UNTAG Law Review (ULREV)
Volume 8, Issue 1, MEI 2024, PP 16-27
ISSN 2549-4910 (online) & ISSN 2579-5279 (print)
http://jurnal.untagsmg.ac.id/indeks.php/ulrev/indeks
www.fakhukum.untagsmg.ac.id

PERSONAL DATA THEFT IN THE ERA OF INFORMATION TECHNOLOGY PROGRESS: IMPACT AND OVERCOMING STRATEGIES IN INDONESIA

Sumartini Dewi[1], Muchlas Rastra Samara[2] Pratiwi Ayu Sri D[3]
[12]Faculty of Law Univeristy of 17 Agustus 1945 Semarang
sumartini.dewi@gmail.com[1], muchlasmuksin02@gmail.com[2],
Pratiwiayu@gmail.com[3]

ABSTRACT; *This article examines the problem of information security crimes in the conditions of technological progress with the globalization of international life, including relations between countries, taking into account the high level of development of technological and information resources. The importance of ensuring information security as an object of legal protection protected by written international and national law. This research method is normative with a statutory, historical and philosophical approach. efforts to improve international and national legal policies to modernize the national legal system for the prevention and eradication of cybercrime. An effective legal regulatory mechanism for objects to be legally protected is essential to ensure information security. Special attention is focused on solving the problem of detection, disclosure and accurate legal evaluation of crimes and violations committed in cyberspace. Administrative instruments, institutions, international cooperation, community participation, dispute resolution and procedural law, prohibitions on the use of personal data and criminal law asLast Remedyto overcome personal data leaks, protect personal data in the process of processing Personal Data in order to guarantee people's constitutional rights.*

Keywords, *Criminal Acts, Information Security, Information Technology, Legal Protection.*

INTRODUCTION

Changes in societal values and systems, there is an increase in awareness of human rights, justice and individual protection. This creates demands for a more progressive and inclusive legal system. Technological advances and globalization have brought dramatic changes in the way people interact, do business and communicate. This creates new challenges in terms of data protection, privacy and cybersecurity, which then require adaptation and development of relevant laws. Global terrorism and changes in the national security paradigm trigger discussions about the balance between societal security and individual rights. Laws focused on preventing cyber terror and protecting citizens' rights are becoming increasingly important.

The desire to protect and promote the basic rights of every individual is the basis for many changes in legislation. Globalization has had a significant impact on Indonesia, and the background involves a number of economic, political, social and technological factors. The following are several background aspects of globalization in Indonesia. Advances in information technology, especially the internet, have opened up access to global information and enabled Indonesia to be involved in data exchange, international communication, et*c e-commerce.* It also facilitates collaboration between businesses, organizations, and individuals around the world.[1]

Personal data protection reflects a response to the need to protect individuals' personal information amidst the growth of technology and increasingly widespread data exchange. Protecting personal data is important because the growth of digital technology, especially the internet, has provided easier and faster access to data. However, this also increases the risk of exploitation and misuse of personal data. With increasing global connectivity, personal data is often accessed and transferred across national borders. This requires an effective and uniform data protection framework to ensure that individual privacy rights are respected across countries.

Data has become a valuable "asset" and commodity in the era of a data-based economy. Large amounts of personal data are collected by companies for analytics, advertising targeting, and product development.[2] Data protection is crucial to prevent misuse of personal data. Increasingly complex cyber attacks, such as hacking,*malware,* and attack*phishing,* puts personal data at high risk. Data protection is the key to reducing vulnerability to attacks and protecting sensitive information of citizens, especially in Indonesia. The right to privacy is considered a fundamental human right.

Personal data protection not only serves as a means to protect personal information, but also to ensure the freedom and security of individuals in the use of their data. As awareness of the importance of protecting personal data increases, many countries

[1] M A Yani, "Pengendalian Sosial Kejahatan (Suatu Tinjauan Terhadap Masalah Penghukuman Dalam Perspektif Sosiologi)," *Jurnal Cita Hukum*, 2015, https://www.neliti.com/publications/95338/pengendalian-sosial-kejahatan-suatu-tinjauan-terhadap-masalah-penghukuman-dalam.

