PERSONAL DATA PROTECTION AND ITS REGULATORY FRAMEWORKS UNDER CYBER LAW

Sal Sabila Khoirotunnisa Utami
Faculty of Law, Sunan Kalijaga State Islamic University
Jl. Laksda Adisucipto, Sleman, Yogyakarta, Indonesia
E-mail: salsabilanutami@gmail.com

Article

Article History:
Submitted: September 2024
Reviewed: October 2024
Accepted: December 2024
Published: December 2024

Keywords:
Cybercrime; Personal Data Protection; Regulation.

Abstract

The purpose of this research is to evaluate the effectiveness of personal data protection legislation and raise awareness among the broader community about the importance of safeguarding personal data against cybercrimes. This study employs a normative juridical approach, focusing on library research that examines secondary data and laws governing personal data protection. Additionally, the research adopts a qualitative methodology to provide an in-depth understanding of societal issues related to personal data protection by presenting findings narratively. The results indicate that personal data protection is explicitly addressed in Law No. 27 of 2022, which strengthens regulatory clarity and enforces stricter actions against violations compared to previous legal frameworks. Evidence suggests that the effectiveness of personal data protection laws has improved, as demonstrated by an increasing number of cases resolved comprehensively. Furthermore, individual preventive measures, such as vigilance and securing personal data online, are essential in mitigating cybercrimes.

A. Introduction

The development of science and technology is increasingly massive in this era of globalization. The Internet as one of the icons of the soaring technology, has given many impacts to the social life of society such as, it can be easily accessed information and easy to interact with other internet users.[1] The development of information technology has significant implications for changes in people's mindsets regarding territorial boundaries, time, values, logical thinking, work patterns, and social behavioral boundaries from manual to virtual.[2] Information technology today has a dual nature, on the one hand it contributes to the

[1] Lalu Aldi Bayu Damara, "Perlindungan Hukum terhadap Data Pribadi Konsumen dari Cyber Hacking", (Thesis, Universitas Mataram, 2019).
[2] Dian Ekawati, "Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan", UNES Law Review 1, no. 2 (2018): 157-171, https://doi.org/10.31933/law.v1i2.24.

advancement of human welfare and civilization, but on the other hand it can be used as a tool to carry out unlawful acts.[3]

Entering the era of society 5.0, the development of computer technology, telecommunications, and information cannot be denied by showing its existence. The use of this technology has accelerated rapid business growth, because various information has been presented sophisticatedly and easily obtained.[4]

The implication is that the sophistication is exploited by some individuals, so that a case called cybercrime is born. The reality is fraud, tapping other people's data, email spamming, and data manipulation with computer programs to access other people's data.[5] This certainly causes concern among the public about the security of personal data that they use for purposes on the internet such as online shopping applications, mobile banking, and social media applications. Moreover, currently many digital applications circulating on the internet ask for personal data to register an account in order to use the application. The high use of applications is partly due to the relatively high consumerist nature of Indonesian society.[6] Contrary to this, some people are less self-aware and have not been maximally careful in selecting applications to guarantee the security of their data. This is what is then exploited by certain individuals to misuse personal data. Even though they are careful, the leakage of personal data is still possible.

The absence of legislation that comprehensively discusses the protection of personal data makes this problem quite complex. Although the 1945 Constitution firmly affirms the protection of human rights, it does not explicitly regulate data protection as part of the recognition or respect of human rights, especially in the form of privacy protection. However, articles 28F and 28G (1) can be interpreted implicitly as a basis for the protection of personal data. Therefore, this is the basis for legislation, including the possibility of establishing a Personal Data Protection Law, to ensure legal certainty and protect privacy as a human right.[7]

[3] A. Aco Agus dan Riskawati, "Penanganan Kasus Cybercrime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar)", Supremasi 10, no. 1 (2016): 20-29, https://doi.org/10.26858/supremasi.v11i1.3023.
[4] Bolu HB and Djaenab, "Tinjauan Yuridis Perlindungan Data Pribadi Terkait Keboocoran Data dalam Ruang Cyber Crime", Petitum 10, no. 1 (2022): 70-76, https://doi.org/10.36090/jh.v10i1.1233.
[5] Ririn Aswandi, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan, "Perlindungan Data dan Informasi Pribadi melalui *Indonesian Data Protection System* (IDPS)", Legislatif 3, no. 2 (2020): 167-190, https://doi.org/10.15900/j.cnki.zylf1995.2018.02.001.
[6] Al Sentot Sudarwanto, Dona Budi Budi Kharisma, "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia", Journal of Financial Crime 29, no. 4 (2022): 1443-1457, https://doi.org/10.1108/JFC-09-2021-0193.
[7] Rizky P.P. Karo-Karo and Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi di Indonesia* (Bandung: Nusa Media, 2021), 34.

