West Science Law and Human Rights
Vol. 3, No. 03, July 2025, pp. 225~235

Inequality in Person Data Protection for Vulnerable Communities in the Digital

Firmansyah Nur Arifin[1], Rina Arum Prastyanti[2]
[1,2]Faculty Law Business, Duta Bangsa University, Surakarta, Indonesia

Article Info

Article history:

Received June, 2025
Revised July, 2025
Accepted July, 2025

Keywords:

Digital Exclusion,
Vulnerable Communities,
Personal Data Regulation gap,
Critical Digital Literacy,
Legal Protection of Data in Developing Countries

ABSTRACT

This study aims to analyze the inequality of personal data protection for vulnerable groups in Indonesia in the context of digital transformation. The scope includes communities with low digital literacy, remote areas, the elderly, and informal sector workers. The methods used are literature study, policy analysis, survey analysis, and case studies. Data were taken from 94 cases of personal data leaks from 2019–2023, with the majority coming from private electronic system organizers. The findings show that data protection tends to be a luxury item that is only enjoyed by empowered groups. According to the data, there were 35 cases of leaks in 2023 alone. This study also proposes a social justice-based governance model to address structural inequality for vulnerable groups.

Corresponding Author:

Name: Firmansyah Nur Arifin
Institution Address: Duta Bangsa University, Surakarta, Indonesia
e-mail: firmansyah12016@gmail.com

1. INTRODUCTION

Amid the rapid wave of digital transformation, Indonesian society faces serious challenges regarding the unequal protection of personal data, particularly in regions with inadequate infrastructure. Although the use of digital technology has expanded into public services and everyday life, personal data protection remains an unequal right, especially for vulnerable groups such as those with low digital literacy, rural communities, the elderly, and informal sector workers. As digital systems become increasingly dominant, disparities in access to information, lack of awareness about privacy rights, and unfamiliarity with legal protection mechanisms further reinforce digital exclusion for these groups [1].

The theory of intersectionality as defined by Kimberle Crenshaw and Critical Legal Studies, which views law as non-neutral, is applied here to explain the inequalities in personal data protection [2]. Power relations and personal technologies cannot be separated from personal data protection. Individuals who possess social and digital capital such as good internet access, education, and legal knowledge are in a better position to control the dissemination of their data. In contrast, groups referred to as vulnerable lack bargaining power and understanding of what data is being collected and for what purpose it is processed [3].

According to the Ministry of Law and Human Rights, all people who face barriers or limitations in attaining an adequate standard of living are classified as vulnerable groups. Some groups require greater consideration and are given basic societal needs attention. This aligns with Article 5 Paragraph (3) of Law Number 39 of 1999 on Human Rights which states [4]. that all people belonging to disadvantaged communities deserve to receive greater benefit and amplified protective measures. Vulnerable populations include the elderly, children, the poor, expectant mothers, and people.

Current literature has a tendency to frame the issue of data privacy as a regulatory, technology, and business problem, omitting the role of social class. However, Madden, Gilman, Levy, and Marwick (2017) illustrate how social class stratifies privacy risks in a differential manner, and they are not evenly distributed. To account for the discriminatory impact of big data and predictive analytics on poor neighborhoods, this article adopts an empirically grounded approach, combining survey data and legal case studies, that analyses the socio-spatial patterning of vulnerability within a structural poverty framework. Following van Dijk (2017), digital inequality is not only an issue of access to technology but also of disparities in the capacity to use digital tools competently, affecting the overall social and economic prospects for individuals. This demands an exploration of data privacy and digital inequalities in a way that addresses their social and economic consequences [5].

The unequal exposure of at-risk populations to privacy infringements reflects their marginalized status. While the situational context offers a bottom threshold of participation, not everyone holds the means to comprehend or provide an informed consent regarding data harvesting. Under such circumstances, privacy emerges as a luxury good that is accessible only to those who possess adequate means. The ideal, however, captures the essence of personal data safeguarding being undertaken in a way that is comprehensive, absolute, and devoid of exclusivity. Justice principles maintain that the state and relevant bodies have a duty to address social vulnerability issues through enabling and not standardizing policies. Madden et al. (2017) highlight that the lower income demographic not only faces heightened surveillance, but there are also greater predictive analytics and algorithmic bias impacts due to gaps in access, digital literacy, and resources available for legal data protection. It is therefore evident that data is no longer tenable from a purely legal perspective, but rather within the context of a digital sphere that requires redistributive justice frameworks [6].

