East Asian Journal of Multidisciplinary Research (EAJMR)
Vol.2, No.11, 2023: 4585-4604

Legal and Ethical Implications in Data Theft Cases in the Digital Era

Hasudungan Sinaga
Universitas Tama Jagakarsa
Corresponding Author: Hasudungan Sinaga hassinaga@gmail.com

A R T I C L E I N F O

Keywords: Legal, Ethics, Digital, Data Theft

Received : 08, September
Revised : 15, October
Accepted: 20, Desember

A B S T R A C T

This research explores the legal and ethical implications in cases of data theft in the digital era in Indonesia. In the context of globalization and digitalization, personal data protection is very important to maintain individual privacy. However, Indonesia still does not have specific laws regarding personal data protection, although preventative efforts have been made. Factors such as lack of legal awareness among the public, lack of security in internet use, lack of knowledge of law enforcement officials, and lack of legislation present challenges in protecting personal data. The importance of legal certainty in protecting personal data demands the ratification of the Draft Law on personal data protection in Indonesia. Other countries such as the UK and Malaysia have ratify and legalize personal data protection laws to provide legal certainty to their citizens. Personal data protection must follow constitutional principles and involve cooperation between legislative, judicial and executive powers. In the judicial process, the principle of lex specialis derogat legi generali applies, allowing specific laws to override general provisions in criminal law. With the existence of specific personal data protection laws, people will feel safer and their privacy can be guaranteed in the era of increasingly advanced digitalization.

DOI prefix: https://doi.org/10.55927/eajmr.v2i11.6791
ISSN-E: 2828-1519
https://journal.formosapublisher.org/index.php/eajmr

INTRODUCTION

Rapid developments in information technology have had a significant impact on society in Indonesia. With easy access to information via the internet and computers, people have integrated information technology into their daily lives. This not only allows individuals to obtain information quickly, but also changes lifestyle, culture, economy, security and law enforcement in Indonesia (Azahrah, 2018). This progress also eliminates time and distance barriers in communication, both between individuals and governments. Companies can develop their business globally through online marketing, while governments can carry out diplomatic activities without having to be in the country concerned, all thanks to the global telecommunications network. Thus, information technology has become an integral part of modern life, expanding the scope of business, education and government in Indonesia. In today's increasingly rapid development, information technology plays a very important role in everyday life (Wijaya, 2021). However, Indonesian society's reliance on information technology also carries risks related to increased crime, known as "cybercrime". Cybercrime refers to various forms of illegal activities carried out via electronic networks, such as the internet.

Crime in cyberspace is increasingly dangerous because its scope is very broad. Criminals can easily infiltrate electronic networks and damage individual privacy and security (Ayu, 2021). Various types of cyber crimes include pornography, online gambling, terrorism, hacking, carding, ATM/EDC skimming, phishing, and many other criminal acts. It is important to remember that these crimes are not only financially detrimental, but can also threaten individual safety and privacy (Kholiviya, 2021). Therefore, it is important for society to increase awareness about the risks associated with the use of information technology. A better understanding of cyber security practices, use of strong passwords, and discretion in sharing personal information can help protect against cybercrime threats. In addition, governments, law enforcement agencies and internet service providers also have an important role in fighting cybercrime. They must work together to develop effective policies, increase penalties for cybercriminals, and educate the public on how to protect themselves from the threat of cybercrime (Putra & Setiawan, 2021). With these steps, it is hoped that we can reduce the negative impact of developments in information technologyand create a safer digital environment for everyone.

THEORETICAL REVIEW

Data theft in the internet world, also known as phishing, is a crime that involves illegally obtaining someone's personal or private information. Phishing perpetrators look for data such as credit card numbers, PINs, User IDs, telephone numbers, account numbers and other personal information (Oriana, 2021). After obtaining this data, the perpetrator can use it to harm the victim whose personal data was stolen and also other victims who are targets of fraud by the perpetrator. In Indonesia, the level of threat of criminal exploitation of information or personal data has increased, especially since the government implemented electronic Resident Identity Cards (e-KTP) in early 2011. E-KTP is a method of collecting people's personal information or data by

the government, which was implemented for the first time as a replacement for the Population Identification Number (NIK). In this policy, every resident is given a lifetime identity, and each person has one e-KTP card with a unique Population Identification Number (NIK) (Vellian, 2021). This card includes a variety of personal information, including physical characteristics and identity. However, problems arise when the data contained in the e-KTP is easily misused by criminals, especially if the security and protection of the data is not strong enough. This creates a risk of identity theft, fraud, or other exploitation of individuals whose personal data is stolen. Therefore, it is very important to increase public awareness about the risks of phishing and the importance of keeping personal information confidential. The government must also take firm steps to strengthen data protection in e-KTP and implement effective security policies. Apart from that, education and training regarding cyber security must also be improved to help the public identify phishing attempts and protect themselves from cybercrime threats (Sari et al., 2021). With these steps, we hope that we can reduce the risk of data theft and protect the privacy of the Indonesian people.

Personal information leaks are a serious problem in Indonesia and occur with high frequency. Especially in the banking sector, the exchange of customer personal data often involves card centers exchanging customer information, disclosing information to third parties, including credit card transactions, or interbank transactions. This can happen through public systems or through third parties, either individuals or companies that collect and trade customers' personal data. In the medical sector, patient data is also often traded or disclosed without the patient's knowledge, used for insurance purposes, employment opportunities, or receipt of government support programs (Wibowo et al., 2021). On online transportation platforms, consumer phone details are often misused and even used to threaten consumers due to bad passenger reviews. Not only does this result in inconvenience for consumers, but it can also convey personal messages that are not relevant to online delivery. In buying and selling transactions through online markets, cookie technology is used to misuse personal identification information such as shopping preferences, shopping locations, communication data, and even tracking online transactions to find out where the consumer's address is. All this shows how important personal data protection and strict policies are in handling and exchanging customer information. To overcome this problem, there needs to be firm steps from the government, related institutions, and companies involved in collecting and exchanging personal data. Strong data protection measures, strict law enforcement against perpetrators of data leaks, as well as increasing public awareness about the importance of maintaining online privacy are very important to reduce the risk of personal information leaks in Indonesia (Firdiawan, 2022).