The issue of personal data protection is increasingly emerging along with the increasing number of mobile phone and internet users. Incidents involving personal data security breaches and resulting in fraud or crimes such as pornography have strengthened the discussion about the need for legal regulations to protect personal data.[8] Attention to the importance of protecting stolen personal data has increased when a leading social media company, Facebook, experienced a data leak caused by a security hole in its data storage system. This has made the public more aware of the need for more serious attention to the issue of personal data protection.[9] Accumulation of personal data can be done easily, for example, when consumers voluntarily provide personal information through Facebook registration forms. This is done consciously by giving consent either explicitly or implicitly.[10] The lack of regularity in the use of personal data and the lack of regulations to protect personal data from leaks in the era of society 5.0 indicate the need for clear policies in the formation of laws that specifically protect the personal data of each individual. Effective countermeasures are also needed, both through legal and non-legal means, to ensure that the development of the digital economy and society 5.0 runs smoothly.[11]

Before continuing this research further and turning it into a scientific work, the researcher first conducted research on several scientific works related to the topic. The purpose of this step is to avoid similarity in titles with previous works. The researcher conducted a literature review and found no research that is identical to the current study. However, several relevant studies were identified that support this research. One of them is a journal titled "Legal Protection of Personal Data as a Privacy Right" by Andy Usmina Wijaya from Wijaya Putra University. This research, conducted in 2021, highlights the importance of legal protection for personal data as a constitutional right for citizens, as outlined in Article 28G, paragraph 1 of the Indonesian Constitution.

In addition, another study titled "Cyber Law and Data Privacy: An Analysis of Global Legal Frameworks" by Sarah K. Johnson in 2020 discusses comparative approaches to personal data protection across jurisdictions and emphasizes the challenges posed by the digital age. This work provides insights into how Indonesia can strengthen its legal framework

[8] Badan Pembinaan Hukum Nasional, "Naskah Akademik RUU Perlindungan Data Pribadi", June 15, 2021, https://bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf, accessed on 20 September 2024.
[9] Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia", Fiat Justicia 12, no. 3 (2018): 206-223, https://doi.org/10.25041/fiatjustisia.v12no3.
[10] *Ibid.*
[11] Muhammad Hasan Rumlus and Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik (Policy The Discontinuation of Personal Data Storage in Electronic Media)", Jurnal HAM 11, no. 2 (2020): 288, http://dx.doi.org/10.30641/ham.2020.11.285-29.

for personal data protection by learning from international best practices. By reviewing multiple relevant studies, this research positions itself as a significant contribution to the academic discussion on personal data protection and its legal implications.

This article will discuss the importance of protecting personal data from cyber crime and legal protection efforts that can be made for internet users who use personal data in using these digital applications as well as the effectiveness of the laws that regulate as the spearhead of this fairly complex problem.

B. Method

Research methods refer to the processes used to explore, discover, and analyze information with the ultimate goal of compiling a report to achieve a stated goal. In this research, the methodology used is as follows:

1. Normative Juridical Approach

   This research employs a normative juridical approach, which involves conducting library legal research by examining secondary data, such as legal texts, regulations, and scholarly works. This approach is used to explore and analyze the existing legal framework surrounding personal data protection in Indonesia, focusing primarily on legislative texts and related legal materials.

2. Qualitative Approach

   The research also utilizes a qualitative approach, which aims to explore societal issues related to personal data protection in a deeper, more comprehensive manner. Rather than relying on statistical data, the qualitative approach emphasizes understanding the meaning, reasoning, and context behind legal and social phenomena. This method allows for a detailed narrative presentation of the issues, providing a holistic view of the challenges and developments in personal data protection.

By combining both normative juridical and qualitative methodologies, this research seeks to evaluate the effectiveness of personal data protection laws and raise public awareness regarding the importance of safeguarding personal data from cybercrimes. The analysis draws on various secondary sources, including legislation, case law, and academic studies, to provide a comprehensive understanding of the current state of personal data protection in Indonesia.

C. Analysis and Discussion

1. Cyber Legal Protection and Regulation of Personal Data

The era of globalization shows a phenomenon where the increasingly tight integration between telecommunications and information technology (global communication networks) has made the internet increasingly popular, so that the world feels smaller and the boundaries of countries and the sovereignty of their people are increasingly blurred.[12] Unfortunately, the dynamic changes in Indonesia as a country that is still in the stage of industrial and information development, do not seem fully ready to follow the progress of this technology. The influence of the internet is very significant for Indonesian society, as a developing country, and indirectly affects the daily lives of the people themselves.[13]

Aspects of life related to the use of computer equipment are closely related to data, and therefore, data integrity (data that can be trusted), data confidentiality (data that should not be accessed by the public), data exclusivity (the ability to deny unauthorized access to data), and consistent availability of computer data (data must always be accessible to computer users) are important. Computer-related crimes are one form of modern crime committed by professionals and criminals in the scope of "white crime".[14] This kind of crime is not done with violence or complex equipment, but by using telecommunications and information technology devices that are capable of processing millions of data every second. It can also be used to damage information data, which can result in major losses or even endanger the security of society or the state.[15]