[2] A W Winarno and A C Isradjuningtias, "Perlindungan Hukum Pelaku Usaha E-Commerce Terhadap Pelaku Pemalsuan Akun Konsumen Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 …," *Bus. LJ* (scholar.archive.org, 2022), https://scholar.archive.org/work/pzzr53a3szbz7hfyezuhrarom4/access/wayback/https://journal.unpak.ac.id/index.php/palar/article/download/5032/pdf.

have begun to pass laws and regulations governing the collection, processing and storage of personal data, especially Indonesia.

Data from the director general of applications and informatics at the Ministry of Communications and Information Technology reveals that there have been 94 cases of data leaks in Indonesia since 2019, with 35 of them occurring in 2023, cases of data leaks of 18.5 million BPJS jobs sold on dark forums containing NIK, full name , date of birth, cell phone number, email address, occupation and company name.[3]Understanding this background, personal data protection is considered an important step in maintaining individual security, building public trust in technology, and creating a safe digital environment.

It reflects the complex dynamics between societal demands, technological developments, and global challenges that require adaptation and evolution in the legal system. Over time, legal protection continues to evolve to reflect emerging values and needs in society which directly pose future challenges to personal data protection in Indonesia. With an understanding of this background, efforts to protect against cybercrime must involve a combination of improving security technology, increasing public awareness, international cooperation, and strict regulations to provide effective protection against ever-evolving cyber security threats.

PROBLEM

Based on the background above, the author formulates the problem, namely:

1. The Impact of Personal Data Theft in the Current Era of Information Technology Progress?
2. What is the strategy for dealing with personal data theft in the era of advances in information technology in Indonesia?

RESEARCH METHODS

The method used in this research is Normative which sets a legal problem within the framework of Norm studies, using a statutory approach, a history approach and a philosophical approach.

DISCUSSION

The Impact of Personal Data Theft in the Current Era of Information Technology Advances

Cybercrime is a serious threat in today's digital era and involves a series of criminal activities carried out using information technology and computer networks. The background to cybercrime involves several factors that reflect technological evolution and social dynamics. The following are some background aspects of cybercrime. Developments in information technology, including the internet,*cloud computing,* and artificial intelligence, have opened up new opportunities for innovation and global connectivity.

[3] https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah

However, on the other hand, this also creates opportunities for cybercriminals to access, steal and damage data in more sophisticated ways. An increasingly globally connected world facilitates the exchange of data and information worldwide. This success also carries risks, because cyber attacks can quickly spread across a country's national borders and create widespread impacts. Many cyber attacks are carried out with economic motives, such as theft of personal data, business information, or those related to finance.

Cybercriminals may seek financial gain through the sale of stolen information. The inequality in security conditions between the attacking party and those being attacked creates gaps that can be exploited by criminals. Organizations with weak security or systems that have not been updated can be the culprit and an easier target to penetrate. Many parties feel that they are less aware of cyber security risks or do not implement adequate security practices.

This lack of awareness can provide an opening for criminals in cyberspace to commit criminal acts of theft of personal data. Cybercrime can also have political and national security dimensions, including attacks on critical infrastructure, such as financial, power, or communications systems, which can have a serious impact on a country's stability.[4]

Personal data leaks can have a serious impact on the Indonesian economy, both at the individual, business and country levels as a whole. Personal data leaks can result in direct financial loss for individuals. Data such as stolen credit card or bank account information can be used to commit fraud, illegal transactions, or other unauthorized uses, causing financial loss on an individual level. Businesses that fall victim to personal data leaks can suffer significant financial losses and a bad reputation.

Consumer trust in the company can be eroded, which can result in decreased sales and loss of customers/consumers. Personal data leaks can cause operational disruptions, as companies must spend more resources to address the security and recovery impacts of data leaks. This can hamper productivity and business growth in Indonesia. Personal data leaks can create distrust and concern among the public and foreign investors regarding the security of their data when carrying out business activities in Indonesia. This can reduce consumers' enthusiasm for using online services or sharing personal information optimally.

Foreign companies will be encouraged to increase investment in security systems and data protection, which may lead to increased operational costs. These increased costs can affect a company's profitability and shrink the resources that can be used for innovation or development. Poor data security can create uncertainty for foreign investors who may be reluctant to invest in countries with high cybersecurity risks.