On May 12 2021, there was a very serious case of theft of information or personal data in Indonesia. A total of 279 million Indonesian citizens' personal data was leaked and sold on hacker forums by an account with the name Kotz. The leaked data includes the full name of the Resident Identification Card

(KTP), telephone number, email, Identity Number (NID), domicile and income. In fact, the 20 million data is also equipped with personal photos of Indonesian residents. In this case, Kotz's account provided 1 million data samples for free by providing links that required a password to access. With a data leak of this magnitude, the privacy and security of thousands of people becomes very vulnerable. Information such as full name, telephone number, and email address can be used by criminals to commit fraud, fake identities, or other criminal activities (Sari, 2022). Meanwhile, other data such as Identity Number (NID) and income can also be exploited for bad purposes. This case highlights the importance of personal data protection and strict security policies in managing public information. Governments, related agencies, and companies must work together to improve data protection, strengthen cybersecurity, and provide training to the public on how to protect themselves from the threat of identity theft and online fraud.

The data leak case that occurred in Indonesia in 2021, which was suspected to be data from the Social Security Administering Agency (BPJS), created serious concerns regarding the privacy and security of people's personal information. In this case, 240MB of data was leaked and sold on online forums, containing sensitive information such as Population Identification Number (NIK), Mobile Number, Address, Email Address, Taxpayer Identification Number (NPWP), residence, number of dependents, and personal data other. In fact, there is 20 million data which also contains photos of residents, and from this data, there is very detailed BPJS Health card number information, with the total data reaching 272,788,202 million residents (Handoko, 2022). This case shows that data leaks and theft, even though they may not involve particularly sensitive information, can have serious consequences for victims. With personal information, including photos, criminals can threaten and abuse victims via social media. This real threat can cause both material and immaterial losses to the victim.

Currently, Indonesia is facing serious challenges related to data theft, which can harm victims materially and immaterially. The Indonesian government needs to take preventive steps and create strong legal protection to anticipate and minimize cases of data theft. The Theft of information or personal data not only threatens individuals, but also communities and the Indonesian people as a whole. However, in Indonesia, provisions regarding personal data protection have not been specifically regulated by law. Regulations related to personal data are still partial and sectoral, and sometimes duplicative (Farwansyah, 2022). These regulations are spread across several laws and only reflect general aspects of personal data protection. One of the laws that regulates some of these aspects is Law no. 11 of 2008 concerning Electronic Information and Transactions which has undergone changes through Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions (UUITE) (Yusuf, 2022).

Therefore, there is an urgent need to develop more comprehensive and specific regulations regarding personal data protection in Indonesia. This regulation must cover important aspects such as individual privacy rights,

company obligations in maintaining data security, as well as strict sanctions for perpetrators of data theft. With strong and effective legal protection, people and companies in Indonesia will feel safer when using information technology, while cybercriminals will be more encouraged to think twice before committing criminal acts.

METHODOLOGY

This research uses a qualitative approach with a focus on literature reviews to explore the legal and ethical implications in cases of data theft in the digital era. This approach allows us to in-depth review of the existing literature and analyze the various perspectives that have been put forward by previous researchers. The first step of this research was to identify relevant literature sources from various academic databases and scientific journals related to law, ethics, information security and cyber crime. These literature sources will include journal articles, books, theses, and other related publications. After collecting relevant literature, the next step is to compile and organize the literature based on the main themes to be researched, such as data protection law, privacy policies, ethical use of technology, and legal aspects related to cyber crime.

Next, the research will involve an in-depth analysis of this literature with a focus on identifying the legal and ethical implications in cases of data theft in the digital era. This analysis will include an in-depth understanding of the existing legal framework, applicable ethical norms, as well as comparisons between applicable regulations in various countries. During the analysis process, the research will also explore the latest developments in the fields of law and ethics related to data theft in the digital era. In addition, researcher will also look for knowledge gaps that may exist in existing literature and try to provide new insights or critical thinking related to the topic.

The results of the analysis will explain the main findings, a comparison between legal and ethical approaches in data theft cases, as well as the practical and theoretical implications of these findings. It is hoped that this research can provide a deeper understanding of the complexity of legal and ethical issues in the digital era and provide a broader view for researchers and practitioners in the fields of law, ethics and information security.

RESULTS AND DISCUSSION

Legal and Ethical Implications of Data Theft in Indonesia

The increasing use of mobile phones and the internet has had a significant impact on the protection of personal information or data. Misuse of personal data and crimes such as buying and selling personal information, account embezzlement, sharing personal information, fraud and pornography crimes are increasingly occurring. In this context, it is important to discuss the protection of personal information through laws and regulations that ensure the security and privacy of individuals. Personal data protection is closely related to the concept of privacy, which involves the integrity and dignity of individuals. Privacy also includes an individual's ability to control who has that information and how that information is used (Putranto, 2022). In developing

countries like Indonesia, where there are many users of modern technology and communication systems, it is important to have special laws that regulate privacy and data protection. However, until now, Indonesia does not have specific laws that address privacy and data protection issues.

