Indonesia. This is caused by a lack of awareness among citizens in protecting their identity and the existence of inadequate laws in providing protection. This situation certainly poses a threat to strengthening civil society in the digital era.
Keywords: *identity theft, cybercrime, data protection*

1. INTRODUCTION

According to the Big Indonesian Dictionary, Identity is the characteristics or special condition of a person or a person's identity. (Kamus Besar Bahasa Indonesia, n.d.)From this understanding, it can be understood that Identity is a distinguishing feature of a person. In the context of the Personal Data Protection Law (PDP Law), the term Identity has the same meaning as personal data. According to the PDP Law, Personal Data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. In Article 4 of the PDP Law, personal data is divided into 2, namely Specific and General Personal Data. Included in general personal data are full name, gender, nationality, religion, marital status, and/or those combined to identify a person. Specific Personal Data includes health data and information, biometric data, genetic data, criminal records, children's data, personal financial data, and other data in accordance with the provisions of laws and regulations.

Nowadays, online financial transactions (E-Commerce) have become a popular transaction medium in Indonesia. The Ministry of Trade of the Republic of Indonesia (Kemendag RI) estimates the value of Digital Trade Transactions (E-Commerce) to reach IDR 533 Trillion by 2023 (Kementerian Perdagangan Republik Indonesia, 2024). However, this popularity is not accompanied by awareness of user security and privacy. This negligence is exploited by cyber criminals to obtain user data for their criminal activities. (Syahbana, n.d.) An example that occurred in 2023 was a data leak case involving Bank Syariah Indonesia (BSI) customers. Before the data was leaked, there were complaints of transaction service disruptions on 8 May 2023. Lockbit claims that the attack on BSI has stolen 1.5 TB of personal data in this data theft case. Lockbit had negotiated with BSI and asked for a ransom of IDR 296 billion. Because it was not redeemed, Lockbit distributed the data on the black market on 16 May 2023. (Febriari, n.d.).

The combination of user negligence and increasing online transaction activity has made Indonesia an easy target for cybercriminals. Statistics from the National Cyber and Crypto Agency (BSSN) show that there will be 370.02 million cyberattacks against Indonesia in 2022. Compared to the previous year (266.74 million cyberattacks), this number increased by 38.72%. The government administration sector is the main target of cyberattacks in Indonesia with 284.09

S. Al Fatih et al. (eds.), *Proceedings of the International Conference on Law Reform (5th Inclar 2024)*, Advances in Social Science, Education and Humanities Research 870,
https://doi.org/10.2991/978-2-38476-362-7_14

million attacks. (BPPTIK, 2024). Of course, there are many direct and indirect impacts caused by this threat, especially on financial transactions. The attack in question is commonly referred to as Identity Theft.

Identity theft is a new type of crime. Even so, the impact of this crime has a massive impact, especially in the banking sector. Basically, Identity Theft has no direct impact, because the victim does not lose anything. The loss will only be felt when the personal data is used to commit a crime. Departing from this, it can be understood that Identity Theft is a preliminary act as a means to commit a crime that can cause enormous financial losses. (Prasetyo, 2016)

There is a question that may be on everyone's mind. Is personal data security part of human rights that must be protected by the state? Referring to the opinion of Mutiara & Maulana quoted by Rosihan Lutfi that based on the Constitutional Court Decision No.5/PUU-VIII/2011, the right to privacy is part of human rights (derogable rights) which is part of information or the right to information privacy, also called data privacy (data protection). (Lutfi, 2022) More clearly, UU PDP Article 1 point 2 defines Personal Data Protection as the overall effort to protect Personal Data in the series of Personal Data processing in order to guarantee the constitutional rights of Personal Data subjects. Based on this description, we can understand that the protection of personal data is a constitutional right of every citizen that must be provided by the state.

Many countries, especially developed countries, have criminalized this act considering the magnitude of the losses that can be caused by this crime. In 2022, Law No. 27 of 2022 on Personal Data Protection was born. This is a breath of fresh air in criminal law enforcement, especially against cybercrime. Based on the background as described above, the question arises how is the protection of personal data in Indonesian criminal law after the emergence of the law?

I. Scope of Personal Data and Form of Personal Data Protection

Referring to Article 1 of the PDP Law, Personal Data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. Furthermore, Article 4 of this law divides Personal Data into 2, namely specific Personal Data and general Personal Data. Specific personal data includes health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and/or other data in accordance with the provisions of laws and regulations. General personal data includes full name, gender, nationality, religion, marital status, and/or personal data combined to identify a person. Looking at what is included in personal data, both specific and general, we can see the importance of protection of personal data security. For this reason, the protection of the security of personal data is the right of the subject of personal data.

