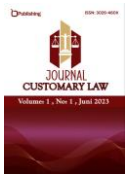

Customary Law Journal Volume: 2, Number 2, 2025, *Page*: 1-21

Personal Data Breach Cases in Indonesia: Perspective Of Personal Data Protection Law

Tanti Kirana Utami*, Salsa Octaviani Suryanto, Kayla Andini Putri, Fina Asriani

Faculty of Law, Suryakancana University

DOI:
https://doi.org/ 10.47134/jcl.v2i2.3742
*Correspondence: Tanti Kirana Utami
Email: kireinatanti78@gmail.com

Received: 11-01-2025
Accepted: 18-02-2025
Published: 25-03-2025

Abstract: This research aims to analyse the situation and frequency of personal data breach cases in Indonesia, identify the factors causing them, and evaluate the preventive efforts that have been made in the context of the Personal Data Protection Law. This research uses a mixed methods approach that combines quantitative and qualitative methods. Quantitative data was obtained through an online survey of Indonesians to measure the level of awareness and experience related to personal data breaches. Meanwhile, qualitative data was obtained through a literature study and in-depth interviews with experts in cybersecurity and law. The results show that cases of personal data breaches in Indonesia are increasing, with the main contributing factors including weak public awareness, lack of data protection by companies, and suboptimal law enforcement. Preventive efforts that need to be improved include socialisation of the Personal Data Protection Law, improving information system security, and cross-sector cooperation. This research provides recommendations for more effective policies to prevent and address cases of personal data breaches in the future.

Keywords: Breach; Cyber; Data; Personal; Protection.

Introduction

In recent decades, the world has undergone a rapid digital transformation, changing the way individuals, companies and governments manage information. Personal data, which includes any information that can directly or indirectly identify a person, has become a key component in the digital ecosystem. In Indonesia, the use of information technology has penetrated into various sectors such as banking, e-commerce, education, and public administration. This transformation allows for faster and more efficient service management, but also opens up new loopholes to potential personal data breaches and misuse. A personal data breach is an act that involves the unauthorised access, use, disclosure or dissemination of personal data, which may violate an individual's right to privacy and has the potential to cause both material and non-material losses (Karo and Prasetyo, 2020; Group, 2024). Cases of personal data breaches in Indonesia have increasingly received public attention, especially due to the high number of hacking activities that occur. This is exacerbated by the significant growth in the number of internet users in Indonesia from year to year. In 2021, internet users were recorded at 202.6 million, increasing to 204.7

million in 2022. This figure continues to jump to 221.5 million in 2023-2024, out of the total population of Indonesia in 2023. This growth in internet users illustrates a significant increase in digital activity, which in turn increases the risk of personal data breaches (Annur, 2022; APJII, 2024). In the period 2019 to 14 May 2024, the Ministry of Communication and Informatics has handled 124 alleged violations related to personal data protection, of which 111 were personal data leak cases (Leda, 2024) .

These leaks included user data from various digital platforms, such as health apps, ride-hailing services, and government agencies, exposing the weakness of Indonesia's data protection system. Some incidents even involved the theft and dissemination of sensitive data, such as identity information, medical history, and financial data, which could potentially be used for criminal offences, including fraud, identity theft, or extortion (Laksana, 2024).Personal data breach cases can be classified into different types based on how the breach occurred and the impact it has on individuals or organisations. One of the most common types is data breaches, where personal information is accessed or exposed without authorisation, usually as a result of a cyberattack, such as a hack into a company or government agency's database system. Another type is identity theft, which occurs when a person's personal data, such as identity numbers or financial information, is used illegally for fraudulent purposes or financial gain. Unauthorised data sales are also a rampant form of breach, where user data is sold to third parties, such as advertisers, without the knowledge or consent of the data owner (Kusuma, 2023).

Usually, perpetrators commit personal data breaches with various motives or backgrounds that encourage them to act illegally. One common motive is economic, where the perpetrator seeks to gain financial benefits by selling or utilizing the stolen personal data. In addition, there are also self-interested motives, such as the desire to hack into systems or access information that should be confidential (Situmeang, 2021; Naylawati Bahtiar, 2022). Not only that, but data breaches are also often influenced by various other factors that exacerbate the situation. One of them is the low awareness of the public and organizations on the importance of digital security and personal data protection and on the other hand, weak regulations related to personal data protection are also a factor that encourages the rise of this breach case (Claudia and Sitaboeana, 2021).

To prevent personal data breaches in Indonesia, the public and government need to understand the risks and complexities of such breaches, including data theft schemes, data leaks, and misuse of personal information. This requires a cross-sectoral approach involving technology, law, and improving people's digital literacy. From a legal perspective, strong regulations and effective law enforcement are needed to provide optimal protection for personal data. In this regard, Law No. 27 of 2022 on Personal Data Protection is an important milestone for strengthening the legal framework that was previously scattered in various other laws such as Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) which has been amended through Law No. 19 of 2016 (Puspitasari *et al.*, 2023). The Personal Data Protection Law aims to provide legal certainty for the protection of personal data, covering the rights of individuals to personal data and the obligation for data controllers to maintain its security. Under this regulation, any violation of personal data, such as

unauthorised access, dissemination, or misuse of data, is subject to strict administrative and criminal sanctions. This is expected to reduce data leakage incidents that often cause material and immaterial losses to individual data owners. In addition, this Law regulates the responsibility of data managers in ensuring transparency and valid consent from data owners (Puspitasari *et al.*, 2023).

Through the implementation of the Personal Data Protection Law, it is expected to encourage cooperation between the government, businesses, and the community in creating a safe digital ecosystem. Strengthening the capacity of law enforcement officials and educating the public about user rights and responsibilities related to personal data are also key steps in addressing this issue comprehensively (Farhan *et al.*, 2023). The Indonesian government's efforts to respond to this issue are starting to show with the passing of the Personal Data Protection Law in 2022. This law is designed to provide legal protection for personal data and ensure that those who manage data adhere to certain security standards. The Personal Data Protection Law regulates the rights of data subjects, the obligations of data controllers, and sanctions for violations that occur. With this regulation, it is expected that data management practices in Indonesia will become more orderly and responsible. However, the implementation of the Personal Data Protection Law does not necessarily solve all problems, considering that the challenges faced are quite complex, ranging from lack of public understanding, lack of supporting infrastructure, to a legal culture that has not fully matured (Putri, 2022).

As in previous research conducted by CSA Teddy Lesmana, Eva Elis, and Siti Hamimah on "The Urgency of Personal Data Protection Law in Ensuring Personal Data Security". This article provides an in-depth analysis of the importance of passing the Personal Data Protection Bill to ensure personal data security as part of the fulfilment of the privacy rights of Indonesian citizens. This article highlights the urgency of more specific regulations to address the legal vacuum in personal data protection amidst the increasing threat of cybercrime. Using a normative juridical research method, this article adopts a statutory, case, and comparative approach, which provides a strong theoretical foundation. However, this article has several shortcomings. Firstly, the lack of empirical data supporting the analysis causes the article to be theoretical without reinforcing the argument with field facts. Second, although the urgency of data protection is explained, the article does not offer concrete practical recommendations for steps that can be taken to accelerate the passage of the Personal Data Protection Bill. Thirdly, the article does not consider the dynamics of technological developments that affect the need for personal data protection, so its relevance to current technological conditions may be limited. The novelty theory of this article is the emphasis on the importance of harmonising Indonesian regulations with data protection policies in other countries, providing a new perspective to strengthen personal data protection at the national and international levels (CSA Teddy Lesmana, Elis and Hamimah, 2022).