Cybercrime has also caused significant financial losses as a direct result of the irresponsible use of communication and information technology facilities, which are ultimately difficult to trace. The public believes that this potential loss is the most crucial aspect of this crime, especially in terms of financial activities in the banking sector, national security, and other important domains. In addition to the financial impact, there are other interests that require protection, such as individual personal data, scientific information, state security, and confidential information related to government administration and crucial documents.[16]

---

[12] Abraham Ethan Martupa Sahat Marune, Brandon Hartanto, "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective", International Journal of Business, Economics, and Social Development 2, no. 4 (2021): 143-152, https://doi.org/10.46336/ijbesd.v2i4.170.
[13] Abdul Halim Barkatullah, *Hukum Transaksi Elektronik (Sebagai Panduan dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia)* (Bandung: Nusa Media, 2017), 4.
[14] *Ibid*, 7.
[15] *Ibid.*
[16] *Ibid.*

The development of personal data protection regulations has grown in line with technological advances, especially in the field of information and communication technology. Data protection regulations emerged in Europe in response to the lack of a clear definition of privacy and private life, which is regulated by Article 8 of the European Convention. This right to data protection is designed to protect individuals in the information society era. Germany was the first country to pass a Data Protection Act in 1970, followed by the United Kingdom and a number of other European countries such as Sweden, France, Switzerland, and Austria. In the United States, a similar development was seen in the Fair Credit Reporting Act in 1970, which also included aspects of data protection.[17]

Violation of personal data on the internet is one form of cyber privacy violation. This form of crime targets a person's highly confidential and sensitive personal information. Generally, this crime targets personal information stored in computerized data forms, which if known by other parties can harm the victim both materially and immaterially, such as credit card numbers, ATM PINs, personal medical information, and the like.[18]

Based on Law Number 27 of 2022 concerning Personal Data Protection, Article 1 paragraph (1) explains that "Personal Data is information about a person that can be identified directly or indirectly through an electronic or non-electronic system." This law was created because personal data protection is considered an important human right in maintaining individual privacy, so a legal basis is needed to secure such personal data. Based on the 1945 Constitution of the Republic of Indonesia, personal data protection aims to guarantee the individual's right to privacy and to increase public awareness of the importance of personal data protection. Currently, regulations regarding personal data have been regulated in several laws and regulations, but to increase the effectiveness of personal data protection, regulations in the law are specifically needed.[19]

Personal data is a sensitive thing that everyone has. Personal data is a person's privacy right that must be protected from various aspects of life. Protection of personal data privacy is a basic principle of a person's personality.[20] Personal data privacy is a constitutional right of every citizen, so this regulation is a form of respect and protection of this right. Regulations that protect personal data privacy can have a positive impact, including increasing Indonesia's

[17] Wahyudi Djafar, "Hukum Perlindungan Data Pribadi di Indonesia: "Tantangan Hukum dalam Era Analisis Big Data", (Thesis, Universitas Gadjah Mada, 2019).
[18] Ibrahim Fikma Edrisy, *Pengantar Hukum Siber* (Lampung: Sai Wawai Publishing, 2019), 7.
[19] Central Government Indonesia, Law Number 27 of 2022 concerning Personal Data Protection (2022).
[20] Sinta Dewi Rosadi, "Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia", Brawijaya Law Journal 5, no. 1 (2018): 143-157, http://dx.doi.org/10.21776/ub.blj.2018.005.01.09.

economic value in the global market. Protection of personal data confidentiality from a comparative law perspective places the right to privacy as one of the constitutional rights of citizens so that the form of respect and protection of this constitutional right is specifically regulated and a special supervisory body is formed or appointed to ensure the implementation of the personal data privacy law.[21] Efforts and policies to create good criminal law regulations are basically inseparable from the goal of combating crime. Thus, criminal law policies or policies are also part of criminal politics.[22]

Personal data consists of specific personal data and general personal data. Specific personal data as referred to in Article 4 paragraph (1) letter a of Law Number 27 of 2022 concerning Personal Data Protection, the category of personal data includes: health information, biometric data, genetic data, criminal records, child data, personal financial data, and/or other data stipulated by laws and regulations. While general personal data as described in paragraph (1) letter b includes: full name, gender, nationality, religion, marital status, and/or personal data combined to identify a person. Although everyone has the right to obtain correct information from electronic media, clear restrictions are needed that the use of information in electronic media involving customer data in fund transfers constitutes a violation of bank confidentiality. Misuse of credit cards via the internet has raised new problems, whether credit card numbers should be explicitly stated as part of bank secrecy. Currently, there is a phenomenon that is very disturbing for credit card organizers and customers, where credit card data tapping tools have become so easy to obtain.[23]