This study focuses on analyzing the forms, causes, and consequences of gaps regarding given levels of data protection for certain groups of people in Indonesia. This research attempts to obtain the gaps by reviewing the literature, policies, and practices around the relevant digital issues to present a strong case towards policy change. The significance of this document arises from the likely gap as regards cybernetics and social justice analysis relevant for policy makers and scholars of cyberethics as well as socially responsible stakeholders which has the less emphasized interface for policymakers and academic as well as socially conscientious actors. This problem needs a lot of attention because in Indonesia currently, as noted by Natamiharja and Setiawan (2024) [7], the system of personal data protection is deficient, as in France, there is an urgent requirement for more Implementing Processes and Controls framed in concepts of accountability, as set out in the authors' governance model which is proposed devoid of the detailed control stipulations in the GDPR, control system integration.

It therefore places privacy issues within an ethical and social justice framework, rather than simply voicing them in legal or technological terms. Inequality in personal data protection is a structural disease that needs to be identified and rectified gradually. It is hoped that this study

will serve as a starting point for the development of administratively effective and socially just data protection regulations, especially for individuals who have been overlooked in online conversations.

2. LITERATURE REVIEW

2.1 Personal Data Protection and Social Inequality

Literature reviews indicate that personal data protection is not merely a legal and technological issue but is also closely tied to social structures. Van Dijk (2017) argues that digital inequality is not only about access but also about the skills to use technology critically and productively. Madden et al. (2017) reveal that the risk of privacy violations is higher among low-income communities due to low digital literacy, limited access, and weak legal protections. The intersectionality approach by Crenshaw and the theory of Critical Legal Studies are used to understand that law is not neutral and often perpetuates dominance over vulnerable groups.

2.2 Global Comparison of Personal Data Regulations

Several countries such as Germany, Finland, the Netherlands, and Canada have strong personal data protection systems. Germany, for instance, is a pioneer of the GDPR and requires companies to adhere to principles of transparency and accountability. Finland integrates data literacy into its basic education curriculum, while Canada enforces PIPEDA, which grants individuals the right to access and correct their personal data. In contrast, Indonesia still faces weaknesses in oversight, law enforcement, and the implementation of the Personal Data Protection Law (UU PDP), as noted by Natamiharja and Setiawan (2024).

2.3 Challenges of Digital Literacy and Social Ethics

A study by the Pew Research Center (2023) indicates that around 56% of Americans tend to agree to privacy policies without reading them, revealing a gap between awareness and behavior. In Indonesia, similar challenges occur, exacerbated by the lack of outreach and digital education for vulnerable groups. Meanwhile, Regan and Tzanou emphasize that personal data protection should be recognized as a standalone human right, not merely as part of privacy rights or consumer protection. This calls for a legal and ethical approach based on distributive justice, rather than purely procedural legalism.

3. METHODS

The methods used in this research include: (1) documentation study method, which is conducted through searches, public policies, and relevant academic literature related to personal data protection and vulnerable communities; (2) survey analysis method, which is by examining reports of public behavior surveys in countries with high data leakage rates, such as the United States, to see patterns of vulnerability, digital unawareness, and people's responses to the risk of personal data loss; and (3) comparative method, which is used to compare the legal framework and practices of personal data protection in Indonesia with countries that have established data protection standards, such as the European Union and Canada. These countries were chosen because they can provide perspectives on a more comprehensive and inclusive legal approach to vulnerable groups in digital systems.

We use Legal Inequality Theory which focuses on inequalities in access to legal protection, incorporating Critical Legal Studies (CLS) perspectives and its theory of vulnerability. This theory emphasizes that law is not neutral, but is influenced by existing social structures, often to the detriment of vulnerable groups. This theory can be combined with a more specific theory of vulnerability in dealing with inequality in personal data protection in the digital era.

The limitations in this research lie in the scope of the area which is limited to the Indonesian context and the limited sources of primary empirical data. This research does not use a quantitative approach so that the results are not statistical generalizations, but rather aims to provide a reflective and critical

understanding of the structure of inequality that occurs in the personal data protection system in the digital era.