Meanwhile, as in previous research conducted by Indriana Firdaus on "Legal Protection Efforts for Privacy Rights Against Personal Data from Hacking Crimes". This article provides an in-depth analysis of the legal protection of people's privacy rights,

especially in the context of personal data being targeted by hacking crimes. The article highlights the importance of strengthening regulations and the role of the government, as well as individual awareness in protecting their personal data. Using recent empirical data, the article identifies the weaknesses of the data protection system in Indonesia and outlines the roles of various parties, including the government, data processors, and law enforcement officials. However, this article has several shortcomings. Firstly, the normative analysis lacks depth, thus not providing a strong legal foundation to support the recommendations put forward. Secondly, the empirical data used is more descriptive and less utilised to produce in-depth analyses or concrete solutions that can be implemented. Thirdly, the focus of this article is limited to aspects of hacking crimes, thus paying less attention to the broader context of personal data protection, such as data governance by institutions or companies. Fourth, although the article discusses the roles of various parties, the specific steps to be taken by each party are not elaborated in detail. The novelty theory of this article is the integration of empirical data with legal analysis that highlights the weaknesses of the implementation of data protection regulations, as well as the need for synergy between various parties to prevent data leakage (Firdaus, 2022). Overall, these two studies have their own strengths and weaknesses. The research by CSA Teddy Lesmana, Eva Elis, and Siti Hamimah provides a strong theoretical foundation and highlights the importance of regulatory harmonisation, but lacks depth in empirical aspects and practical implementation. Meanwhile, the research by Indriana Firdaus is superior in presenting empirical data and discussing the roles of various parties, but lacks depth in normative analysis and applicable solutions. These two studies provide a valuable basis for collaboration in further research, in order to produce a more comprehensive and applicable study of personal data protection in Indonesia.

This problem can be viewed through several main aspects. First, the increasing frequency in the number of personal data breach cases in Indonesia over the past few years reflects the vulnerability of the data management system to various threats, both from within and outside. Second, some of the underlying factors that triggered the high number of cases include weaknesses in cybersecurity, lack of awareness of companies and the public on the importance of safeguarding personal data, and the lack of adequate regulations prior to the implementation of the Personal Data Protection Law. Third, preventive efforts involving the government, companies, and the public are needed. The government needs to strengthen the implementation of regulations, companies should allocate more resources for technology security, and the public needs to be educated about the importance of personal data protection. This journal aims to assess the situation and trends of personal data breach cases in Indonesia, reveal the main factors that influence the high number of breaches, and assess the effectiveness of the implementation of the Personal Data Protection Law in providing protection for personal data. This analysis is expected to produce strategic recommendations that can improve data protection in Indonesia while strengthening existing regulations.

Methodology

This research was prepared using a mixed methods approach as a comprehensive analytical framework to investigate the phenomenon of personal data breaches in Indonesia in the context of the implementation of the Personal Data Protection Law (PDP Law). By combining quantitative and qualitative methods, this research aims to gain an in-depth and holistic understanding, both from a numerical and narrative perspective.

The data used in the research is divided into primary and secondary data. Primary data was collected through an online survey using Google Forms distributed to the general public from various age groups, occupations, and education levels, with a total of 78 respondents. This survey was designed to measure the level of awareness, understanding, and direct experience of the public regarding personal data breaches.

Meanwhile, secondary data was obtained through a literature study by analyzing scientific journals, books, reports, and other documents relevant to the research theme used to build a strong theoretical framework and empirical context. This document analysis includes a critical review of the contents of the Personal Data Protection Law and its relevance in the context of personal data breach cases in Indonesia. In addition, several real-life cases of personal data breaches in Indonesia are also analyzed to provide concrete illustrations of how the Personal Data Protection Law is applied and the challenges faced. Thus, this research is expected to make a significant contribution to understanding the dynamics of personal data breaches in Indonesia as well as its implications for the protection of individual rights in the digital era.

With a systematic and integrated approach, this research is expected to contribute to various parties in understanding and addressing cases of personal data breaches in Indonesia, as well as evaluating the effectiveness of the Personal Data Protection Law in protecting people's rights.

Result and Discussion

Situation and Frequency of Personal Data Breach Cases in Indonesia

The rapid growth of digitalisation along with advances in technology and information has brought many conveniences and efficiencies to human life, ranging from access to information, communication, to various digital services. However, behind its benefits, digitalisation also brings a dark side that is the root of various forms of contemporary crime in the modern era (Br. Sinulingga, 2024). Technology designed to make life easier is now often misused by irresponsible parties to commit criminal acts, one of which is cyber crime. Indonesia was ranked second only to Ukraine and ranked third with the most cyber crimes in the world (Hapsari and Pambayun, 2023).

Cyber actions that are often carried out by the perpetrators are taking someone's personal data information by using the convenience contained in the technology. Based on Article 1 Paragraph (1) of Law Number 27 Year 2022 states that "Personal Data is data about an individual who is identified or can be identified individually or in combination with other information either directly or indirectly through electronic or non-electronic systems". Personal data is an important thing that must be guarded and protected, because when someone's personal data falls into the hands of irresponsible parties, the risks posed will be

very large. Cybercriminals can use the data for various illegal acts, such as fraud, identity theft, or even account hacking that can harm victims materially and reputationally. For example, criminals can use financial information to make unauthorised transactions or forge identities for unlawful purposes.

In recent years, personal data breach cases in Indonesia have shown a significant increase. This is due to the increasing use of digital technology in various sectors, including e-commerce, banking, and public services. User data leaks from major platforms have become one of the main concerns of the public. Incidents such as customer data leaks from major marketplaces and telecommunication companies, for example, have created unrest among the public. This phenomenon also shows weaknesses in data management and protection in strategic sectors, which in turn requires special attention from policy makers and industry players (Bahtiar, 2022).

According to a report released by a cybersecurity research institute, the number of personal data breach cases in Indonesia continues to increase every year. Data from the past few years shows increasingly sophisticated cyberattack patterns, ranging from phishing to ransomware targeting large organisations (Alfi, Yundari and Tsaqif, 2023). In 2021, for example, there were several major cases involving millions of Indonesians' personal data leaked to the public. This incident raises questions about the readiness of companies and institutions in maintaining data security, including the implementation of appropriate security standards.

Personal data breach cases are the cases with the highest classification or type of data leak compared to other data leak cases. This can be seen from the data presented by Breached.to.