The challenge in implementing and enforcing the law against cybercrime lies in the difficulty in resolving the case. This condition, which fully uses technology (paperless), creates difficulties in collecting evidence related to information that is processed, stored, or sent electronically. The use of electronic evidence in the process of proving criminal acts, especially due to the lack of a clear legal basis for the use of electronic evidence in legislation, is a fundamental issue.[24] In addition, the difficulty in identifying perpetrators and certain

[21] Mays Amelia and Tomy Michael, "Protection of Personal Data in the Care Application", Journal of International Trade, Logistic and Law 8, no. 1 (2022): 23-27, https://www.jital.org/index.php/jital/article/view/259.
[22] Ahmad Bahiej and Ach. Tahir, "Kebijakan Penanggulangan Kejahatan Studi Terhadap Resolusi Kongres Pbb Viii/1990 Tentang Computer-Related Crime", Asy-Syir'ah 46, no. 11 (2012), 641-664, https://doi.org/10.14421/ajish.v46i2.54.
[23] Ahmad M. Ramli, *Hukum Telematika* (Tangerang: Universitas Terbuka, 2020), 9-10.
[24] Diana Setiawati, Hary Abdul Hakim, Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore", Indonesia Comparative Law Review 2, no. 2 (2020): 95-109, https://doi.org/10.18196/iclr.2219.

crimes that are often difficult to prove, creates its own challenges in enforcing the law related to cybercrime.[25]

According to the provisions of Article 65 paragraph 1-3 of Law No. 27 of 2022 concerning Personal Data Protection, it is clearly stated that (1) the act of obtaining or collecting Personal Data that does not belong to him/her with the aim of benefiting oneself or others that can harm the Personal Data Subject is prohibited by law; (2) disclosing Personal Data that does not belong to him/her unlawfully is also prohibited; and (3) using Personal Data that does not belong to him/her without permission is an unlawful act. In addition, Article 66 emphasizes that creating false Personal Data or falsifying Personal Data with the intention of benefiting oneself or others that results in harming others is also prohibited. Several criminal provisions against someone who violates personal data, at least for now, there are statutory regulations contained in Law No. 27 of 2022 concerning Personal Data Protection in Article 67, namely.[26]Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him/her with the intention of obtaining personal gain or for another person that may be detrimental to the subject of the personal data, as explained in Article 65 paragraph (1), will be subject to a maximum prison sentence of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

(1) Any individual who intentionally and unlawfully discloses personal data that is not his/hers as described in Article 65 paragraph (2) shall be subject to a maximum prison sentence of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000.00 (four billion rupiah). In addition, individuals who intentionally and unlawfully use personal data that is not his/hers as described in Article 65 paragraph (3) shall be subject to a maximum prison sentence of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah).

Other criminal provisions including if the perpetrator of the crime is a corporation are also regulated in this Law from Article 68 to Article 73. Law number 27 of 2022 is a breath of fresh air that is used as a reinforcement and explanation of the previous legislation that was still vague. The strengthening of this legislation is expected to become a fortress for the wider community so that they can more easily obtain their rights if something happens to their data. It is hoped that with the existence of these criminal provisions, someone can be more careful and not become a perpetrator of the crime.

The growing challenges in enforcing personal data protection laws arise not only from technological advancements but also from the lack of clear and effective mechanisms for

[25] Sahat Maruli T. Situmeang, *Cyber Law* (Bandung: CV. Cakra, 2020), 42.

[26] Central Government Indonesia, *Loc.Cit.*

holding violators accountable.[27] One significant obstacle is the transnational nature of cybercrimes, where perpetrators may operate from jurisdictions with weak or underdeveloped laws, making it difficult for Indonesian authorities to prosecute these crimes effectively. Furthermore, the anonymity offered by digital platforms exacerbates the difficulty of identifying offenders, and in many cases, criminal activities may be conducted through encrypted channels that are difficult to trace or monitor.[28] In light of this, Law No. 27 of 2022 introduces provisions aimed at addressing these complexities by enhancing data security and establishing clear guidelines for handling breaches. However, enforcement mechanisms still face significant barriers, particularly when dealing with cross-border data transfers and the enforcement of penalties in international contexts. International cooperation and harmonization of data protection laws could play a vital role in tackling these issues more effectively.[29] As seen in Europe, with the General Data Protection Regulation (GDPR), countries that share a commitment to protecting personal data may work together more seamlessly to hold offenders accountable across borders.[30] Additionally, the increasing sophistication of cybercrimes underscores the need for continued advancements in technology, both for preventive measures and for tools that can aid in the detection and prosecution of data violations. The integration of Artificial Intelligence (AI) in monitoring and securing personal data is one promising development that could significantly improve the enforcement of personal data protection laws. AI-driven systems can be used to detect unusual patterns of data access, identify potential security vulnerabilities, and even predict where breaches may occur, allowing authorities to respond proactively rather than reactively. Lastly, public awareness remains a critical component in safeguarding personal data. While the legislation, including Law No. 27 of 2022, provides a legal framework for protecting data, individual vigilance is also necessary. Public education campaigns that teach citizens how to safeguard their personal data, identify phishing attempts, and use secure communication channels are essential in reducing the risk of personal data misuse. A well-informed public is