[4] R A Agustian and J D N Manik, "Tindak Pidana Informasi Elektronik Dalam Kerangka Hukum Positif," *PROGRESIF: Jurnal Hukum* (scholar.archive.org, 2021), https://scholar.archive.org/work/fenzcm7zxne2res4jixnl2t6fy/access/wayback/https://www.journal.ubb.ac.id/index.php/progresif/article/download/2236/1499/.

This can affect the flow of foreign direct investment *(Foreign Direct Investment/FDI)* to Indonesia.[5]

Cyber attacks targeting state financial institutions/institutions can threaten the stability of the financial sector. Theft of financial data or attacks on payment systems can create economic instability at the national level. Personal data leaks involving government services can undermine public trust in the government. This could hamper the success of government digital programs and cause public dissatisfaction. Therefore, personal data protection is critical to maintaining individual security, business and economic stability. Efforts to protect data and good cyber security must be a priority for companies, governments and society in order to overcome the threat of personal data leakage.[6]

Personal data leaks can have a serious impact on the Indonesian economy, both at the individual, business and country levels as a whole. Personal data leaks can result in direct financial loss for individuals. Data such as stolen credit card or bank account information can be used to commit fraud, illegal transactions, or other unauthorized uses, causing financial loss on an individual level.

Businesses that fall victim to personal data leaks can suffer significant financial and reputational losses. Consumer trust in the company can be eroded, which can result in decreased sales and lost customers. Personal data leaks can cause operational disruptions as companies have to spend resources to address the security impact and recover from attacks. This can hinder productivity and business growth.[7]

Personal data leaks can create distrust and concern among people regarding the security of their data. This can reduce consumers' enthusiasm for using online services or sharing personal information online. Companies and organizations will be encouraged to increase investment in security systems and data protection, which may lead to increased operational costs. These increased costs can affect a company's profitability and shrink the resources that can be used for innovation or development.[8]

Cyber attacks targeting financial institutions can threaten the stability of the financial sector. Theft of financial data or attacks on payment systems can create economic instability at the national level. Personal data leaks involving government services can undermine public trust in the government. This could hamper the success of government digital programs and cause public dissatisfaction. Therefore, personal data protection is critical to maintaining individual security, business and economic stability. Efforts to protect data and good cyber security must be a priority for

[5] A A Pangindoman, "Penyelesaian Hukum Tindak Pidana Financial Technology Sebagai Upaya Perlindungan Hukum Bagi Konsumen Pengguna Pinjaman Dana Online," *Lex Lata*, 2021, http://journal.fh.unsri.ac.id/index.php/LexS/article/view/1184.

[6] R P Saputra, "Perkembangan Tindak Pidana Pencurian Di Indonesia," *Jurnal Pahlawan*, 2019, http://journal.universitaspahlawan.ac.id/index.php/jp/article/view/573.

[7] H A Sutiawan, E Mulyati, and I Tajudin, "Perlindungan Nasabah Terkait Praktik Pembukaan Rahasia Bank Oleh Pegawai Bank Dalam Proses Penegakan Hukum Tindak Pidana Pencucian Uang …," *Jurnal Hukum & Pembangunan* (academia.edu, 2018), https://www.academia.edu/download/70367196/1502.pdf.

[8] D Arianti and H Muhammad, "Etika Komunikasi Bisnis Online Di Era New Normal Perspektif Hukum Bisnis Islam," *... Studi Hukum ...*, 2021, http://ejournal.staidarussalamlampung.ac.id/index.php/assalam/article/view/207.

companies, governments and society in order to overcome the threat of personal data leakage.

In line with the development of information technology and the increasing need to protect personal data, many countries, including Indonesia, have taken steps to develop laws and regulations that specifically regulate the use of technology and the protection of personal data. Several legislative developments related to technology and personal data protection in Indonesia include Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE).

The ITE Law is the initial law in Indonesia that regulates electronic transactions and touches on certain aspects of electronic data protection. Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (PP PSTE) PP PSTE provides a more detailed framework regarding the implementation of electronic systems and transactions. It also refers to the protection of personal data and requires the processing of personal data in accordance with certain principles.

Law Number 19 of 2016 concerning Copyright (Copyright Law) covers aspects of copyright protection in the digital and electronic world, which involves data protection for creative works and other intellectual property rights.