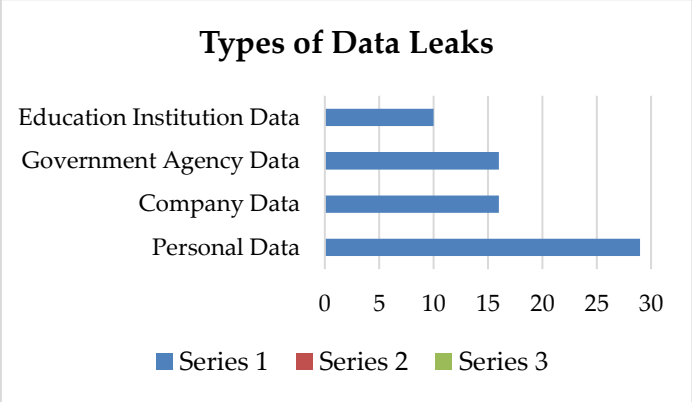

Figure 1. Types of Data Leaks
Source: Breached.to website

In the data, it can be seen that personal data breach cases are the most frequent type of data leakage to the Indonesian people. The frequency of personal data breach cases is very far when compared to cases of breaches of educational institutions, government agencies and company data (Yaputra, 2024).

For example, several cases of data leakage and cybercrime that have occurred in Indonesia almost every year continue to occur without stopping. Between 2020 and 2023,

there were four major incidents that exposed serious vulnerabilities in Indonesia's data protection system. In 2020, there was a data leak at e-commerce platform Tokopedia that revealed 91 million users' data, including full names, email addresses and passwords. Then, in 2021, the BPJS Health data leak affected 279 million participants' data, which included names, addresses, phone numbers, and medical history. The data was even found to be traded on the dark web (Indonesia, 2020; Maharani and Meiliana, 2021).

The incidents continued in 2022, when 105 million voters' data belonging to the General Election Commission (KPU), including full names, Population Registration Numbers (NIK), and addresses, were successfully hacked by a hacker named Bjorka and sold illegally (Cloudeka, 2023). It did not stop there, in 2023, another major data leak involved 337 million data of the Directorate General of Population and Civil Registration (Dukcapil) of the Ministry of Home Affairs. The data stolen by the BreachForums hacker group included complete information such as name, NIK, Family Card number, and other family data (Basyari, 2023).

Even in June 2024, a cyberattack involving the Lockbit 3.0 ransomware successfully crippled the servers of the Temporary National Data Centre. This attack had a serious impact on various public services that rely on the data infrastructure, causing operational disruptions and public concerns over the security of their data. Two months later, in August 2024, there were allegations of a massive data leak in the One Data ASN system managed by the National Civil Service Agency. This leak allegedly involved around 4.7 million personal data, including Employee Identification Numbers (NIP) and Population Identification Numbers (NIK) belonging to state civil servants, exposing security gaps in government data management (Yaputra, 2024). These incidents not only caused public unrest but also underscored serious weaknesses in data protection across strategic institutions in Indonesia.

In the context of regulation, the Indonesian government has responded to this situation by passing Law Number 27 Year 2022 on Personal Data Protection. This law is an important milestone in providing a legal umbrella for the protection of people's personal data. One of the key points of this law is the obligation for electronic system providers to ensure the security of personal data that electronic system providers manage. However, the implementation of the Personal Data Protection Law still faces various challenges, especially in terms of law enforcement and supervision of violators (Rahman, 2021).

Although Law No. 27 of 2022 has been officially enacted by the government and law enforcement agencies, cybercrime cases continue to rise. This is exacerbated by the fact that Indonesia is one of the countries with the largest number of smartphone and internet users in the world, which makes its people even more vulnerable to the threat of personal data hacking. Moreover, since the COVID-19 pandemic began in mid-March 2020, internet usage has increased significantly. This is due to various activities that must be carried out from home in accordance with the government's appeal to break the chain of virus spread. These activities include working from home to the teaching and learning process, from elementary school to college, all of which are carried out online (Putri and Fahrozi, 2020)

Seeing this, it is not surprising that Indonesia is very vulnerable to crime with cases of personal data breaches, criminals will be increasingly interested in the data contained in an application, website or other site that will benefit the perpetrators of crime. Whereas it is clear in Article 65 paragraphs (1), (2) and (3) that every person is prohibited from unlawfully obtaining, disclosing and using personal data of a person who does not belong to him, this is also confirmed in Article 66 of Law Number 27 of 2022 which states that it is not allowed to create or falsify personal data.

Threats and criminal provisions related to the perpetrators have also been outlined in Law Number 27 Year 2022, which includes Article 67 to Article 73. For example in Article 67 paragraph (1) "Every person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him/her with the intention of benefiting himself/herself or others which may result in the loss of Personal Data Subjects as referred to in Article 65 paragraph (1) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiah)" (Sianturi, Nababan and Siregar, 2024). In these provisions it is clearly regulated regarding fines and imprisonment, but it seems that the perpetrators of crime are not deterred and are not afraid of the positive legal regulations that apply in the country of Indonesia.

Thus, this situation demands close collaboration between the government, the private sector and the community. The government needs to increase supervision and impose strict sanctions on violators. Meanwhile, the private sector must be more proactive in implementing adequate data security standards. On the other hand, the public must also be more aware of the importance of protecting personal information and understand the risks that may arise (Ghozali and Hardyanthi, 2024).

Factors That Lead To High Cases Of Personal Data Breaches In Indonesia

The high number of personal data breach cases in Indonesia is a complex phenomenon involving various factors. The rapid development of technology and the widespread access to the internet have created a very conducive environment for cyber criminals to operate. The interconnection of devices and society's dependence on information technology has opened the door for various kinds of cyber attacks, such as data theft. The increasing number of internet users globally, especially in Indonesia, has increased the target of attacks and expanded the range of criminal activities in cyberspace (Mahira Dewantoro and Setiawan, 2023).

Aside from the high rate of internet usage, one of the main causes that has led to the surge in personal data breach cases is the weak cybersecurity systems in many organisations. Many institutions, both from the public and private sectors, have not implemented adequate security measures to protect user data (Hapsari and Pambayun, 2023). The absence of encryption mechanisms, delayed software updates, and uncontrolled access management make these systems easy targets for cyberattacks. This is evident from a number of major incidents, such as data leaks in the telecommunications and e-commerce sectors, involving millions of Indonesians' personal data.

The lack of digital literacy among the public is also one of the main factors. Most Indonesians do not fully understand the importance of protecting personal data. Many individuals easily provide sensitive information to untrusted parties, such as through apps or online forms, without realising the risks of data breaches. This phenomenon is exacerbated by low awareness of the importance of reading terms and conditions when using digital services, which often include explicit consent to the use of personal data (Hildawati *et al.*, 2024).

In addition, the lack of transparency from providers of electronic systems, application systems and other systems is also a factor that can lead to cases of personal data breaches, as many companies and digital service providers are not open about how they manage users' personal data. In some cases, data is even misused for commercial purposes or sold to third parties without consent. Such practices show a lack of responsibility on the part of service providers in maintaining user trust, thus increasing the potential for breaches.

In terms of regulation, prior to the enactment of the Personal Data Protection Law, Indonesia faced significant legal gaps in protecting people's personal data. Existing regulations, such as those contained in the Electronic Information and Transaction Law (ITE Law), were partial and not comprehensive enough to address the complexity of data breach issues. As a result, there is no firm legal umbrella to provide protection and enforce sanctions against perpetrators of personal data breaches.