As the use of technology grows, regulations regarding privacy and data protection do not develop in line with the rapid pace of technology. Many existing regulations cannot keep up with rapid technological developments, so there are legal loopholes that affect privacy and the protection of people's personal data. Therefore, clear and comprehensive regulations regarding privacy and personal data protection are needed in Indonesia. This regulation is expected to be able to overcome problems arising from misuse of personal information or data, protect individual privacy rights, and provide security for technology users in carrying out their online activities. Effective protection of personal data is essential to creating a safe and trusted digital environment for Indonesians.

Personal information and data have a very important role in social life, especially in the current era of digitalization. In this context, every aspect of our lives relies heavily on technology, and access to information and connections between people are no longer limited by distance or time. However, with these benefits also come risks to the security of personal data. Therefore, it is important to understand personal data protection in accordance with applicable legal provisions. According to Article 20, Article 1, Paragraph 1 of the 2016 Minister of Communication and Information Technology Regulation concerning the Protection of Personal Data in Electronic Systems, personal data is certain individual information that is stored, maintained and maintained as true and protected as confidential. In the context of information and personal data theft which is increasingly common in Indonesia, it cannot be ignored that advances in communication and information technology have triggered the emergence of new criminal acts that are different from conventional criminal acts (Fikri & Alhakim, 2022). Computer exploitation is one of the impacts of technological advances that brings unique and complex challenges to handling. A clear example of a criminal act that emerged as a result of the development of information and telecommunications technology is cybercrime, which involves crimes that occur via the internet. These crimes include various illegal activities such as data theft, online fraud, website hacking and other criminal activities involving the use of digital technology.

The rapid growth of internet users, especially in Asia including Indonesia, reflects the significant impact of advances in information and communication technology. In 2017, more than half of the world's population, or around 51.7%, used the internet. In Asia, there are 50% of the total 1,938,075,631 internet users worldwide. Indonesia, with 1,132,700,000 internet users, is ranked 4th in Asia and 8th in the world in terms of internet usage. Java Island is the region in Indonesia with the highest internet usage. These technological advances not only change the way we communicate and work, but also influence human behavior patterns, social values, and lifestyle.

Personal data protection is becoming increasingly important because information stored online involves highly sensitive personal data, such as credit/debit card account information, biometric data, medical records, and others. Personal data protection is a legal system that provides constitutional rights in many countries, also known as "*you have data*". This system involves regulations and laws that aim to protect sensitive user information from misuse or unauthorized access (Widayanti, 2022). Personal data protection includes important aspects such as privacy, integrity and confidentiality of information held by individuals.

Currently, there are no legal provisions that specifically regulate the protection of personal information or data in Indonesia. However, protection of privacy rights is regulated in Article 28G of the 1945 Constitution, although it does not specifically discuss the protection of a person's personal data. Nevertheless, this article can be used as a basis for forming regulations regarding personal data protection, although this is still an area that requires more attention in legal regulations. The Indonesian government has taken preventive measures to protect personal data through several policies regulated by several existing regulations. Some of them include the ITE Law, Law no. 36 of 1999 concerning Telecommunications (Telecommunications Law), Law no. 8 of 1997 concerning Company Documents, Law no. 7 of 1971 concerning Basic Provisions for Archives, Law no. 36 of 2009 concerning Health, Law no. 10 of 1998 concerning Amendments to Law no. 7 of 1992 concerning Banking, as well as Law no. 24 of 2013 concerning Amendments to Law no. 23 of 2006 concerning Population Administration (UU Adminduk) (Darmilis et al., 2023).

Government Regulation no. 52 of 2000 concerning Telecommunications Operations is an implementing regulation of the Telecommunications Law and identifies the internet as a type of multimedia service which is a provider of information technology-based telecommunications services. From a regulatory perspective, the internet is included in the realm of the Telecommunications Law and regulates several matters related to the confidentiality of personal data.

Law no. 36 of 1999 concerning Telecommunications (Telecommunications Law) in Indonesia has provisions that prohibit acts of manipulation and unauthorized access to telecommunications networks. Article 22 of the Telecommunications Law states that every person is prohibited from carrying out acts without rights, illegality, or manipulation of access to telecommunications networks, access to telecommunications services, or access to special telecommunications networks. Violation of this provision can be subject to a maximum prison sentence of six years and/or a maximum fine of IDR 600 million. In addition, Article 40 of the Telecommunications Law prohibits interception of all forms of information sent via telecommunications networks. Violation of this provision can result in a maximum prison sentence of up to 15 years.

The Telecommunications Law also regulates the obligations of telecommunications service providers to store messages sent and received by telecommunications service customers via the telecommunications network

and/or telecommunications services provided (Article 42 paragraph (1)). Violation of this obligation can be subject to a maximum prison sentence of 2 years and/or a maximum fine of IDR 200 million (Roni et al., 2023). Although the Telecommunications Law does not explicitly regulate the protection of personal data, the Information and Electronic Transactions Law (UU ITE) regulates various aspects related to the use and protection of electronic data. The ITE Law provides a new understanding of the protection of the existence of electronic data or information, both public and private. Even though it does not directly regulate personal data protection such as special personal data protection laws, the ITE Law provides a relevant legal basis regarding the use and security of electronic data.

Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (PP PSTE) mandates further classification of personal data. Protection of personal data in an electronic system according to the Information and Electronic Transactions Law (UU ITE) includes protection against unauthorized use of data, protection for electronic system operators, as well as protection from illegal access and interference. In relation to the use of personal data without permission, Article 26 of the ITE Law stipulates that any use of a person's personal data via electronic media must be carried out with the permission of the individual concerned.