Global recognition of the right to privacy is also regulated in the Universal Declaration of Human Rights (UDHR), which states explicitly that the right to privacy is included in one of the most fundamental human rights. Article 12 states that no one can be disturbed regarding their personal affairs, indeed not explicitly. expressly mentions personal data but this article becomes *"umberella terms"* because this article is related to other articles.[9]

Apart from that, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) is the same as Article 12 of the UUDHR. The difference between these two articles is paragraph 2 of Article 17 of the ICCPR which emphasizes the protection of the right to privacy. However, it is not explicit that personal data is part of the right to privacy, but the United Nations Human Rights Committee (HRC) has provided detailed guidelines to provide a detailed explanation of the scope of the right to privacy. This explanation is contained in*CCPR General Comment No.16 : Article 17 (right to privacy)*.

This development reflects global awareness of the importance of protecting personal data in the digital era. This law aims to create clear standards and guidelines for organizations to ensure that personal data management is carried out with a high level of ethics, integrity and security. The crime of personal data theft refers to all forms of action aimed at obtaining or accessing someone's personal information without permission/illegally or with bad intentions. This may involve illegal harvesting of data, unauthorized access to systems or databases, or use of such information for personal gain or other crimes. Some forms of criminal acts of theft of personal data involve penetrating or accessing without permission to a computer system or network to steal personal data stored therein.

[9] Eliezer Nathaniel and I Gede Putra Ariana, "Data Pribadi Pengguna Layanan Jejaring Layanan" 9, no. 7 (n.d.).

The act of stealing personal data from a company or institution database, either through hacking methods (*hacking)* or access fraud.**Phishing/**Using manipulative social techniques to persuade individuals to provide personal information, such as passwords or credit card numbers, by posing as a trusted entity.**Use of Malicious Software (Malware)**Personal data theft can be carried out through the use of malicious software such as viruses, trojans or ransomware to access or damage data. Attacks on network infrastructure leading to illegal access to personal data or attacks on critical information systems.[10]

The act of illegally selling personal data to third parties, who can then use the data for harmful purposes.**Identity Fraud:** Using other people's personal information for fraudulent purposes or other illegal activities. Theft of electronic devices such as laptops, smartphones, or tablets that contain personal data can be a physical form of data theft. personal data theft involving a major hack or attack on a large organization that stores the personal information of thousands or millions of people. Accessing an unsecured network or Wi-Fi to steal personal data sent over that network.

Many countries have laws and regulations that state that theft of personal data is illegal and can be subject to criminal sanctions. These penalties may include fines, imprisonment, or other sanctions, depending on the jurisdiction and the level of harm caused by the act. Therefore, personal data protection and cyber security are very important in preventing and overcoming this criminal act.[11]

Strategy for Overcoming Personal Data Theft in the Era of Information Technology Advances in Indonesia

The development of criminal law in Indonesia always follows the evolution of crime in society, with the process of forming and drafting criminal law referring to applicable legal principles, values and theories. Currently, there is significant progress in the field of information technology which has a broad influence on various aspects of Indonesian society's life. The focus of this research is the impact of developments in information technology on the crime of theft of personal data and formal obstacles in enforcing criminal law to combat this crime. The impact of these conditions means that criminal law enforcement against acts of theft of personal data cannot be implemented optimally.

This is due to the general nature and lack of criminal provisions in several laws and regulations under the Law.[12] This limitation is contained in the legal regulations in Indonesia, which stipulate that criminal provisions can only be contained in Laws, Provincial Regional Regulations, or Regency/City Regional Regulations, as regulated in Article 15 of Law of the Republic of Indonesia Number 15 of 2019 concerning Amendments to Law Number 12 of 2011 concerning the Formation of Legislative Regulations.

[10] Saputra, "Perkembangan Tindak Pidana Pencurian Di Indonesia."

[11] H B Setiawan and F U Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data," *Jurnal* ... (download.garuda.kemdikbud.go.id, 2022), http://download.garuda.kemdikbud.go.id/article.php?article=3034567&val=20674&title=Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data.

[12] K Benuf, "Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi," *Majalah Hukum Nasional*, 2021, http://mhn.bphn.go.id/index.php/MHN/article/view/148.