[27] Andriyanto Adhi Nugroho, Atik Winanti, Surahmad Surahmad, "Personal Data Protection in Indonesia: Legal Perspective", International Journal of Multicultural and Multireligious Understanding 7, no. 7 (2020): 183-189, http://dx.doi.org/10.18415/ijmmu.v7i7.1773.
[28] H Kusnadi, *Perlindungan Data Pribadi di Indonesia* (Yogyakarta: Pustaka Hukum, 2021), 59.
[29] Yohanes Leonardus Ngompat and Mary Grace Megumi Maran, "Legal Development and Urgency of Personal Data Protection in Indonesia", Indonesia Law and Policy Review 5, no. 3 (2024): 627-635, https://doi.org/10.56371/jirpl.v5i3.284.
[30] Central Government Indonesia, *Loc.Cit.*

one of the strongest defenses against cybercrimes, as it minimizes the potential for exploitation by malicious actors.[31]

2. Cases of Personal Data Leaks in Indonesia

Data leak cases in Indonesia are no longer a secret, because cybercrime cases against personal data protection do not only attack personally, but have even spread to the corporate sector which of course has been fortified with a qualified level of security. The reality is that cybercrime is indeed endless, several cases of personal data leaks that have occurred in Indonesia are presented in the table below:

Table 1.

Types of Data Leak Cases and Their Regulations

Case	Regulation	Resolution of the Case
Facebook User Data Leak Case (2018): Although this is an international case, Facebook user data in Indonesia was also affected.	Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Protection of Personal Data.	Indonesia took limited action to demand accountability from Facebook. No specific penalties or user compensation reported. Efforts are ongoing to align global tech practices with Indonesian regulations.
BPJS Health Data Leak Case (2018): In 2018, there was a data leak case from the Social Security Administering Agency (BPJS) Health, which resulted in personal data of BPJS participants being	Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and Government Regulation Number 82 of 2012 concerning Protection of Personal Data in Electronic Systems.	Government Regulation Number 82 of 2012 concerning Protection of Personal Data in Electronic Systems. The government initiated an investigation and strengthened BPJS system security. BPJS apologized publicly, and data protection protocols were updated. However, sanctions or compensation for affected individuals were not explicitly reported, reflecting gaps in

[31] Andi Rifky Maulana Efendy, "Towards Enhanced Personal Data Protection: A Novel Approach to Regulation and Practice in Indonesia", E-Justice 1, no. 1 (2024): 1-15, http://lenkasia.com/ejustice/article/view/2.

spread on the internet.		enforcement of personal data protection laws at the time.
General Election Commission (KPU): In May 2020, a hacker admitted to having breached the KPU and obtained the data of 2.3 million Indonesian citizens.	Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Electronic Transactions. Law Number 7 of 2017 concerning General Elections.	Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Electronic Transactions. Law Number 7 of 2017 concerning General Elections. The KPU collaborated with the Ministry of Communication and Information Technology to investigate the breach and secure its systems. The KPU stated that the leaked data was limited to publicly available information, and no sensitive data was exposed. However, this incident highlighted the need for stricter cybersecurity measures and raised public awareness about data protection during elections.
Cermati and Lazada: In July 2020, customer data of financial technology company Cermati and e-commerce platform Lazada was leaked.	Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Electronic Transactions.	Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Electronic Transactions. Both companies issued public statements acknowledging the data breach and implemented tighter security measures. Lazada specifically worked with cybersecurity firms to investigate the breach, while Cermati assured users of immediate system updates to prevent further incidents. Law

		enforcement authorities were also involved to trace the perpetrators.
MyPertamina and PeduliLindungi: In November 2022, data from several users of the MyPertamina and PeduliLindungi applications was leaked.	Law Number 11 of 2008 which regulates Electronic Information and Transactions (ITE) and Government Regulation Number 71 of 2019 which regulates the Implementation of Electronic Systems and Electronic Transactions. Law Number 19 of 2016 concerning Population Administration.	Several users of the MyPertamina and PeduliLindungi applications was leaked. - Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Electronic Transactions. Law Number 19 of 2016 concerning Population Administration. The Ministry of Communication and Information Technology (Kominfo) conducted an investigation and temporarily suspended some application features to enhance security. Public officials emphasized the importance of securing critical infrastructure and digital services. Kominfo also issued warnings to application providers to comply with national data protection standards.
Dukcapil Ministry of Home Affairs: July 2023, Data of 337 Million Indonesians Allegedly Hacked Dukcapil Ministry of Home Affairs: the law and penalties.	Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which regulates electronic data security issues, and Law Number 24 of 2013 concerning Population Administration, which relates to the	Allegedly hacked in July 2023. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE). Law Number 24 of 2013 concerning Population Administration. The Ministry of Home Affairs collaborated with cybersecurity teams and law enforcement to track