Anyone who violates this provision may be sued for losses incurred. In its explanation, Article 26 of the ITE Law states that personal data is part of an individual's right to privacy (Azahrah, 2018). Article 1 PP PSTE defines direct data as personal data of an individual that is stored, maintained and protected confidentially in good faith. The explanation of article 26 paragraph (1) of the ITE Law also illustrates that the use of information technology and the protection of information or personal data is part of an individual's right to privacy. Therefore, any use of personal data in the context of electronic technology must obtain permission from the individual concerned, and violations of this right may result in legal claims for damages. Thus, this setting aims to protect individual privacy and personal data in the digital era.

Law Number 24 of 2013 concerning Population Administration does have an important role in providing protection for the personal data of residents in Indonesia. This regulation regulates the protection of personal data such as information about physical or mental disabilities, fingerprints, signatures and other elements that constitute a person's privacy. Article 95A in the Law also provides strict sanctions for violators who distribute personal data without authorization, with the threat of imprisonment for 2 years and a fine of Rp. 25,000,000.00. Government Regulation no. 82 of 2012 and the Information and Electronic Transactions Law (UU ITE) are legal instruments that regulate the protection of personal data in the context of electronic systems and transactions in Indonesia. Government Regulation no. 82 of 2012 defines personal data as certain individual data that is stored, maintained as true and protected as confidential. However, in this regulation, it is not explained in detail what information is considered personal data. This creates uncertainty as to whether anonymous data or publicly available data falls within the definition

of personal data. On the other hand, the ITE Law also regulates legal protection efforts for users of online administration services (Kholiviya, 2021). Article 26 paragraphs 1 and 2 of the ITE Law states that the use of a person's personal data must be based on the data subject's consent. If there is a violation of this agreement, the aggrieved data subject has the right to file a lawsuit against the losses suffered as a result of the action.

Personal rights have very important implications in the context of individual life, especially in the digital era. Privacy rights involve the right to have an inviolable private life, the right to communicate with others without being spied on, and the right to access information about one's life and personal data. Within the Indonesian legal framework, the ITE Law does have provisions governing the protection of personal data. Articles 30-33 and Article 35 of the ITE Law regulate activities that are not permitted, including the prohibition of illegal access to other people's data through electronic systems with the aim of violating security systems and obtaining information. Apart from that, the ITE Law also clearly prohibits wiretapping unless carried out by parties who have the right to do so with legal permission. If an individual feels disadvantaged by behavior that violates these provisions, they have the right to demand compensation, and the perpetrator will be responsible for the actions they have committed. Thus, the ITE Law provides an important legal basis for protecting the privacy rights and personal data of individuals in Indonesia.

Personal data protection is a shared responsibility between individuals, society, legal entities and the government. The government plays a very important role in forming legal policies that protect citizens' personal data. In this case, legal policies must not only be based on common sense considerations, but must also be able to provide effective protection to the Indonesian people. Preventive and repressive efforts can be taken to protect personal data. Preventive efforts involve careful disclosure and monitoring of personal information. In this case, supervision can be carried out by the private sector and the government. Private parties, such as online content and service providers and internet service providers, have a responsibility to maintain the confidentiality of their customers' data. On the other hand, the government has a role in regulating and supervising personal data management practices, as well as enforcing the law through repressive measures against personal data violations (Oriana, 2021). Through collaboration between the private sector, society, legal entities and the government, personal data protection can be improved and people can feel safer when using information technology and the internet. This is important to maintain the privacy and security of personal data in the era of increasingly advanced digitalization.

Law no. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) has great sociological significance in Indonesian society. The ITE Law is a very important legal basis for regulating various activities carried out by the public when interacting in cyberspace or the internet. In the era of globalization of information, where access to information is increasingly easier and faster, protecting network operators and the public's interests in accessing information becomes very crucial. The ITE Law provides the legal framework necessary to

protect the interests of all parties involved in online activities. Apart from that, the ITE Law also reflects the values, moral principles and norms that apply in society. The regulations in the ITE Law were made taking into account the values believed in and upheld by the Indonesian people. With the legal certainty provided by the ITE Law, people can feel safer and more protected when carrying out activities in the digital world. They know that there are rules that regulate online behavior and provide sanctions for certain violations.

Protection of personal data is very important in supporting the right to individual privacy. To ensure effective protection, provisions for the protection of personal information or data should be placed in the Constitution or legal documents with the highest authority in a country. The Constitution, as the highest legal instrument, provides a strong basis for individual rights, including the right to privacy and security of personal data. By including these rights in the Constitution, the country affirms its commitment to protecting the privacy of individuals and their personal data. This provides a solid legal basis for the development of more detailed and technical regulations regarding personal data protection. In addition, the legal certainty provided by the Constitution guarantees the public that their privacy rights are recognized and respected by the state.

Factors that Cause Data Theft in the Digital Era

Crimes involving information technology, or what is often referred to as cybercrime, can be classified as white crime. White crime refers to crimes committed by people who have technical knowledge or skills in the field of technology or the internet. These cybercriminals have a deep understanding of internet applications and are often highly skilled in the field. They utilize their skills to carry out various types of criminal acts in cyberspace. In addition, criminal acts in cyberspace are often transnational, meaning that the crime involves more than one country or crosses borders between countries.

This transnational criterion shows that the criminal act is not limited to one particular region of the country, but rather involves different countries. Some examples of criminal cases on the internet that often occur among Indonesian people include online fraud, online gambling, spreading fake news (hoaxes), cracking (hacking systems), and theft of personal data via the internet. With the increasingly rapid development of information technology and the use of the internet in various aspects of people's lives in Indonesia, computer security has become very important. Threats to computer security can be physical, such as hardware theft, or non-physical, such as network attacks and malicious software such as viruses.