In other words, the regulations regarding personal data protection currently regulated in the ITE Law are general in nature, and laws and regulations under this law cannot include provisions for criminal sanctions. Therefore, this is a formal obstacle in enforcing criminal law against crimes of personal data theft in Indonesia. Currently, criminal law enforcement in Indonesia is still very tied to formal positivistic nuances, where implementation is based on existing criminal law regulations. It has also been explained previously that current criminal law is still based on the principle of formal legality.

Therefore, criminal law enforcement against crimes of personal data theft in Indonesia must follow the applicable criminal law provisions. One of the crucial elements in enforcing criminal law against crimes of personal data theft in Indonesia is the element of unlawful acts. The existence of this element of unlawful conduct is very important in the context of criminal law enforcement, considering that almost all criminal acts must fulfill this element. [13]

Even though there is an expansion of meaning regarding elements of unlawful acts, in practice, courts often have to specify the articles and laws that were violated in the criminal act. Thus, in the context of the crime of personal data theft in Indonesia which has not been specifically regulated in a personal data protection law, there are formal obstacles in enforcing criminal law. If there is a special law regarding the crime of theft of personal data in Indonesia, such as the case of the theft of personal data of Tokopedia consumers by Fintech producers, then the legal process can be carried out without any formal obstacles, whether administrative, civil or criminal.

Criminal law has the characteristics of "ultimum remedium" which involves philosophical considerations, ethics and principles of justice in structuring the criminal law system. The basic idea behind "ultimum remedium" is the need to maintain justice in the criminal law system. In order to achieve justice, the use of criminal law must be balanced and in accordance with the level of error committed by the individual. Excessive application of criminal law can endanger the "human rights" of a nation because it seems very repressive. Therefore, this principle was born as an effort to ensure that criminal law actions do not violate constitutional rights of citizens.

Focusing on prevention and rehabilitation, punishment should not only punish, but also provide opportunities for recovery and reconciliation. The use of criminal law as a final solution reflects a country's desire to ensure efficiency and effectiveness in the criminal justice system. Taking into account other alternatives first through administrative and civil measures, the system can be run more efficiently. The principle of "ultimum remedium" aims to achieve a balance between the protection of society, individual rights, and the efficiency of the criminal justice system. This principle emphasizes the importance of understanding criminal law policies to ensure that the use of criminal sanctions always takes into account the principles of justice and human rights.[14]

[13] A P Arzita, *Penegakan Hukum Terhadap Pencurian Data Pribadi Pengguna Provider* (digilib.unila.ac.id, 2019), http://digilib.unila.ac.id/58274/.

[14] D Bunga, "Politik Hukum Pidana Terhadap Penanggulangan Cybercrime," *Jurnal Legislasi Indonesia* (download.garuda.kemdikbud.go.id, 2019),

The act of theft of personal data is carried out through electronic media, so this crime is known as information technology law, cyber law and mayantara law. Overcoming personal data theft in the era of advances in information technology in Indonesia requires a holistic and sustainable approach. Here are some strategies that governments, companies and individuals can adopt to improve personal data protection:

1. Strengthening Regulations and Compliance withUpdate and strengthen laws and regulations relating to personal data protection. Ensure that the organization complies with existing regulations and imposes strict sanctions for violations.
2. Public Education and Awareness withPromote public awareness campaigns about the importance of protecting personal data and how to avoid actions that could obtain data illegally. Providing education about cyber attacks, phishing, and good cyber security practices in the community.
3. Strengthening System Security Protection withImplement the latest security technology, such as firewalls, encryption, and sophisticated security software and carry out regular software updates to address security gaps that may be exploited by criminals.[15]

Apart from that, Indonesia has Law Number 27 of 2022 concerning personal data protection, which has sociological reasons, the formulation of regulations regarding Personal Data Protection can be understood as a response to the need to protect the rights of individuals in society related to collection, processing, management. and dissemination of personal data. Adequate protection efforts for data and individual privacy will bring people's trust in providing personal information for the public interest without fear of misuse or violating their personal rights. Therefore, it is hoped that this regulation can create a balance between individual rights and the interests of society represented by the state. In this context, Personal Data Protection regulations are expected to make a significant contribution to creating order and progress in the information society.[16]

However, from a sociological perspective, it appears that Indonesian society may not fully or have little respect for privacy because these values are not yet fully embedded in Indonesian culture. Although sociologically, society also has values of respect for the continuity of attitudes and actions that are in accordance with norms in society, without disrupting or disrupting the lives of each individual as part of society. Actions that violate privacy are often considered inappropriate or even contrary to the noble values of the nation and state.