Rapid technological advancements bring new challenges in protecting personal data. The use of technologies such as the Internet of Things (IoT) and cloud computing is increasing, but many companies are adopting them without understanding the security implications that come with them. These new technologies create more points of vulnerability that can be exploited by irresponsible parties, increasing the risk of data leakage (Judijanto *et al.*, 2024).

The shortage of experts in the field of cybersecurity also worsens the situation. Indonesia still faces a large gap in the availability of human resources with specialised expertise in this field. This leaves many organisations without sufficient capacity to manage complex threats. In addition, training and development of cybersecurity expertise for staff in both government and private institutions is still minimal, adding to the overall vulnerability of the system. According to ISACA Indonesia Chapter President, Syahraki Syahrir, the number of experts who are members of this organisation is far less than neighbouring countries such as Singapore and Malaysia. Indonesia only has 1,100 members, compared to Singapore's 5,500 and Malaysia's 3,000. This is seen as a result of the lack of IT-related education and literacy that is socialised to the public. In addition, until now, not many schools or universities provide specialised learning on cybersecurity (Ramadhan, 2024).

Finally, the high level of organised cybercrime activity further increases the risk of personal data breaches. These groups use increasingly sophisticated methods to exploit weaknesses in security systems, as well as capitalise on people's low digital literacy and loopholes in regulations. Therefore, a holistic and collaborative approach, including

strengthening the implementation of the Personal Data Protection Law, increasing public awareness, and developing a more robust cybersecurity infrastructure, is needed to reduce the high number of personal data breach cases in Indonesia.

Preventive Efforts to Reduce The Increase in Personal Data Breach Cases in Indonesia

Preventive efforts to reduce the number of personal data breaches in Indonesia require close collaboration between the government, companies and communities. The government has a strategic role in building a strong legal and regulatory framework to protect the personal data of its citizens. The enacted Personal Data Protection Law, is an important milestone to create a better data protection system. However, the implementation of this law requires strict supervision, clear sanctions for violators, and the establishment of an independent institution responsible for personal data breaches. These efforts can be strengthened by the integration of national policies that promote digital security as part of Indonesia's technological infrastructure development (Judijanto *et al.*, 2024).

Based on the results of a survey that has been conducted through google form with 78 respondents, it shows that:

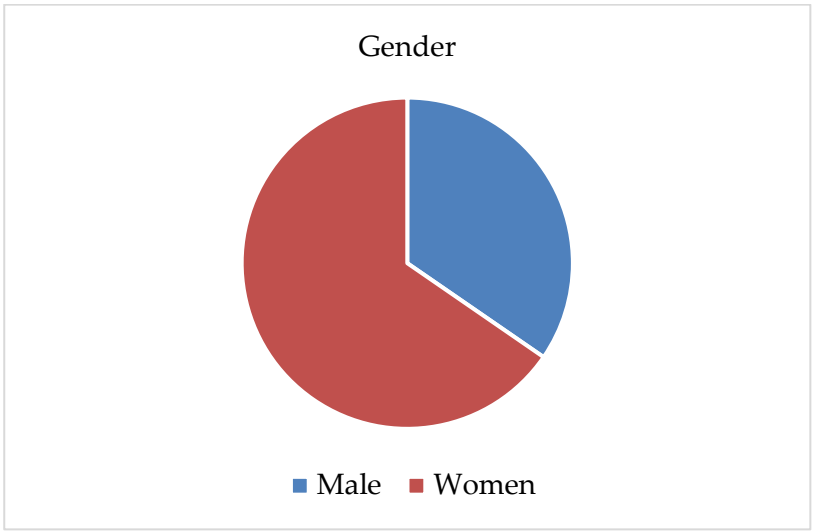

Figure 2. Gender
Source: Research conducted personally through google form with 78 respondents

A total of 65.4% (sixty-five point four per cent) of the respondents were female, i.e. 51 people, while 34.6% (thirty-four point six per cent) or 27 people were male.

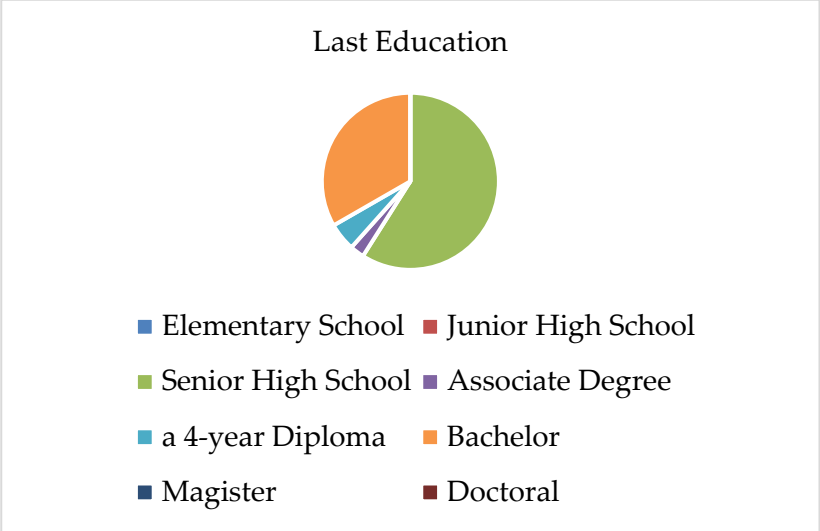

Figure 3. Last Education
Source: Research conducted personally through google form with 78 respondents

The majority of respondents had a senior high school education with 59% (fifty-nine per cent) or 46 people. The S1 education level ranks second with 33.3% (thirty-three point three per cent) or 26 people, followed by D4 with 5.1% (five point one per cent) or 4 people, and D3 with 2.6% (two point six per cent) or 2 people.

Figure 4. How Familiar with Indonesian Personal Data Protection Law
Source: Research conducted personally through google form with 78 respondents

A total of 50% (fifty per cent) or 39 people claimed to be quite familiar with this law, while 30.8% (thirty point eight per cent) or 24 people felt not very familiar. Respondents who were very familiar totalled 17.9% (seventeen point nine per cent) or 14 people, and only 1 respondent (1.3%) was not familiar at all.