Many things are included in personal data where each personal data requires protection of its confidentiality. Data confidentiality is the right of personal data subjects that must be protected. For this reason, the government regulates a comprehensive personal data management mechanism. In order to ensure the implementation of management that is able to guarantee the security of personal data, the law provides several rights to personal data subjects, including:

a. Right to access: The right to obtain confirmation as to whether or not the personal data concerned is being processed, as well as the right to access such data.
b. Right to rectification: The right to correct inaccurate personal data.
c. Right to erasure: The right to delete personal data under certain circumstances
d. Right to restriction of processing: The right to restrict processing of personal data in certain circumstances
e. Right to data portability: The right to receive personal data in a structured, commonly used and machine-readable format.
f. Right to object: The right to object to the processing of personal data under certain circumstances

In order to guarantee protection in the process of managing personal data, the PDP Law applies several principles that are used as a basis:

a. Principle of Protection
   Every processing of Personal Data is carried out by providing protection to the Personal Data Subject for his/her Personal Data and the Personal Data from being misused.
b. Principle of Legal Certainty
   Every Personal Data processing is conducted based on a legal basis to realize Personal Data Protection and everything that supports it so as to obtain legal recognition inside and outside the court.

Principle of Legal Interest

In the Protection of Personal Data, the public interest or the community at large must be considered. Such public interests include the interests of state administration and national defence and security.

Principle of Benefit

Regulation of Personal Data Protection must be beneficial to the national interest, particularly in realizing the ideals of general welfare.

Principle of Prudence

The parties related to the processing and supervision of Personal Data must pay attention to all aspects that have the potential to cause harm.

Principle of Balance

As an effort of Personal Data Protection to balance the right to Personal Data on the one hand with the legitimate state rights based on public interest.

Principle of Responsibility

All parties related to the processing and control of Personal Data shall act responsibly so as to ensure the balance of rights and obligations of the parties concerned, including the Personal Data Subject.

Principle of Confidentiality

Personal Data is protected from unauthorized parties and/or from unauthorized Personal Data processing activities.

Law No. 27 of 2022 on Personal Data Protection takes a comprehensive approach to data protection in Indonesia by providing clear guidelines and strict protections. By aligning with international standards, the PDP Law not only enhances the protection of individual privacy, but also public trust and confidence in the already thriving digital economy.

The biggest challenge in ensuring the protection of personal data is the unlawful theft and misuse of personal data by irresponsible parties. These illegal efforts are commonly referred to as Identity Theft. To anticipate this threat, the PDP Law regulates the prohibition of such irresponsible actions.

Definition of Identity Theft

The Canadian Privacy Commissioner as quoted by Prasetyo said that personal data theft is the unlawful collection and use of personal data intended to commit a crime. The Department of the Solicitor General of Canada and the United States Department of Justice, convey the same thing that Identity theft is the act of taking and using other people's personal data unlawfully for financial gain.(Prasetyo et al., 2019) Jonathan Clough in his book Principles of Cybercrime he explains that identity theft is the act of taking over and sending other people's personal data unlawfully. This crime is a preparatory crime, which criminalizes the unlawful misuse of another person's personal data. In relation to the criminalisation, it does not matter whether the personal data is ultimately used to commit a crime or not.(Jonathan, 2010) Based on Clough's opinion, identity theft is a preparatory crime. The object of this criminal offence is other people's personal data, both general and specific. It is called a preparatory criminal offence because the ultimate goal of this crime is not personal data, the main goal of the perpetrator is to gain financial benefits.

Referring to the provisions of the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft and Assumption Deterrence Act of 1998, 1998) of the United States of America, an act that is classified as Identity Theft is the act of unlawfully sending or using another person's personal data intended to commit a crime.

Construction of Acts in Identity Theft

The author has stated above that the term ‘identity theft’ is understood in a broad sense, namely any act aimed at collecting or obtaining personal data of another person and using it unlawfully. Personal data can be obtained from various sources using various methods. The methods used are constantly evolving. Starting from conventional methods to sophisticated methods using information technology and a combination of both. The following are the usual modes used by identity theft perpetrators:(Prasetyo et al., 2019)

Theft of wallets, smartphone, computers and other sources of personal data

Wallets, smartphone, computers and other storage sources are where credit cards, debit cards, cheques, driver's licenses, account information, social insurance numbers and other personal data are stored. Most people have credit cards, especially debit cards. They will usually keep their credit card/debit card in their wallet. In electronic devices (smartphone and computers), personal data is usually stored. By taking the wallet and electronic devices, the perpetrator will get credit cards, debit cards, ID cards, driving licenses, and other identity cards stored in the wallet. The perpetrator can also take the

personal data of the electronic device user from the device storage device. Personal data that has been controlled by the perpetrator, will be used by the perpetrator to carry out other actions to obtain personal gain unlawfully which will harm the owner of the personal data.

b. Taking electronic data/information stored in an electronic device storage device.