	protection of population data.	the hackers and secure the leaked data. They also initiated efforts to update the database system with stronger encryption protocols. Public campaigns were launched to educate citizens about the importance of safeguarding their personal data.
Casemanipulating electronic documents with the aim of making electronic documents.	Article 51 paragraph 1 of Law of the Republic of Indonesia No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions.	Electronic Document Manipulation Case: Manipulating electronic documents with the intention of altering or creating falsified data. | Article 51 paragraph 1 of Law of the Republic of Indonesia No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 11 of 2008 concerning Information and Electronic Transactions. The perpetrators were identified and prosecuted under the ITE Law. Law enforcement emphasized the importance of using digital forensics to collect evidence and secure convictions. Courts issued penalties in the form of fines and prison sentences depending on the severity of the manipulation and its impact.

Source: Author Self Analysis

The data above is a description of the many cases of cybercrime, especially in the protection of personal data. In line with the results of the interviews that have been conducted, sources at the Yogyakarta District Court also paid sufficient attention to cybercrime. Yogyakarta itself is still not considered too significant in terms of cybercrime cases cyber. This is validated by the small number of decisions made by the Yogyakarta District Court regarding ITE cases. However, looking at the general reality, it is important and central to

this cybercrime. The regulation of the cases presented above according to the existing literature has provided an overview of the administrative sanctions that will be obtained when someone commits a cybercrime.[32]

3. How to Protect Personal Data on the Internet

According to Law No. 1 of 2024, which amends Law No. 19 of 2016 concerning Electronic Information and Transactions, Article 1 paragraph (1) states:

> Electronic Information refers to individual or collective electronic data, including but not limited to text, sound, images, maps, designs, photos, electronic data interchange (EDI), electronic mail, telegrams, telex, facsimile, or other forms of electronic communication, symbols, signs, access codes, numbers, or perforations that have been processed to contain meaning or can be understood by individuals who are able to interpret them.

This adjustment is made to address the growing need for the protection and management of electronic information in today's digital era, while also considering technological developments and the protection of data and privacy rights.[33] Of course, it is important to know the definition so that the use of information technology is carried out safely to prevent its misuse by considering the religious and socio-cultural values of Indonesian citizens. In order realize a just rule of law, Society 5.0 requires law enforcement reform. Some forms of reform include: first, using the principle of fair law as a basis for decision-making by state officials. Second, the judiciary needs to maintain independence, impartiality, and freedom in deciding cases. Third, increasing the professionalism of law enforcement officers. Fourth, law enforcement based on the principles of justice. Fifth, advancing and protecting Human Rights. Finally, involving public participation and ensuring an effective oversight mechanism. Law enforcement in the Society 5.0 Era includes the use of the Internet of Things, allowing the public to easily access law enforcement agencies.[34] Personal data leaks on the internet, especially in e-commerce, m-banking, and social media. Of course, cause people to be vigilant and able to protect their personal data. Social media uses in an innovative and rapidly changing advanced technology environment, it is difficult to provide a detailed enough explanation to facilitate

[32] Interview with Agnes Hari Nugrahenin, Judge of Yogyakarta District Court, 20 October 2023.
[33] Central Government Indonesia, Law Number 19 of 20216 concerning Electronic Information and Transaction (2016).
[34] Ilham Wiryadi Muhammad, "Suhartoyo: Perlu Reformasi Penegakan Hukum Menghadapi Tantangan Era Society 5.0", October 31, 2021, https://www.mkri.id/index.php?page, accessed on 20 November 2022.

a long regulatory process.[35] When regulations are finally passed, products or services have often changed, especially in areas related to consumer activities that are social in nature. From the perspective of many consumers, this is relatively harmless compared to many other priorities in the criminal justice system.

Since its launch in 2004, Facebook has been embroiled in data privacy issues. The case involving Cambridge Analytica and the 2016 US presidential election is a prime example. In 2013, a psychology professor named Alexander Kogan was granted permission by Facebook to collect Facebook user data through a personality quiz app that initially seemed harmless. However, Professor Kogan later sold the data of 50 million American Facebook users to Cambridge Analytica. According to the latter's CEO, Alexander Nix, the way the information was used may have had a significant impact on the outcome of the 2016 US election.[36]