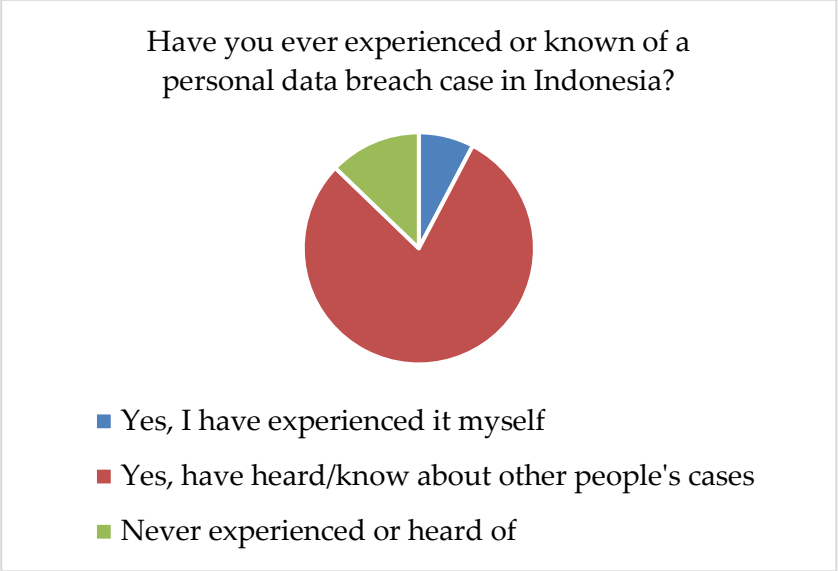

Figure 5. Experienced or Known of a Personal Data Breach Case in Indonesia
Source: Research conducted personally through google form with 78 respondents

A total of 79.5% (seventy-nine point five per cent) or 62 people have heard or known of personal data breaches in others, while 12.8% (twelve point eight per cent) or 10 people have never directly experienced a personal data breach, and 7.7% (seven point seven per cent) or 6 people have experienced the case directly.

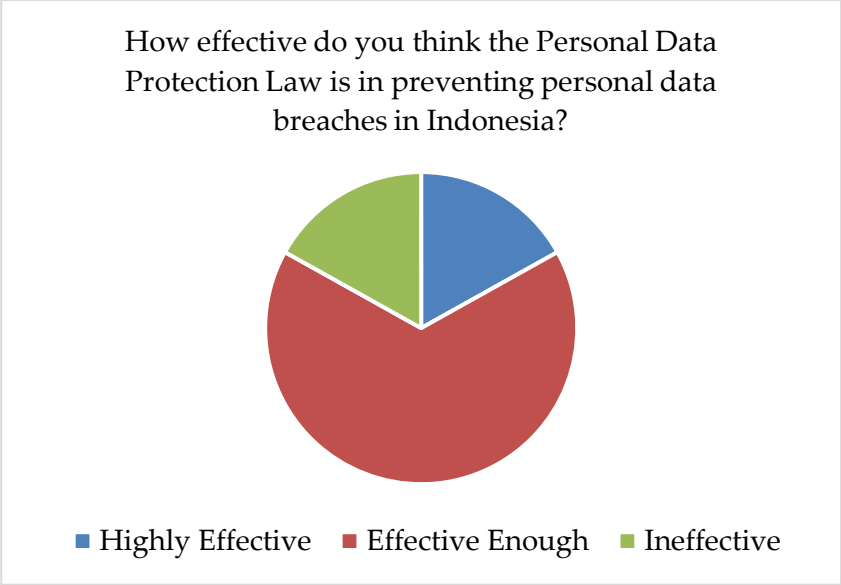

Figure 6. How Effective Think the Personal Data Protection Law in Personal Data Breaches in Indonesia
Source: Research conducted personally through google form with 78 respondents

Most respondents, 60.3% (sixty point three per cent) or 47 people, rated the law as moderately effective, followed by 24.4% (twenty-four point four per cent) or 19 people who felt it was ineffective, and 15.4% (fifteen point four per cent) or 12 people who rated it as very effective.

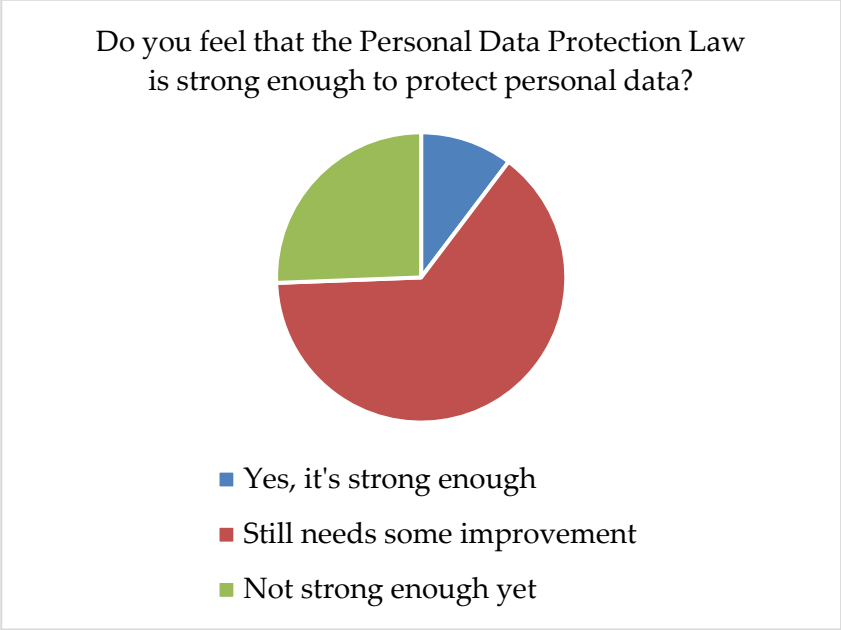

Figure 7. Feel the Personal Data Protection Law to Protect Personal Data
Source: Research conducted personally through google form with 78 respondents

The majority of respondents, 64.1% (sixty-four point one per cent) or 50 people, felt that the law still needs some improvement to be more effective. A total of 25.6% (twenty-five point six per cent) or 20 people said the Personal Data Protection Law was not strong enough, and only 10.3% (ten point three per cent) or 8 people thought it was strong enough.

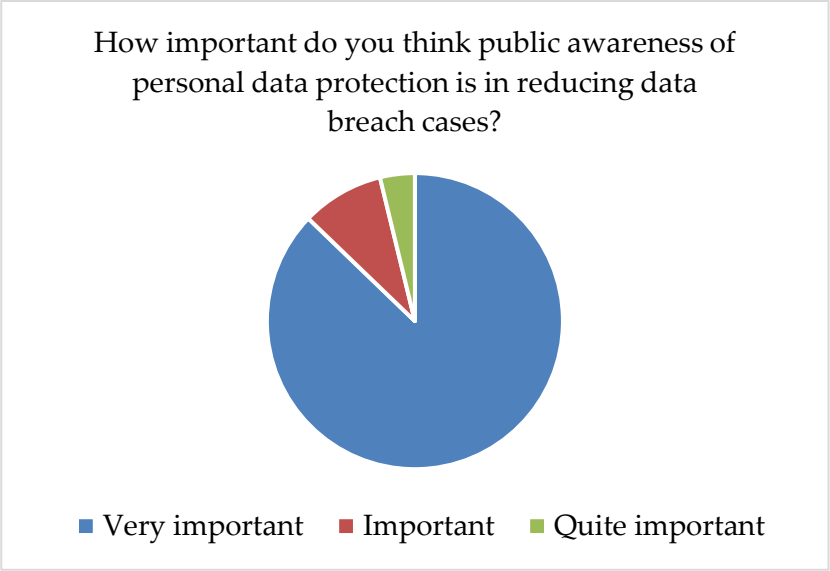

Figure 8. How Important Think Public Awereness of Personal Data Protection in Reducing Data Breach Cases
Source: Research conducted personally through google form with 78 respondents

Most respondents considered public awareness to be very important in reducing cases of personal data breaches, as many as 87.2% (eighty-seven point two per cent) or 68 people. The remaining 9% (nine per cent) or 7 people said it was important, and 3 people (3.8%) said it was quite important.