4. RESULTS AND DISCUSSION

Data protection has emerged as one of the most important concerns in this digital age. Countries all over the world have been forced to make major measures to protect the data of their citizens due to the increasing number of data breaches and the misuse of personal information. Data security is becoming more and more crucial as we produce more data every day. Our personal information may be abused for a number of detrimental reasons, such as identity theft or fraud.

The increasing number of personal data leakage cases in Indonesia shows the need to strengthen cybersecurity and data protection systems, especially in the private sector. According to Semuel Pangerapan, Director General of Informatics Applications at the Ministry of Communication and Information Technology, from 2019 to 2023 there were 94 cases of personal data leakage handled, with 62 of them coming from private electronic system providers. The highest number occurred in 2023 with 35 cases, plus another 15 cases until June. Of these cases, 28 were not personal data protection violations, but were related to system weaknesses or cybersecurity violations. A total of 25 cases have been given recommendations for improvement, and 19 cases were sanctioned in the form of warnings. Kominfo handles these cases together with the National Cyber and Crypto Agency and emphasizes that the organizers are responsible for the data leakage that occurred.

Indonesians suffered the impact of 94.22 million leaked accounts putting Indonesia at 8th place on the Surfshark's data leak list. Together with China, Russia, India and the United States, Indonesia finds itself lower on the chart with total accounts leaked reaching 994.72 million. The massive data leaks that occur in Indonesia is due to the absence of a protective framework for personal data and a regulation system for service providers.

As noted by Awanapps Team (2024), the protection of personal data serves as the backbone of privacy in the present-day world which is digitally advanced. Information technology is presently at the helm of all technological advancements. In such a context, personal data is like an unprotected asset which can be easily exploited. This is the reason why there need to be sharp laws in place along with proper supervision so that data can be managed safely and sustainably. It is not only Australia but many other countries of the world have adopted exemplary measures for data protection and can act as role models for other countries including Indonesia.

Germany is the frontrunner of data protection policies having greatly contributed toward developing the General Data Protection Regulation (GDPR) in the European Union (EU). The country focuses on privacy and grants individuals the right to access their data and make changes. Not adhering to such clauses comes at a cost in terms of fines, thus encouraging companies to run disciplined data management practices. Sweden also has remarkable advances in their system of protecting personal data. With the establishment of self-governing bodies such as the Data Protection Authority, citizens are provided with the means to access, change or delete their data without hurdles [8].

Finland combines regulation with early education and takes an innovative approach as a whole. The country integrates data literacy into the school curriculum and mandates the reporting of data breach incidents within 72 hours. The Netherlands does not stand idle either regarding GDPR enforcement. The supervisory authority, Autoriteit Persoonsgegevens, periodically holds educational sessions for the public and guides companies on compliance with data protection standards. It is evident that a synergistic approach combining regulation, education, and enforcement from these countries results in a strong data protection system [9].

Outside the European region, Canada implements the Personal Information Protection and Electronic Documents Act (PIPEDA) which provides individuals the right to ascertain the methods employed in gathering and utilizing their data. Under the Privacy Act 1988, Australia focuses on enhancing digital literacy among citizens while prioritizing accountability in the management of data. Singapore is the leader in the Asian region in offering a solid legal structure and educating the private sector through the Personal Data Protection Act (PDPA). Norway as a member of the European Economic Area (EEA) enforces strict compliance with the GDPR policies and places a great emphasis on public awareness regarding privacy rights [10].

Sadly, Indonesia has not demonstrated a similar outcome. Surfshark data released by Databoks (2024) shows Indonesia as one of the top ten countries in the world by the number of data leaks between January 2020 to January 2024. Indonesia ranks in eighth position with approximately 94.22 million accounts affected. This collection suggests that there is virtually no personal data security system in place, or very poor supervision of data gathering and management processes by digital service providers. It is high time that these data gaps are adequately addressed by government and other relevant stakeholders by taking the necessary actions and creating a culture that puts in place regulations that strengthen data management awareness.

Observing the steps taken by the American society as one of the countries with a high rate of personal data leaks, based on the data that has been found. After that, we will compare it with countries known for having strong data protection systems. This comparison aims to understand the differences in approaches, public awareness, and the effectiveness of regulations implemented, thereby providing a clearer picture of the factors influencing the level of personal data security in a country.