Personal data needs to be protected for certain reasons, including avoiding cases of online bullying and harassment, to prevent potential defamation, and to guarantee the right to control personal data, which has been guaranteed in the Universal Declaration of Human Rights 1948 Article 12 and the International Covenant on Civil and Political Rights (ICCPR) 1966 Article 17, various recommendations can be applied to protect personal data when using the internet. Some of these recommendations include ensuring the use of data encryption, where each site is equipped with an encryption security system to protect data when sent through the website. For example, the use of the HTTPS protocol and SSL certification. Sites that use data encryption can generally be recognized by the site address starting with "https". In addition, security can be identified by the presence of a padlock logo on the top left of the site link.

a. Please be careful when using Wi-Fi networks because these networks can be misused by irresponsible parties to steal personal data. One of the modes is through the use of fake access points that can cause theft of personal data when someone logs in. It is recommended to avoid access points that ask for personal information such as usernames, passwords, and other data.
b. In addition, it is necessary to be aware of phishing links that often use the name of a particular agency or organization. Some of these links may direct users to fake

[35] Moody Rizqy Syailendra, Gunardi Lie, and Amad Sudiro, "Personal Data Protection Law in Indonesia: Challenges and Opportunities", Indonesia Law Review 14, no. 2 (2024): 56-72, https://doi.org/10.15742/ilrev.v14n2.1.
[36] Danrivanto Budhijanto, *Cyber Law dan Revolusi Industri 4.0* (Bandung: Logoz Publishing, 2019), xi.

login pages that aim to steal personal data. It is advisable not to provide personal information to untrusted sites, and always check the site address (domain) carefully, especially for government sites that should use the ".go.id" domain.

c. It is also important to use a password that is difficult to guess and avoid using birth dates or personal names. It is recommended to change passwords regularly, at least once every three months.
d. For further security, it is recommended to use incognito mode when surfing the internet. Many advanced browsers provide this feature, which will turn off data storage while browsing. This mode prevents the browser from recording the addresses of sites and pages visited and protects personal data, such as usernames, passwords, cache, and cookies from visited websites.

D. Conclusion

Personal Data refers to information about an individual that can be identified alone or in combination with other data, either directly or indirectly, through electronic or non-electronic systems. The protection of personal data is currently detailed in Law No. 27 of 2022, which aims to clarify regulations and actions concerning perpetrators who commit crimes against personal data. This law was introduced because previous legislation was deemed insufficient in strengthening the protection of personal data.

The importance of protecting personal data is underscored by the potential risks posed by cybercrimes, particularly with the rapid technological advancements. Individuals need to be conscious of the data they share online to prevent its misuse by irresponsible parties, which could lead to harm. Despite the existence of regulations that have a significant impact on curbing cybercrime, incidents of personal data leaks continue to occur. In many cases, even corporations with credible security systems are unable to fully prevent breaches involving individuals' personal data.

Therefore, to combat cybercrime and better protect personal data, the following actions are recommended: 1) Strengthening Public Awareness, it is essential to raise public awareness about the significance of personal data protection and the role individuals play in safeguarding their own data. Public education initiatives should be implemented to enhance literacy on personal data protection, starting with individual responsibility; 2) Updating and Strengthening Regulations, Governments and regulatory bodies must continually update and enhance regulations surrounding personal data protection to keep pace with technological developments. This ensures that legal frameworks remain effective in addressing new and

emerging threats; and 3) Stronger Law Enforcement, there should be stricter enforcement of laws related to personal data breaches, including harsher penalties for companies or individuals who violate these laws. This would serve as a deterrent to those who deliberately engage in crimes related to personal data. Despite the availability of advanced security systems, cybercrimes can still occur, particularly against individuals who may have inadequate security measures in place. Personal data leaks on a large scale often originate within the corporate sector, making them more profitable for cybercriminals. The hope is that by implementing more structured sanctions, cybercrime will be minimized due to stronger deterrence and government intervention.

References

Books

Barkatullah, Abdul Halim, *Hukum Transaksi Elektronik (Sebagai Panduan dalam Menghadapi Era Digital Bisnis e-Commerce di Indonesia)*, Bandung: Nusa Media, 2017.

Budhijanto, Danrivanto, *Cyber Law dan Revolusi Industri 4.0*, Bandung: Logoz Publishing, 2019).

Edrisy, Ibrahim Fikma, *Pengantar Hukum Siber*, Lampung: Sai Wawai Publishing, 2019.

Karo-Karo, Rizky P.P. and Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi di Indonesia*, Bandung: Nusa Media, 2021.

Kusnadi, H, *Perlindungan Data Pribadi di Indonesia,* Yogyakarta: Pustaka Hukum, 2021.

Ramli, Ahmad M., *Hukum Telematika*, Tangerang: Universitas Terbuka, 2020.

Situmeang, Sahat Maruli T., *Cyber Law*, Bandung: CV. Cakra, 2020.

Journal Articles

Agus, A. Aco dan Riskawati, "Penanganan Kasus Cybercrime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kot a Besar Makassar)", *Supremasi* 10, no. 1 (2016): 20-29, https://doi.org/10.26858/supremasi.v11i1.3023.