Figure 9. Aware Regarding Personal Data Protection Under the Personal Data Protection Law
Source: Research conducted personally through google form with 78 respondents

A total of 42.3% (forty-two point three per cent) or 33 people knew little about their rights, followed by the same number, 42.3% (forty-two point three per cent) or 33 people who knew enough. A total of 10.3% (ten point three per cent) or 8 people knew their rights very well, while 4 people (5.1%) did not know at all.

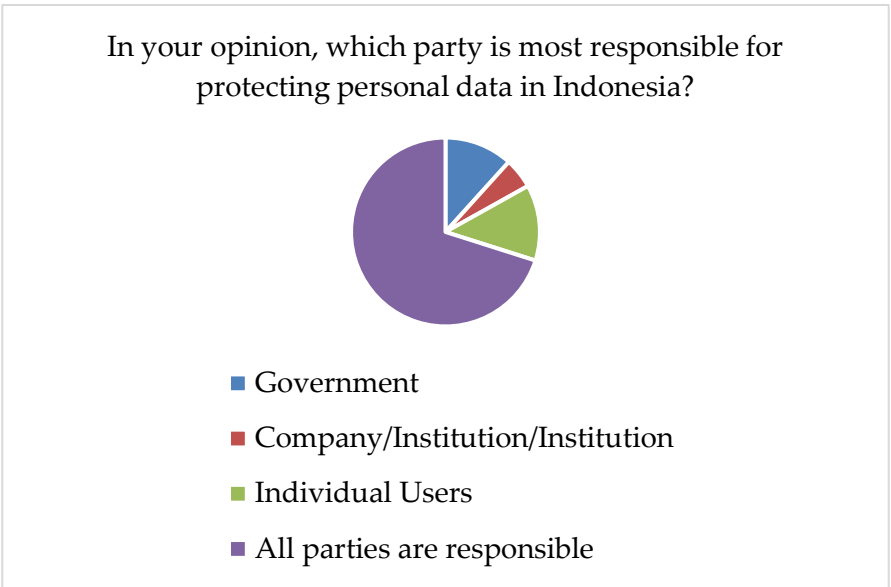

Figure 10. Opinion Most Responsible for Protecting Personal Data in Indonesia
Source: Research conducted personally through google form with 78 respondents

A total of 70.1% (seventy point one per cent) or 54 people stated that all parties are responsible for protecting personal data. Thirteen per cent (13%) or 10 people mentioned individual users, 11.7% (eleven point seven per cent) or 9 people mentioned the

government, and 5.2% (five point two per cent) or 4 people mentioned companies/institutions.

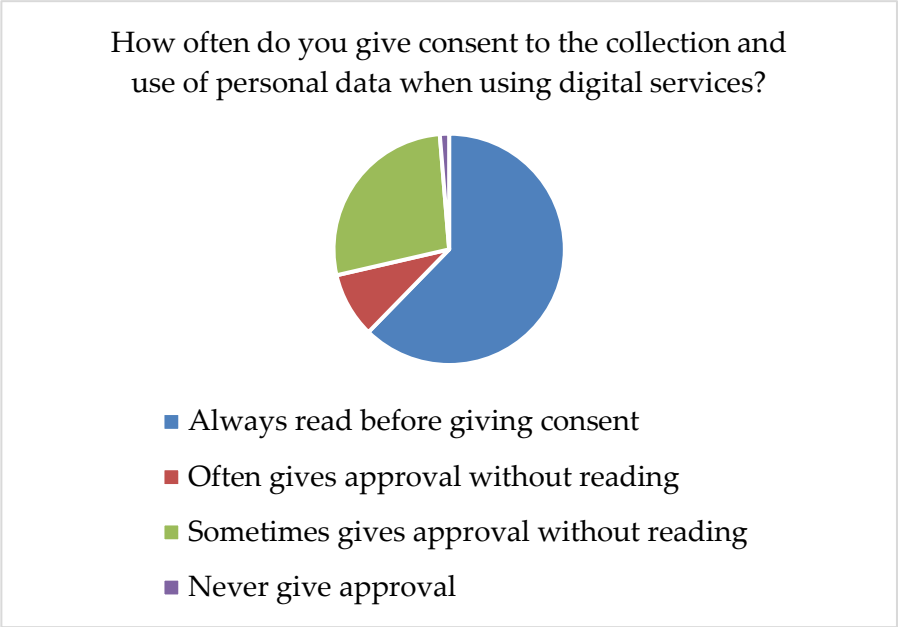

Figure 11. How often Consent to the collection and use of Personal data when using Digital Services
Source: Research conducted personally through google form with 78 respondents

A total of 62.3% (sixty-two point three per cent) or 48 people always read before giving approval. A total of 27.3% (twenty-seven point three per cent) or 21 people answered that they sometimes gave consent without reading, while 9.1% (nine point one per cent) or 7 people often gave consent without reading. Only 1 person (1.3%) never gave consent.

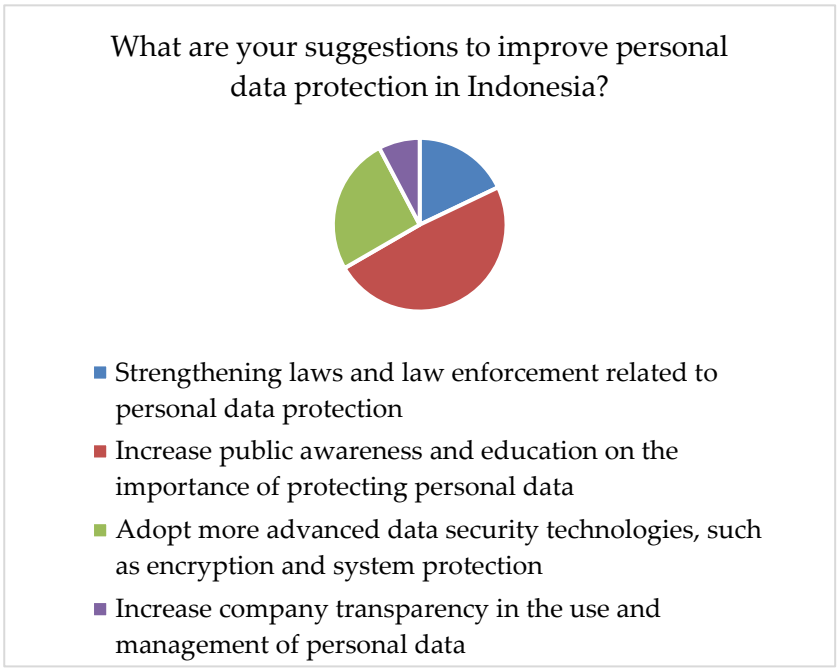

Figure 12. Suggestions tp Improve Personal Data Protection in Indonesia
Source: Research conducted personally through google form with 78 respondents

Respondents provided various suggestions, including strengthening laws and law enforcement, improving public education on the importance of protecting personal data, adopting more advanced data security technologies such as encryption, and increasing company transparency in personal data management.