Personal data or information related to the population and demographics in Indonesia, such as Family Cards (KK), Population Identification Numbers (NIK), and Electronic Identity Cards (E-KTP), is very sensitive information and must be properly protected. Cases of personal data theft in Indonesia show various forms of data exploitation that can harm the individual (Vellian, 2021). One form of exploitation of personal data is data buying and selling, where criminals sell the personal information they steal to other parties. The

information can then be used for a variety of purposes, including data profiling, research, marketing purposes, and espionage activities. In addition, stolen personal data can also be misused for criminal activities such as illegal transactions, fraud, creating fake accounts, and money laundering. Criminals often use the personal data they obtain from victims as a source of income, selling it to parties who need the information.

Personal data or information refers to data about individual characteristics, such as name, age, address, occupation, education, family status and gender. Juridically, the personal data that has been explained is regulated based on Republic of Indonesia Government Regulation No. 82 of 2012 concerning Implementation of Electronic Systems and Transactions. According to this regulation, special individual data that is maintained, stored and kept confidential and correct includes information or personal data of residents that must be carefully protected.

Personal information or data that must be protected includes family card number, population identification number (NIK), date of birth, health information, father's NIK, mother's NIK, sibling's NIK, as well as several other important event records. The importance of protecting personal information or data lies in efforts to prevent misuse by perpetrators of personal data theft. In the context of the use of technology and electronic transactions, protecting personal data is very important to prevent unauthorized access, illegal use and exploitation of data by irresponsible parties (Firdiawan, 2022). Therefore, effective personal data protection efforts and compliance with regulations governing this matter are very necessary to maintain individual privacy and security.

Personal data or information that does not have a physical form is often ignored, especially in the context of social life. Many people ignore the protection of their personal data because the information does not have to be published on the internet to remain at risk, and this could lead to the destruction of other people's personal information. The ignorance and friendliness of society, which is a cultural characteristic in Indonesia, often provides opportunities for criminals regarding ownership of personal data. The culture of tolerance and tendency to forgive in Indonesian society can create an environment that is vulnerable to fraud and exploitation, especially in cyberspace.

This tolerant nature influences the level of reporting to the authorities, especially when victims of online fraud choose to remain silent rather than report the incident. In some cases, victims may choose not to report the crime to law enforcement, especially if the material losses suffered are not significant. However, in Indonesia, if material losses exceed a certain limit, namely Rp. 500,000, the public will generally report it to the authorities. Nevertheless, it is important for the public to raise awareness about the importance of protecting their personal information and reporting crimes related to personal data to create a safer and more trustworthy online environment for everyone.

The factor of individual negligence is the biggest gap in the causes of criminal cases of data theft. For example, using passwords that are easy to guess or rarely changing passwords regularly can provide opportunities for criminals to access personal data. Apart from that, giving cell phone access to other people without careful consideration can also open up the potential for data theft. One of the biggest threats in information security today is social engineering attacks, where perpetrators exploit human weaknesses, such as ignorance or negligence, to steal information or hack accounts. In fact, workers in the Information Technology (IT) sector, even though they understand the importance of security, still often experience incidents of negligence or are exposed to various forms of attacks.

The general public, especially those who do not understand the security aspects of technology, are vulnerable to social engineering attacks. Criminals tend to take advantage of human carelessness, lack of knowledge and trust to achieve their goals. Therefore, increasing awareness and knowledge about information security and being careful in sharing personal data is very important to protect yourself from the threat of cybercrime. Based on the phenomena that occur among Indonesian society, several conclusions can be drawn regarding the factors that cause cases of theft of information or personal data:

a) Lack of Legal Awareness Among the Community

Legal awareness based on knowledge of the rules and laws that apply in society is still lacking. Currently, public legal awareness of cybercrime is still considered inadequate due to a lack of understanding of cybercrime, both in terms of behavior and impact. The level of people's knowledge about technology and activities in cyberspace also influences their understanding of online activities. The less a person knows about technology, the more likely they are to be exploited by criminals.

b) Lack of Security in Internet Use

Cybercriminals take advantage of internet opportunities that can be accessed in various places, both in closed and open areas. However, because the internet protection system is still not optimal, everyone has the freedom to carry out activities in cyberspace without understanding the limitations which can contribute to the spread of cybercrime.

c) Lack of Knowledge of Law Enforcement Officials

Some law enforcement officials may still not understand the techniques used by cybercriminals. Cybercrime is becoming more intense in Indonesia, and cybercriminals tend to be more skilled than law enforcement officials. It is important to optimize the role of qualified and structured law enforcement officers, as well as consolidate a community dedicated to dealing with all types of cybercrime.

d) Inadequate Legislation

Indonesia does not yet have specific regulations controlling cybercrime, although the Criminal Law and ITE Law should be used to handle these cases. However, the lack of insight and skills in cyberspace makes existing regulations difficult to implement. Many cases of theft of personal information and data have occurred, but there are still many victims who are not aware of this risk or ignore it, so that personal data is not stored properly.

It is important to increase legal awareness, internet security, knowledge of law enforcement officials, and improve existing legislation to protect the public from the threat of theft of information and personal data in cyberspace (Farwansyah, 2022). This requires cooperation between the government, law enforcement agencies, and the community in order to create a safe and trustworthy online environment.

Legal and Ethical Urgency of Misuse of Personal Data in Efforts to Provide Legal Certainty

Understanding that needs to be improved regarding personal data protection is very important so that people understand the importance of maintaining the confidentiality of their personal information. This awareness is a fundamental first step to protect personal data from theft and misuse. The public needs to understand that secure personal data is a shared responsibility, and each individual has a role in maintaining the confidentiality of their own data. To achieve optimal data protection, the government needs to establish legal arrangements or laws that regulate personal data protection. This law will provide a clear legal basis and regulate procedures for the use, collection, storage and dissemination of personal data.