With the development of information technology as it is today, it is very possible for someone to use their smartphone or laptop to transact, both in e-commerce and e-banking. Therefore, the user's personal data will be stored in the device they use. The storage of personal data in the electronic device attracts criminals to enter (browse) the electronic system and take it without the knowledge of the owner of the electronic device. These efforts can be done conventionally (by repairing the device) or using the internet network or commonly known as hacking. In this way, the perpetrator can control the victim's personal data.

c. *Skimming (magnetic strip duplication)*

On one side of the credit/debit card, there is a magnetic tape that is used as a storage place for the personal data of the credit/debit card holder. This data can be read by a skimmer embedded in an EDC (Electronic Data Capture) machine. EDC is a machine used to process electronic transactions. By using the skimmer, the perpetrator can copy and store the personal data of the credit/debit card holder stored on the magnetic tape of the credit/debit card. A skimmer is a device to record/retrieve (or read, pen) the data of a card. The way this tool works is by copying the data contained in the card's magnetic tape when swiped on the tool. (Vyctoria, 2013) So, skimming is a person's attempt to copy the data / information contained on the magnetic tape of a card, whether a debit card, credit card or other card using a skimmer tool. The cardholder's personal data can be installed on another card (fake card) so that it can be used by the perpetrator as a means of payment without authorization so that it will harm the actual cardholder.

d. Mail theft

Mail is an excellent source of personal data, such as bank notification letters about credit/debit cards, driving licenses, credit card application forms, and so on. These will provide details of personal data, such as bank name, account number, credit card number, CVV code, debit card PIN, and so on. Theft of this mail is an easy way to obtain personal data. Based on a CALPIRG survey of American law enforcement officers, 68% of the officers surveyed recognized mail theft as a major concern related to identity theft. (Parkes, 2013) The personal data can be misused by the perpetrators for personal gain unlawfully.

e. Insider theft

Insider theft is the theft committed by individuals who work at institutions managing personal data, such as banks or financial service providers, mobile network providers, population offices, and others. Employees working in institutions managing personal data have a significant opportunity to steal personal data. These individuals have direct access to the personal data and can easily copy any personal data they desire. This opportunity increases if the institution's monitoring is lax. The copied personal data can be sold on the black market or used illegally.

f. Purchasing stolen personal

Purchasing stolen personal data is the easiest way to obtain personal data without arousing suspicion. The personal data in question is stolen data. This data is usually available on the "dark market" network, an underground network trading in personal data, including credit card information.

g. Social engineering

Social engineering is an attempt to obtain personal data through deception by exploiting human weaknesses, making them trust others easily (Vyctoria, 2013). According to McQuade, social engineering involves manipulating or deceiving someone or multiple people to provide personal or financial data or information related to security, or to give access to storage of such personal or financial data. (McQuade, 2009)

h. Phising or pharming

Phishing is internet-based fraud that involves sending spam emails to trick recipients into voluntarily providing their personal data. (Syahdeini, 2009) *These emails are fake but appear legitimate, making the victim believe and willingly provide their personal data*. (Schell & Martin, 2006) This method relies on the victim's lack of knowledge in identifying the authenticity of the email content. (Kevin Wang & Huang, 2024)

Pharming is an attempt to direct victims to fake websites by poisoning DNS with fake IP addresses. Pharming is similar to phishing, but more sophisticated. The link appears genuine, and even a thorough examination of the URL won't reveal suspicious elements because the IP address in the DNS has changed. (Parsons & Oja, 2013) Victims won't suspect anything as the site appears identical to the original. Pharming, like phishing, aims to deceive victims into believing the

fake site is real and ultimately leads them to enter their personal data. Once the victim submits their personal data, it is then controlled by the perpetrator.

i. Man in the middle attack/interception

Man in the middle attack involves an attacker intercepting data and responding, making it seem like the response comes from the intended recipient. A victim may unknowingly provide personal data that can be used for fraud. (Schell & Martin, 2006) Technically, this attack is eavesdropping, where the attacker intercepts the data transmission path between two or more parties without permission or knowledge. In this position, the attacker can record every transmitted data, including personal data. Once the personal data is obtained, the attacker can use it for transactions, causing losses to the victim.