It can be seen in the survey results that the public still does not fully understand the Personal Data Protection Law, which has an impact on the lack of awareness of their rights regarding personal data, such as giving access permission to dangerous websites or applications. This condition is a reminder for the government to take the issue of personal data breaches more seriously and find solutions so that people can better understand the limits and rules that apply.

Public education and awareness are key in this preventive effort. People need to be equipped with knowledge about their rights to personal data, including how to protect their information from misuse. Public campaigns organised by the government and non-governmental organisations can play a role in improving digital literacy. For example, through seminars, webinars or easily accessible online guides, people can be taught how to recognise digital threats such as phishing and malware, as well as preventive measures that people can take independently (Zahwani and Nasution, 2023).

Other efforts that can be made by the community as users are to use strong passwords, set privacy on social media more strictly, and not carelessly share personal information on digital platforms. Susanto (2017) added that users also need to be careful of phishing and other online scams that can steal personal data. It is important for users to recognise the signs of fraud and immediately report them to the authorities or digital service providers if they find suspicious activity (Zahwani and Nasution, 2023).

In addition, efforts that can be made by the government are to strengthen regulations regarding personal data breaches because even though Law No. 27 of 2022 has been passed, the perpetrators of personal data hacking crimes are still rampant. As a comparison, the UK, one of the developed countries in the European region, has a comprehensive regulatory framework related to personal data protection. The provisions are contained in the Data Protection Act 1998, which came into force in 2000 as a replacement for the previous regulation, namely the Data Protection Act 1984. This law provides legal protection for individual privacy rights related to personal data, including giving data subjects the right to know how their personal data is processed and preventing data processing that potentially violates privacy rights. To ensure the implementation of this regulation, the UK established a special body called The Data Protection Commissioner (Disemadi, 2021).

On the other hand, companies as the main managers of personal data have a great responsibility in ensuring the security of consumer data. Preventive measures that can be taken include the implementation of encryption technology, cloud-based data management with high security standards, and regular system updates to close security gaps. Companies should also develop internal policies governing personal data management, including employee training on the importance of maintaining data confidentiality. In addition, the appointment of a data protection officer can help ensure that all company policies are in line with the Personal Data Protection Law (Zahwani and Nasution, 2023).

Collaboration between the government and companies also needs to be strengthened through the implementation of joint programmes. One example is a regular data security audit programme for companies that manage large amounts of personal data. The government can work with the private sector to provide secure infrastructure and ensure that the technology used meets international standards. In addition, incentives in the form of tax breaks or subsidies can be given to companies that invest in data protection technology.

The development of more advanced cybersecurity technologies should be a national priority. The government can collaborate with universities and research institutions to create innovative solutions to address digital security issues. By developing a domestic technology ecosystem, Indonesia will not only rely on foreign technologies, but also be able to create solutions that are more relevant to the local context. This step can also encourage safer and more sustainable digital economic growth. Bandung Institute of Technology (ITB) and Economic Research Institute for ASEAN and East Asia (ERIA) held a Cybersecurity and Autonomous Vehicles Workshop on 8 May 2024 at Multipurpose Hall, CRCS Building, ITB Ganesha Campus, Bandung. This activity aims to provide a comprehensive understanding of cybersecurity and technology, as well as encourage the establishment of a robust cybersecurity policy framework (Nindita, 2024).

Strict and transparent law enforcement against personal data breaches is also an important element in this preventive effort. The government needs to ensure that violators, both individuals and corporations, are subject to appropriate sanctions to provide a deterrent effect. In addition, transparency in handling data breach cases can increase public confidence in the government's ability to protect people's rights to personal data.

Ultimately, the success of these preventive efforts requires a strong synergy between all parties. The government must be the main facilitator, companies must prioritise data security as part of corporate responsibility, and the public needs to play an active role in protecting their personal data. With this integrated approach, it is hoped that the number of personal data breaches in Indonesia can be significantly reduced, creating a safer and more trusted digital ecosystem.

Conclusion

The situation and frequency of personal data breach cases in Indonesia continue to increase along with the development of digital technology. Despite the enactment of the Personal Data Protection Law, the level of public awareness and compliance with personal data management is still low. Data shows that most people are not familiar with the contents and provisions of the Personal Data Protection Law, which is one of the factors that weaken the protection of their rights in the digital context.

The high number of personal data breach cases in Indonesia is caused by several factors, including a lack of cybersecurity experts, weak implementation of regulations, and low digital literacy. In addition, dependence on foreign technology and lack of domestic technology development exacerbate the situation, as available solutions are not always

relevant to local needs. Loopholes in regulations and weak supervision of digital service providers also contribute significantly to the prevalence of breaches.

As a preventive measure, strong collaboration between the government, companies and communities is needed. The government must strengthen regulations and ensure their effective implementation. Companies need to implement more sophisticated cybersecurity technology and be transparent in managing user data. On the other hand, the public should be encouraged to improve their digital literacy through continuous education. With these efforts, it is hoped that the number of personal data breaches can be minimised, and public trust in the digital ecosystem can be better built.

References

Alfi, M., Yundari, N.P. and Tsaqif, A. (2023) 'Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia', *Jurnal Kajian Stratejik Ketahanan Nasional*, 6(2), p. 5. Available at: https://doi.org/10.7454/jkskn.v6i2.10082.

Annur, C.M. (2022) *Ada 204,7 Juta Pengguna Internet di Indonesia Awal 2022*, *databoks.katadata.co.id*. Available at: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/f7af290483a1152/ada-2047-juta-pengguna-internet-di-indonesia-awal-2022#:~:text=Indonesia merupakan salah satu negara,Facebook Terbanyak%2C Urutan Berapa?) (Accessed: 28 November 2024).

APJII (2024) *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*, *apjii.or.id*. Available at: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang (Accessed: 17 July 2024).

Bahtiar, N. (2022) 'Darurat Kebocoran Data : Kebutuhan Regulasi Pemerintah', *Development Policy and Management Review*, 2(1), pp. 85–100.

Basyari, I. (2023) *Kemendagri Investigasi Dugaan Kebocoran 337 Juta Data Dukcapil*, *kompas.id*. Available at: https://www.kompas.id/baca/polhuk/2023/07/17/337-juta-data-dukcapil-diduga-bocor (Accessed: 27 November 2024).

Br. Sinulingga, S.P. (2024) 'Analisis Tantangan dan Peluang Dalam Perkembangan Teknologi Informasi dan Komunikasi di Era Digital : Perspektif Masa Depan', *Jurnal Ilmiah Ekonomi dan Manajemen*, 2(12), pp. 25–35. Available at: https://doi.org/https://doi.org/10.61722/jiem.v2i12.3018.

Claudia, J. and Sitaboeana, T.H. (2021) 'Analisis Hak Privasi Perlindungan Data Pribadi Masyarakat di Indonesia', *Jurnal Hukum Adigana*, 4(2), pp. 1915–1939. Available at: https://journal.untar.ac.id/index.php/adigama/article/download/17138/9169/48479.