With this law, people can feel safer because there is legal certainty that protects them from misuse of personal data. The importance of legal regulations related to personal data protection is to provide guarantees of protection to the public and create legal certainty in handling problems related to personal data in society. With clear legal regulations, perpetrators of criminal acts of theft of personal data can be prosecuted in accordance with applicable law, and people can feel more confident in using services and interacting in the digital world without fear of their personal data being misused for illegal personal interests.

With the existence of special laws that protect and guarantee the security of personal data, the public can obtain legal certainty. Laws that are specific and regulate in detail regarding the protection of personal data have greater legal force than laws that regulate in general. For example, when there is a specific law that regulates personal data theft, perpetrators who are proven to have committed data theft can be punished according to the provisions in that law (Putranto, 2022). However, even though there are laws that protect personal data, rapid technological developments also create opportunities for criminals to access personal data in more sophisticated ways. Therefore, society and authorities need to take preventive steps to prevent theft of personal data.

When an incident of personal data theft occurs, investigative steps must be taken immediately to determine the extent of the case involving personal data and immediately take appropriate legal action. Reports regarding theft of

personal data can be made either verbally or in writing. The report must be signed by the reporter to validate the truth of the information submitted. If there is misuse of personal data involving Indonesian citizens, the case will be resolved in accordance with Indonesian law and enforced in courts in Indonesian jurisdiction. With firm legal action and the existence of supporting laws, it is expected that perpetrators of criminal acts of theft of personal data can be stopped and people can feel safer in using digital services without worrying that their personal data will be misused.

Prevention is the first step in legal protection against misuse of personal data, which is known as Self Regulation. This is important because until now, the Bill (Draft Law) on personal data protection that should have existed in Indonesia has not been passed. In comparison, other countries such as the UK and Malaysia have gone a step further in protecting the personal data of their citizens. In the UK, protection of personal identity has been regulated since 2000 through the Data Protection Act 1998 (Fikri & Alhakim, 2022). The implementing body, known as The Data Protection Commissioner, is tasked with monitoring the use of personal data, both by individuals and by entities that manage personal data. The main aim is to ensure that personal data is not misused and is processed correctly in accordance with applicable regulations.

The country of Malaysia has also passed a personal data protection law in 2010, known as the Personal Data Protection Act (PDPA). This law aims to regulate the management of personal data in the context of commercial administration. PDPA Malaysia aims to guarantee the interests of data subjects, namely individuals whose personal data is managed by other parties, so that the use of such data does not violate the privacy and rights of these individuals. With the existence of personal data protection laws, both in the UK and in Malaysia, the public and individuals have legal certainty regarding the use of their personal data. However, in Indonesia, personal data protection still relies on self-prevention measures (Self Regulation) because the law that regulates this does not yet fully exist. Therefore, it is important for the Indonesian government to immediately pass the personal data protection bill to protect the privacy rights and security of people's personal data.

Currently, Indonesia does not have specific and firm legal regulations regarding the theft of personal data. Although several laws have been mentioned separately, such as Law Number 19 of 2016 concerning Electronic Information and Transactions which replaces Law Number 11 of 2008 concerning Electronic Information and Transactions, as well as Government Regulation Number 2 of 2012 concerning System Implementation and Electronic Transactions, there is still a need for specific and clear laws regarding misuse of personal data. Looking at the various guarantees and protections that other countries have, Indonesia should have protection that is at least comparable or even better. With specific laws in place, society and individuals will have stronger legal certainty regarding the use and protection of their personal data.

The law must regulate in detail the legal actions that will be taken against perpetrators of personal data theft, including strict sanctions in order to provide a deterrent effect to the perpetrators of these crimes (Darmilis et al., 2023). With specific and strict legal regulations, people will feel safer and protected from potential theft of personal data. Apart from that, the existence of clear laws will also increase public awareness regarding their rights regarding privacy and security of personal data. Therefore, it is important for the Indonesian government to immediately formulate adequate personal data protection laws to protect the interests of society and follow international data protection standards that have been set by developed countries.

The Indonesian government has responded to the situation of personal data theft with a more effective and structured approach. One of the steps taken is to formulate a law that specifically protects personal data specifically. This approach includes a series of actions related to personal data collection practices, both for individuals and government agencies. One example of implementing this approach is through the Population Identification Number (NIK) program which is mandated by Law Number 24 of 2013 concerning Population Administration. Since 2011, the Indonesian government has started recording residents' personal data through the electronic identity card (e-KTP) program.

This program is technically regulated through Presidential Regulation Number 67 of 2011 concerning Resident Identity Cards Based on National Population Identification Numbers. In this regulation, there are provisions governing the types of residents' personal data recorded on e-KTP. This approach reflects the government's efforts to protect citizens' personal data in a structured and measurable way. By having regulations governing personal data collection practices, the government can ensure that residents' personal data is safe and protected from potential misuse. In addition, this approach also provides clarity to the public regarding their rights and protection regarding personal data, thereby creating trust and awareness of the importance of maintaining privacy in an increasingly complex digital world.

The situation that requires the Population Identification Number (NIK) to be included in the e-KTP as the main prerequisite for obtaining various public services, both from the government and the private sector, shows the urgency of legal regulations that regulate the process, how to manage and protect personal data, including the role of the parties thirdly in the process of recording personal data. However, it is unfortunate that provisions regarding this matter are not regulated in law. Protection of personal data is very important because it is a form of respect for individual privacy rights. To start this process, correct and specific legal arrangements are needed. Guarantees for the protection of personal data must be adapted to legal instruments that have much higher power, namely the constitution.