In fact, there is public awareness and expectations regarding the protection of privacy and personal data, as seen in the survey results. However, neglect of privacy

http://download.garuda.kemdikbud.go.id/article.php?article=949835&val=14663&title=POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME.

[15] W Ulya, "Perlindungan Hukum Bagi Pelaku Usaha Pada Transaksi Bisnis Social Commerce TikTok Shop (Perspektif Hukum Positif Dan Hukum Islam)," *Journal of Indonesian Comparative of Syari'ah …*, 2023, https://ejournal.unida.gontor.ac.id/index.php/jicl/article/view/9746.

[16] sociological basis for the formation of legislation number 27 of 2022 concerning personal data protection

protection and lack of public awareness of the importance of protecting their privacy provide opportunities for violations and misuse of personal data. The case of buying and selling citizen data in Indonesia, which is then used for marketing practices for various products, reflects the fragmentation of data use in various sectors, showing the need for stronger awareness and protection in society. The juridical basis for the formation of the Law on Personal Data Protection is found in Article 28G of the 1945 Constitution of the Republic of Indonesia.

Therefore, Personal Data Protection is considered an implementation of the constitutional mandate and must be regulated through the existence of a Law. Article 28G of the 1945 Constitution of the Republic of Indonesia, the Fourth Amendment, emphasizes that every individual has the right to be protected in terms of privacy, family, honor, dignity and property under his or her control. Apart from that, individuals also have the right to feel safe and protected from threats or fear of carrying out or not carrying out an action, all of which are human rights.

This article emphasizes the need to establish laws and regulations that can protect personal data. Constitutional Court decision Number 006/PUU-I/2003 further confirms that regulations related to Personal Data Protection must be regulated in the form of a law.[17] In this decision, it is explained that all provisions relating to Human Rights (HAM) must be regulated through a higher legal instrument, namely the Law. This confirms that the establishment of Personal Data Protection regulations must also comply with higher legal procedures, in accordance with human rights principles.

Law Number 27 of 2022 provides a legal umbrella for the protection of personal data which carries a specific criminal threat as regulated in chapter XIV articles 67 to article 73 with the formulation of a maximum prison sentence of 6 years and/or a maximum fine of 6 billion rupiah. Apart from that, this law provides a special criminal threat for corporate actors in article 70 which states that the fine imposed on corporations is only a fine and a maximum of 10 (ten times) the maximum fine that is threatened, apart from that it can be punished . Additional punishment as intended in articles 67 and article 68 is in the form of confiscation of profits and/or assets obtained from criminal acts and payment of compensation.

CONCLUSION

Personal data leaks can have a serious impact on the Indonesian economy, both at the individual, business and country levels as a whole. Personal data leaks can result in direct financial loss for individuals. Data such as stolen credit card or bank account information can be used to commit fraud, illegal transactions, or other unauthorized uses, causing financial loss on an individual level. Businesses that fall victim to personal data leaks can suffer significant financial and reputational losses. Consumer trust in the company can be eroded, which can result in decreased sales and lost customers.

Personal data leaks can cause operational disruptions as companies have to spend resources to address the security impact and recover from attacks. This can hamper

[17] juridical basis for the formation of legislation number 27 of 2022 concerning personal data protection

business productivity and growth. Personal data leaks can create distrust and concern among people regarding the security of their data. Overcoming personal data theft in the era of advances in information technology in Indonesia requires a holistic and sustainable approach.**with**strengthen laws and regulations relating to personal data protection. Promote public awareness campaigns about the importance of protecting personal data and how to avoid actions that could obtain data illegally.

And Implementing the latest security technology, such as firewalls, encryption, and sophisticated security software and Carrying out regular software updates to address security gaps that may be exploited by criminals. And other preventive efforts related to people's personal data.

The need to increase the quality of public and human resource awareness regarding the impact of personal data leaks is a crucial step to protect individuals and strengthen overall information security. Widespread outreach campaigns through mass media, the internet and social campaigns to increase understanding of the risks of data leaks and how to protect personal information.