Referring to the description of identity theft methods commonly used by perpetrators above, it can be understood that the construction of identity theft is an intentional act by an individual to obtain/collect (by any means) another person's personal data without permission (illegally) and/or use that personal data for personal gain illegally, causing harm to others. This construction involves two actions: first, the perpetrator intentionally obtains/collects (by any means) another person's personal data without permission (illegally). Second, the individual uses another person's personal data for personal gain illegally, causing harm to others.

The Personal Data Protection Act (PDP Act) is considered comprehensive and complete in providing personal data protection. This law sets strict guidelines for personal data management, including rights and obligations of all parties related to personal data, and prohibits actions that may threaten personal data security, commonly known as identity theft. Referring to the construction of identity theft as described above, the act fulfils the criteria prohibited under the PDP Act, specifically articles 65 paragraphs (1) to (3), as follows:

(1) Any person is prohibited from illegally obtaining or collecting personal data not belonging to them with the intent to benefit themselves or others, potentially causing harm to the personal data subject.
(2) Any person is prohibited from illegally disclosing personal data not belonging to them.
(3) Any person is prohibited from illegally using personal data not belonging to them.

IV. Conclusion

Based on the discussion in the previous sections, it can be concluded that Law Number 27 of 2022 on Personal Data Protection (PDP Act) provides comprehensive guidelines for personal data protection by regulating the rights and obligations of each party related to personal data management. The PDP Act also prohibits actions that may threaten personal data security along with criminal threats. Actions threatening personal data security are commonly known as identity theft, defined as intentional acts by an individual to obtain/collect (by any means) another person's personal data without permission (illegally) and/or use that personal data for personal gain illegally, causing harm to others. The prohibition of such actions is stipulated in Article 65, and the criminal threats are stipulated in Article 67.

References

BPPTIK. (2024). *Jenis-Jenis Serangan Siber di Era Digital*. https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital

Febriari, S. (n.d.). *Deretan Kasus Kebocoran Data Pribadi di Indonesia Sepanjang 2022-2023*. Retrieved July 26, 2024, from https://www.metrotvnews.com/play/NA0CXWqa-deretan-kasus-kebocoran-data-pribadi-di-indonesia-sepanjang-2022-2023

Identity Theft and Assumption Deterrence Act of 1998. (1998, October 30). https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text#003

Kamus Besar Bahasa Indonesia. (n.d.).

Kementerian Perdagangan Republik Indonesia. (2024, January 5). *Kemendag Ramal Transaksi E-Commerce di RI Tembus Rp533 Triliun*. https://www.kemendag.go.id/berita/pojok-media/kemendag-ramal-transaksi-e-commerce-di-ri-tembus-rp533-triliun

-

Kevin Wang, S. Y., & Huang, W. (2024). *The Evolutional View of The Types of Identity Thefts and Online Frauds in The Era of The Internet*. Internet Journal of Criminology. https://pdfs.semanticscholar.org/0eef/a29e059b755373d1f4637 cf2e50e52919579.pdf

Lutfi, R. (2022). Perlindungan Data Pribadi sebagai Perwujudan Perlindungan Hak Asasi Manusia", Jurnal Sosial dan Teknologi. *Jurnal Sosial Dan Teknologi*, *2*(5), 434.

McQuade, S. C. (2009). *Encyclopedia of Cybercrime*.

Parkes, W. (2013). *Techniques of Identity Theft*. Canadian Internet Policy and Public Interest Clinic (CIPPIC).

Parsons, J. J., & Oja. (2013). *New Perspective on Computer Concepts 2014: Comprehensive, Course Technology*.

Prasetyo, S. N. (2016). Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia Ditinjau dari Asas Legalitas. *Jurnail Ilmiah Hukum Legality*, *24*(1), 109.

Prasetyo, S. N., Tongat, & Hidayah, N. P. (2019). Identity Theft and the Rules in Indonesia's Criminal Law. *Atlantis Press*, 30.

Schell, B., & Martin, C. (2006). *Webster New World Hacker Dictionary*. Wiley Publishing.

Syahbana, F. (n.d.). *Hati-Hati! Pencurian Identitas Semakin Mengancam Indonesia*. Retrieved July 26, 2024, from http://inet.detik.com/security/d-2975750/hati-hati-pencurian-identitas-semakin-mengancam-indonesia>,

Syahdeini, S. R. (2009). *Kejahatan dan Tindak PIdana Komputer*. Grafiti.

Vyctoria. (2013). *, Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*. ANDI.