When the state guarantees and establishes these rights in line with the constitution, it will be easy to identify individual privacy rights in a country, the legal rules that will be used, and what criminal offenses will be imposed. By having clear legal regulations regarding the protection of personal data, the

Indonesian state can ensure that the privacy rights of its citizens are well protected. This step not only creates legal certainty for individuals but also strengthens the legal foundation that supports the right to privacy as a value upheld in society. Thus, the existence of legal arrangements governing personal data protection will ensure that individual personal information is safe and is not misused by unauthorized parties.

In the context of law enforcement in Indonesia, there are three policy stages involving three important instruments of state power. First, legislative power, which is tasked with determining and formulating actions that can be criminalized and sanctions that will be imposed. Second, the judicial power, which is responsible for implementing the new laws that have been established. Lastly, executive power, which plays the role of implementing criminal acts. These three instruments of state power are expected to be able to provide protection for personal data. As a rule of law country that complies with the constitution, legal arrangements related to this issue should position citizens as the main priority. Thus, the protection of personal data in Indonesia can be guaranteed effectively through cooperation between the legislative, judicial and executive powers, which work in accordance with the provisions of the constitution and applicable laws.

The judicial process for a criminal offense in Indonesia is based on Law Number 8 of 1981 concerning Criminal Procedure Law (KUHAP). The Criminal Procedure Code is a procedural law that regulates the procedures for resolving or handling criminal cases, starting from inquiry, investigation, prosecution, trial, examination proceedings, appeals, cassation, to judicial review. The Criminal Procedure Code together with the Criminal Code (KUHP) is the basis of general law (lex generali) in criminal law in Indonesia. In the context of criminal law, the principle of lex specialis derogat legi generali applies, which means that laws that are special in nature and have specific procedural laws and criminal sanctions will override the general provisions contained in the Criminal Procedure Code and the Criminal Code.

This means that if there are other laws outside the Criminal Procedure Code and Criminal Code that regulate judicial procedures and criminal sanctions for certain cases, then these special provisions will apply (lex specialis) over the general provisions contained in the Criminal Procedure Code and Criminal Code (lex generali) . With this principle, criminal law in Indonesia can accommodate special and complex cases in accordance with applicable laws.

In our research, we found that until now, there are no regulations that specifically regulate criminal sanctions for perpetrators of personal data theft in Indonesia. However, the government and the House of Representatives (DPR) are in the process of ratifying the Personal Data Protection Bill (RUU). This bill has been prioritized as a priority by the House members so that it can be quickly passed into law, addressing the existing legal vacuum in terms of personal data protection. With this bill, it is hoped that there will be a clear legal basis, including criminal sanctions, to protect the personal data of Indonesian

people from theft and misuse. The bill reflects the government's efforts to address data security issues in an increasingly complex digital era.

Permenkominfo 20/2016 is Minister of Communication and Information Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. This regulation regulates the protection of personal data in electronic systems and provides administrative sanctions for violations of personal data protection. Administrative sanctions regulated in Permenkominfo 20/2016 include:

a) Violators may receive a verbal warning as a form of direct reprimand regarding violations of personal data protection.
b) Violators can receive a written warning that officially records the violation that has been committed and reminds them to comply with personal data protection rules.
c) In cases of more serious violations, a temporary suspension of activities involving the processing of personal data may be imposed as a sanction measure.
d) Very serious violations may result in the violation being announced on sites within the network, so that the public is aware of the violation's actions and understands the consequences.

These administrative sanctions aim to provide encouragement to companies and individuals to comply with personal data protection provisions and prevent misuse of other people's personal data. However, it is important to note that Permenkominfo 20/2016 still contains administrative sanctions and does not include criminal sanctions. Therefore, the Personal Data Protection Bill which is currently in the process of being ratified is expected to provide a more comprehensive legal basis, including criminal sanctions, to protect the personal data of the Indonesian people more effectively.

CONCLUSIONS AND RECOMMENDATIONS

Based on this research, it can be concluded that theft of personal data has serious implications in the legal and ethical context in Indonesia. The era of digitalization brings ease of access to information and communication, but also increases risks to the security of personal data. In Indonesia, there is no law that specifically regulates the protection of personal data, although several related laws exist, such as the ITE Law and the Population Administration Law. However, protecting personal data is becoming increasingly important considering the rapid growth of internet use in Indonesia.

Factors such as lack of legal awareness, lack of security when using the internet, lack of knowledge of law enforcement officials, and inadequate legislation are causes of data theft. Therefore, the existence of specific and strict personal data protection laws is very important. Clear legal regulations with constitutional force will provide legal certainty for individuals, increase public awareness about their privacy rights, and strengthen the legal foundation that supports the protection of personal data as a value upheld in Indonesian

society. Apart from that, personal data protection also involves cooperation between individuals, society, legal entities and the government to ensure information security and personal data privacy in an era of increasingly advanced digitalization.

FURTHER STUDY

Through this research, it is hoped that new insights and a more comprehensive understanding of the legal and ethical implications of data theft will emerge. The results of this research are expected to make a positive contribution to policy makers, legal practitioners, and the wider community in facing the growing challenges in the realm of digital data security.