Amelia, Mays and Tomy Michael, "Protection of Personal Data in the Care Application", *Journal of International Trade, Logistic and Law* 8, no. 1 (2022): 23-27, https://www.jital.org/index.php/jital/article/view/259.

Aswandi, Ririn Aswandi, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan, "Perlindungan Data dan Informasi Pribadi melalui *Indonesian Data Protection System* (IDPS)", *Legislatif* 3, no. 2 (2020): 167-190, https://doi.org/10.15900/j.cnki.zylf1995.2018.02.001.

Bahiej, Ahmad and Ach. Tahir, "Kebijakan Penanggulangan Kejahatan Studi Terhadap Resolusi Kongres Pbb Viii/1990 Tentang Computer-Related Crime", *Asy-Syir'ah* 46, no. 11 (2012), 641-664, https://doi.org/10.14421/ajish.v46i2.54.

Ekawati, Dian, "Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan", *UNES Law Review* 1, no. 2 (2018): 157-171, https://doi.org/10.31933/law.v1i2.24.

HB, Bolu and Djaenab, "Tinjauan Yuridis Perlindungan Data Pribadi Terkait Keboocoran Data dalam Ruang Cyber Crime", *Petitum* 10, no. 1 (2022): 70-76, https://doi.org/10.36090/jh.v10i1.1233.

Marune, Abraham Ethan Martupa Sahat and Brandon Hartanto, "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective", *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143-152, https://doi.org/10.46336/ijbesd.v2i4.170.

Natamiharja, Rudi, "A Case Study on Facebook Data Theft in Indonesia", *Fiat Justicia* 12, no. 3 (2018): 206-223, https://doi.org/10.25041/fiatjustisia.v12no3.

Ngompat, Yohanes Leonardus and Mary Grace Megumi Maran, "Legal Development and Urgency of Personal Data Protection in Indonesia", *Indonesia Law and Policy Review* 5, no. 3 (2024): 627-635, https://doi.org/10.56371/jirpl.v5i3.284.

Nugroho, Andriyanto Adhi, Atik Winanti, Surahmad Surahmad, "Personal Data Protection in Indonesia: Legal Perspective", *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (2020): 183-189, http://dx.doi.org/10.18415/ijmmu.v7i7.1773.

Rifky, Andi and Maulana Efendy, "Towards Enhanced Personal Data Protection: A Novel Approach to Regulation and Practice in Indonesia", *E-Justice* 1, no. 1 (2024): 1-15, http://lenkasia.com/ejustice/article/view/2.

Rosadi, Sinta Dewi, "Protecting Privacy On Personal Data In Digital Economic Era: Legal Framework In Indonesia", *Brawijaya Law Journal* 5, no. 1 (2018): 143-157, http://dx.doi.org/10.21776/ub.blj.2018.005.01.09.

Rumlus, Muhammad Hasan and Hanif Hartadi, "Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media)", *Jurnal HAM* 11, no. 2 (2020): 288, http://dx.doi.org/10.30641/ham.2020.11.285-29.

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore", Indonesia *Comparative Law Review* 2, no. 2 (2020): 95-109, https://doi.org/10.18196/iclr.2219.

Sudarwanto, Al Sentot, Dona Budi Budi Kharisma, "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia", *Journal of Financial Crime* 29, no. 4 (2022): 1443-1457, https://doi.org/10.1108/JFC-09-2021-0193.

Syailendra, Moody Rizqy, Gunardi Lie, and Amad Sudiro, "Personal Data Protection Law in Indonesia: Challenges and Opportunities", *Indonesia Law Review* 14, no. 2 (2024): 56-72, https://doi.org/10.15742/ilrev.v14n2.1.

Research Results

Damara, Lalu Aldi Bayu, "Perlindungan Hukum terhadap Data Pribadi Konsumen dari Cyber Hacking" (Thesis, Universitas Mataram, 2019).

Djafar, Wahyudi, "Hukum Perlindungan Data Pribadi di Indonesia: "Tantangan Hukum dalam Era Analisis Big Data" (Thesis, Universitas Gadjah Mada, 2019).

Internet

Badan Pembinaan Hukum Nasional, "Naskah Akademik RUU Perlindungan Data Pribadi", June 15, 2021, *https://bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf*.

Muhammad, Ilham Wiryadi, "Suhartoyo: Perlu Reformasi Penegakan Hukum Menghadapi Tantangan Era Society 5.0", October 31, 2021, *https://www.mkri.id/index.php?page*.

Law and Regulations

Indonesia, Central Government. Law Number 19 of 20216 concerning Electronic Information and Transaction (2016).

_____. Law Number 27 of 2022 concerning Personal Data Protection (2022).

Interview Result

Interview with Agnes Hari Nugrahenin, Judge of Yogyakarta District Court, 20 October 2023.