Cloudeka, L. (2023) *Ini Dia 10 Rangkuman Kasus Kebocoran Data di Indonesia dan di Dunia*, *cloudeka.id*. Available at: https://www.cloudeka.id/id/berita/web-sec/kasus-kebocoran-data/ (Accessed: 20 November 2024).

CSA Teddy Lesmana, Elis, E. and Hamimah, S. (2022) 'Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia', *Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia*, 3(2), pp. 1–7. Available at: https://doi.org/https://doi.org/10.52005/rechten.v3i2.78.

Disemadi, H.S. (2021) 'Urgensi Regulasi Khusus dan Pemanfaatan Artificial Intelligence dalam Mewujudkan Perlindungan Data Pribadi di Indonesia', *Jurnal Wawasan Yuridika*, 5(2), p. 177. Available at: https://doi.org/10.25072/jwy.v5i2.460.

Farhan, M. *et al.* (2023) 'Penerapan Hukum Dalam Menanggulangi Kejahatan Siber Penegakan Hukum Terhadap Tindak Pidana Siber', *Kultura : Jurnal Ilmu Hukum, Sosial, dan Humaniora*, 1(6), pp. 8–20. Available at: https://doi.org/https://doi.org/10.572349/kultura.v1i6.569.

Firdaus, I. (2022) 'Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan', *Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia*, 4(2), pp. 23–31. Available at: https://doi.org/https://doi.org/10.52005/rechten.v4i2.98.

Ghozali, F. Al and Hardyanthi, T. (2024) 'Perlindungan Konsumen pada Platform E-Commerce: Regulasi dan Peran Pemerintah', *Ethics and Law Journal: Business and Notary*, 2(3), pp. 136–141. Available at: https://doi.org/10.61292/eljbn.220.

Group, G. (2024) *Pelanggaran Data Pribadi, generali.co.id*. Available at: https://www.generali.co.id/id/pelanggaran-data-pribadi (Accessed: 9 December 2024).

Hapsari, R.D. and Pambayun, K.G. (2023) 'Ancaman Cybercrime di indonesia: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Konstituen*, 5(1), pp. 1–17. Available at: https://doi.org/10.33701/jk.v5i1.3208.

Hildawati *et al.* (2024) *Literasi Digital : Membangun Wawasan Cerdas dalam Era Digital terkini*. Edited by E. Rianty. Yogyakarta: PT. Green Pustaka Indonesia.

Indonesia, C. (2020) *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual, cnnindonesia.com*. Available at: https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual#:~:text=%22Peretasan dilakukan pada Maret 2020,password%2C nama%2C%22 lanjutnya.&text=Cuitan tersebut langsung ramai ditanggapi,hany (Accessed: 29 November 2024).

Judijanto, L. *et al.* (2024) *Literasi Digital di Era Society 5.0 : Panduan Cerdas Menghadapi Transformasi Digital*. Edited by Efitra. Jambi: PT. Sonpedia Publishing Indonesia.

Karo, R.P.P.K. and Prasetyo, T. (2020) *Pengaturan Perlindungan Data Pribadi di Indonesia Perspektif Teori Keadilan Bermatabat*. Cetakan 1. Edited by M. Mahardika. Bandung:

Nusa Media.

Kusuma, S.C.B. (2023) *Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. Universitas Islam Sultan Agung. Available at: https://repository.unissula.ac.id/31440/.

Laksana, T.G. (2024) 'Perlindungan Hukum Konsumen E-Commerce pada Produk Kesehatan: Pembelajaran pada Kejahatan Siber', *Indo Green Journal*, 2(1), pp. 31–44. Available at: https://doi.org/https://doi.org/10.31004/green.v2i1.45.

Leda, H.A. (2024) *Perlindungan Data Pribadi dan Hak Asasi Manusia*, *kompasiana.com*. Available at: https://www.kompasiana.com/hen12684/66a65d0fed64154615240a02/perlindungan-data-pribadi-dan-hak-asasi-manusia?page=2&page_images=1 (Accessed: 29 November 2024).

Maharani, T. and Meiliana, D. (2021) *Dugaan Kebocoran Data 279 Juta WNI, BPJS Kesehatan Tempuh Langkah Hukum*, *Kompas.com*. Available at: https://nasional.kompas.com/read/2021/05/25/11140881/dugaan-kebocoran-data-279-juta-wni-bpjs-kesehatan-tempuh-langkah-hukum#:~:text=Bertalian dengan itu%2C saat ini,dan undang-undang yang berlaku.&text=Dia mengklaim sistem keamanan data,pihak yang tidak b (Accessed: 29 November 2024).

Mahira Dewantoro, N. and Setiawan, D.A. (2023) 'Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik', *Bandung Conference Series: Law Studies*, 3(2), pp. 892–900. Available at: https://doi.org/10.29313/bcsls.v3i2.7247.

Naylawati Bahtiar (2022) 'Darurat Kebocoran Data : Kebutuhan Regulasi Pemerintah', -, 2(1), pp. 1–16. Available at: file:///C:/Users/user/Downloads/32144-Article Text-109597-1-10-20240320.pdf.

Nindita, A. (2024) *Kolaborasi ITB dan ERIA, Bangun Kerangka Keamanan Siber untuk Masa Depan*, *Institus Teknologi Bandung*.

Puspitasari, D. *et al.* (2023) 'Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk', *Journal of Administrative and Social Science*, 4(2), pp. 195–205. Available at: https://doi.org/https://doi.org/10.55606/jass.v4i2.403.

Putri, D.D.F. and Fahrozi, M.H. (2020) 'Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-commerce Bhineka.com)', *National Conference On Law Studies*, pp. 255–273. Available at: https://doi.org/https://doi.org/10.35334/bolrev.v5i1.2014.

Putri, E.P. (2022) *Pentingnya Perlindungan Data Di Indonesia Sebagai Upaya Tanggungjawab Hukum Atas Kebocoran Data*. Universitas Islam Indonesia. Available at: https://dspace.uii.ac.id/handle/123456789/41660.

Rahman, F. (2021) 'Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia', *Jurnal Legislasi Indonesia*, 18(1), p. 81. Available at: https://doi.org/10.54629/jli.v18i1.736.

Ramadhan, F. (2024) *Indonesia Kekurangan Tenaga Ahli Keamanan Siber*, *Media Indonesia*.

Sianturi, C.G.S., Nababan, R. and Siregar, R.J. (2024) 'Peran Hukum Dalam Melindungi Data Pribadi', *Journal Of Social Science Research Volume*, 4, pp. 1–18.

Situmeang, S.M.T. (2021) 'Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber', *Sasi*, 27(1), p. 38. Available at: https://doi.org/10.47268/sasi.v27i1.394.

Yaputra, H. (2024) *Daftar Kebocoran Data Pribadi di Era Jokowi, Paling Banyak di Instansi Pemerintah*, *Tempo*.

Zahwani, S.T. and Nasution, M.I.P. (2023) 'Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital', *Analisis Kesadaran Masyarakat (Zahwani, dkk.) JoSES: Journal of Sharia Economics Scholar*, 2(2), pp. 105–109. Available at: https://doi.org/https://doi.org/10.5281/zenodo.12608751.