REFERENCES

AYU, D. G. (2021). *PENYIDIKAN TINDAK PIDANA PENCURIAN DATA NASABAH MELALUI MESIN ANJUNGAN TUNAI MANDIRI (ATM)(Studi di Polres Kota Mataram)*. eprints.unram.ac.id. http://eprints.unram.ac.id/id/eprint/20930

Azahrah, W. (2018). *Perlindungan Hukum Terhadap Korban Tindak Pidana dalam Kasus Pencurian Data Nasabah Bank Mandiri*. dspace.uii.ac.id. https://dspace.uii.ac.id/handle/123456789/5740

Darmilis, D., Yustrisia, L., & Zulfiko, R. (2023). KAJIAN YURIDIS PENGATURAN HUKUM TINDAK PIDANA PENCURIAN DATA PRIBADI (PHISING) DI INDONESIA. *Ensiklopedia of Journal*. https://jurnal.ensiklopediaku.org/ojs-2.4.8-3/index.php/ensiklopedia/article/view/1947

Farwansyah, A. (2022). *Penegakan Hukum Tindak Pidana Pencurian Data Kartu Kredit (CARDING) Di Wilayah Hukum Kepolisian Daerah Riau*. repository.uir.ac.id. https://repository.uir.ac.id/15332/

Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *YUSTISI*. https://ejournal.uika-bogor.ac.id/index.php/YUSTISI/article/view/7474

Firdiawan, M. A. (2022). *Penegakan hukum terhadap pelaku tindak pidana pencurian data kartu kredit (Carding) dihubungkan dengan Pasal 30 Ayat (2) Jo Pasal 46 Ayat (2) Undang-undang …*. etheses.uinsgd.ac.id. https://etheses.uinsgd.ac.id/56954/

Handoko, D. (2022). *ANALISIS YURIDIS PERLINDUNGAN KORBAN TINDAK PIDANA PENCURIAN DATA PRIBADI MELALUI SISTEM ELEKTRONIK*. repository.unas.ac.id. http://repository.unas.ac.id/5296/

Kholiviya, H. (2021). *PERLINDUNGAN HUKUM TERHADAP KORBAN PENCURIAN DATA PRIBADI DALAM KASUS TINDAK PIDANA MAYANTARA (CYBER CRIME)*. repository.unissula.ac.id. http://repository.unissula.ac.id/24642/

Oriana, R. (2021). *kebijakan formulasi dalam penanggulangan tindak pidana pencurian data bank (skimming)*. etd.repository.ugm.ac.id. https://etd.repository.ugm.ac.id/penelitian/detail/202263

Putra, F. D., & Setiawan, D. A. (2021). *Kebijakan Hukum Pidana dalam Perlindungan Hukum Terhadap Korban Tindak Pidana Pencurian Data Pribadi Dalam Transaksi Elektronik Ditinjau dari Undang ….* repository.unisba.ac.id. http://repository.unisba.ac.id/handle/123456789/28290

Putranto, A. W. (2022). *Pertanggungjawaban Pidana Pelaku Tindak Pidana Pencurian Data Pribadi dengan Teknik Phising*. digilib.uns.ac.id. https://digilib.uns.ac.id/dokumen/detail/98737/

Roni, R., Yustrisia, L., & Munandar, S. (2023). Proses Penegakan Hukum Pidana Terhadap Pelaku Tindak Pidana Pencurian Data Nasabah Bank Melalu Mesin Atm Sebagai Penyalahgunaan Teknologi …. *Ensiklopedia of Journal*. https://jurnal.ensiklopediaku.org/ojs-2.4.8-3/index.php/ensiklopedia/article/view/1816

Sari, M. P., Mamang, D., & Zakky, M. (2021). Penegakkan Hukum terhadap Tindak Pidana Pencurian Data Pribadi melalui Internet Ditinjau dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas …. *Jurnal Hukum Jurisdictie*. https://journalfhuia.ac.id/Jurisdictie/article/view/44

SARI, S. (2022). *… tindak pidana terhadap pencurian data di Kota Makassar dan faktor apa saja yang menjadi penghambat kepolisian terhadap Pelaku Tindak Pidana Pencurian Data ….* repository.unibos.ac.id. https://repository.unibos.ac.id/xmlui/handle/123456789/3034

Vellian, L. M. (2021). *PERBANDINGAN FORMULASI TINDAK PIDANA PENCURIAN DATA (DATA THEFT) DALAM KEBIJAKAN HUKUM PIDANA INDONESIA DAN HUKUM PIDANA ….* repository.unika.ac.id. http://repository.unika.ac.id/27336/

Wibowo, S. A., Syahrin, A., & ... (2021). Pertanggungjawaban Pidana Bagi Pelaku Tindak Pidana Pencurian Data Nasabah Perbankan Dengan Metode Skimming Di Tinjau Menurut Undang-Undang …. *Iuris Studia: Jurnal ….* http://jurnal.bundamediagrup.co.id/index.php/iuris/article/view/100

Widayanti, P. W. (2022). Tindak Pidana Pencurian Data Nasabah Dalam Bidang Perbankan Sebagai Cyber Crime. *Legacy: Jurnal Hukum Dan Perundang …*. https://ejournal.uinsatu.ac.id/index.php/legacy/article/view/6218

WIJAYA, A. I. (2021). *ANALISIS KEBIJAKAN FORMULASI TERHADAP TINDAK PIDANA PENCURIAN DATA PRIBADI DI DUNIA MAYA (ANALISIS UU ITE DAN RUU PDP)*. digilib.unila.ac.id. http://digilib.unila.ac.id/id/eprint/60731

YUSUF, M. (2022). PENEGAKAN HUKUM BAGI PELAKU TINDAK PIDANA PENCURIAN DATA NASABAH PERBANKAN MENURUT UNDANG–UNDANG INFORMASI DAN TRANSAKSI …. *NATIONAL JOURNAL of LAW*. http://journal.unas.ac.id/law/article/view/1682