There is a need to conduct more specific studies and make comparisons regarding strategies for handling cases of personal data leakage in other developed countries. So it will strengthen the state's steps to tackle personal data crime.

REFERENCES

Agustian, R A, and J D N Manik. "Tindak Pidana Informasi Elektronik Dalam Kerangka Hukum Positif." *PROGRESIF: Jurnal Hukum*. scholar.archive.org, 2021. https://scholar.archive.org/work/fenzcm7zxne2res4jixnl2t6fy/access/wayback/https://www.journal.ubb.ac.id/index.php/progresif/article/download/2236/1499/.

Arianti, D, and H Muhammad. "Etika Komunikasi Bisnis Online Di Era New Normal Perspektif Hukum Bisnis Islam." *... Studi Hukum ...*, 2021. http://ejournal.staidarussalamlampung.ac.id/index.php/assalam/article/view/207.

Arzita, A P. *Penegakan Hukum Terhadap Pencurian Data Pribadi Pengguna Provider*. digilib.unila.ac.id, 2019. http://digilib.unila.ac.id/58274/.

Benuf, K. "Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi." *Majalah Hukum Nasional*, 2021. http://mhn.bphn.go.id/index.php/MHN/article/view/148.

Bunga, D. "Politik Hukum Pidana Terhadap Penanggulangan Cybercrime." *Jurnal Legislasi Indonesia*. download.garuda.kemdikbud.go.id, 2019. http://download.garuda.kemdikbud.go.id/article.php?article=949835&val=14663&title=POLITIK HUKUM PIDANA TERHADAP PENANGGULANGAN CYBERCRIME.

Nathaniel, Eliezer, and I Gede Putra Ariana. "Data Pribadi Pengguna Layanan Jejaring Layanan" 9, no. 7 (n.d.).

Pangindoman, A A. "Penyelesaian Hukum Tindak Pidana Financial Technology Sebagai Upaya Perlindungan Hukum Bagi Konsumen Pengguna Pinjaman Dana Online." *Lex Lata*, 2021.

http://journal.fh.unsri.ac.id/index.php/LexS/article/view/1184.

Saputra, R P. "Perkembangan Tindak Pidana Pencurian Di Indonesia." *Jurnal Pahlawan*, 2019. http://journal.universitaspahlawan.ac.id/index.php/jp/article/view/573.

Setiawan, H B, and F U Najicha. "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data." *Jurnal ...*. download.garuda.kemdikbud.go.id, 2022. http://download.garuda.kemdikbud.go.id/article.php?article=3034567&val=20674&title=Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data.

Sutiawan, H A, E Mulyati, and I Tajudin. "Perlindungan Nasabah Terkait Praktik Pembukaan Rahasia Bank Oleh Pegawai Bank Dalam Proses Penegakan Hukum Tindak Pidana Pencucian Uang ...." *Jurnal Hukum & Pembangunan*. academia.edu, 2018. https://www.academia.edu/download/70367196/1502.pdf.

Ulya, W. "Perlindungan Hukum Bagi Pelaku Usaha Pada Transaksi Bisnis Social Commerce TikTok Shop (Perspektif Hukum Positif Dan Hukum Islam)." *Journal of Indonesian Comparative of Syari'ah ...*, 2023. https://ejournal.unida.gontor.ac.id/index.php/jicl/article/view/9746.

Winarno, A W, and A C Isradjuningtias. "Perlindungan Hukum Pelaku Usaha E-Commerce Terhadap Pelaku Pemalsuan Akun Konsumen Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 ...." *Bus. LJ*. scholar.archive.org, 2022. https://scholar.archive.org/work/pzzr53a3szbz7hfyezuhrarom4/access/wayback/https://journal.unpak.ac.id/index.php/palar/article/download/5032/pdf.

Yani, M A. "Pengendalian Sosial Kejahatan (Suatu Tinjauan Terhadap Masalah Penghukuman Dalam Perspektif Sosiologi)." *Jurnal Cita Hukum*, 2015. https://www.neliti.com/publications/95338/pengendalian-sosial-kejahatan-suatu-tinjauan-terhadap-masalah-penghukuman-dalam.