The agreements and policies provided by apps, websites, and other online services grant users the opportunity to review and consent on how their information will be utilized. However, some parties claim that the lengthy and complex nature of these policies minimize their effectiveness and do not give consumers real choices. Research indicates that Americans as a whole tend to disregard such policies, in fact, 56% of them claimed that they usually click “agree” without bothering to read anything. Furthermore, people are also less convincing about the usefulness of privacy policies, with 61% describing them as incapable of explaining the processes through which personal data is treated, while 69% deem it a mere procedural hurdle to overcome.

However, some riskier privacy habits still persist. Specifically, 16% of smartphone users reported that they do not use security features such as passwords, fingerprints, or facial recognition to unlock their phones. These habits are more common among older smartphone users. Those aged 65 and over are more likely than adults under 30 to say that they do not use security features to unlock their mobile devices (28% vs. 9%). Nevertheless, the majority of users across various age groups continue to take these security measures.

In countries with strong data protection systems such as Germany, Sweden, Finland, and the Netherlands, public awareness of the importance of data privacy tends to be high. This is closely related to the role of strict regulations, consistent education from an early age, and the active involvement of supervisory agencies in educating the public. For example, in Finland, data literacy has been taught since elementary school, creating a society that understands how to independently protect their personal data. Similarly, in Sweden and the Netherlands, citizens are given full rights to access, modify, and delete their data, as well as being encouraged to report suspicious incidents. This culture promotes more cautious digital behavior, such as the use of two-factor authentication, encryption of communications, and an understanding of digital security risks [11].

The behavior of society is a key element in the effectiveness of personal data

protection. Strong regulations and oversight will not be optimal if not accompanied by wise digital behavior from the public. Therefore, countries with robust data protection systems generally also have an educated, critical, and responsible society in using digital technology [12].

The main issue found in this finding is the disparity between the increasing threat of data leaks and the readiness of society and regulations that are still weak. Low digital literacy, a permissive attitude towards privacy policies, and the ineffectiveness of legal instruments worsen the position of society in facing personal data exploitation. In the context of Indonesia, the weak implementation of the Personal Data Protection Law (UU PDP) also serves as a hindering factor for effective protection [13].

This finding is consistent with various previous studies. Solove & Schwartz (2020) note that society often experiences privacy fatigue due to the lack of control over their data [14]. Mark Jacob Amiradakis (2020) This article discusses how technology companies use digital platforms to manipulate user attention and behavior, exploiting regulatory weaknesses and low digital literacy [15]. The study "Understanding Data Breach from a Global Perspective Incident Visualization and Data Protection Law Review (2024)" compares the maturity levels of data protection regulations across various regions. It was found that although developing countries like Brazil and India have adopted data protection laws that mimic the GDPR, weak implementation and law enforcement lead to low effectiveness in data protection. In contrast, countries with strong data protection legal systems, such as those in Europe and Japan, show lower risks of data breaches. This underscores that the strength of regulation and law enforcement significantly contributes to the reduction of data breach risks [16].

A survey by the Pew Research Center revealed that more than 90% of Americans feel they have lost control over their personal data. Despite high concerns about privacy, many of them continue to use digital services without taking adequate protective measures. This indicates a gap between awareness and action in personal data protection [17].

In the literature review, personal data protection is recognized as a fundamental right. Regan emphasizes the importance of a human rights-based approach to data regulation. She states that data protection policies should be rooted in respect for individual rights, not merely in balancing economic interests and consumer protection. Tzanou argues that the right to personal data protection has developed into a standalone fundamental right, separate from the right to privacy, and requires a legal framework responsive to digital era challenges, such as large-scale data processing and the use of Artificial Intelligence.

Several parties need to take action. The government must enforce the Personal Data Protection Law, strengthen oversight, and promote transparency. Educational institutions and the media need to enhance digital literacy, especially among vulnerable groups. Digital companies need to be more accountable in their privacy policies, including simplifying language and clarifying the consequences of user consent. The internationalization of data protection standards also needs to be promoted to create a safer and fairer digital ecosystem [18].

This study has limitations: it relies on secondary and foreign data mainly from the United States, which has a legal, social, and cultural context different from Indonesia and the lack of local quantitative data makes conclusions about Indonesian society still assumptive. Further empirical research in Indonesia, especially on vulnerable groups such as the elderly, informal workers, and children, is urgently needed.

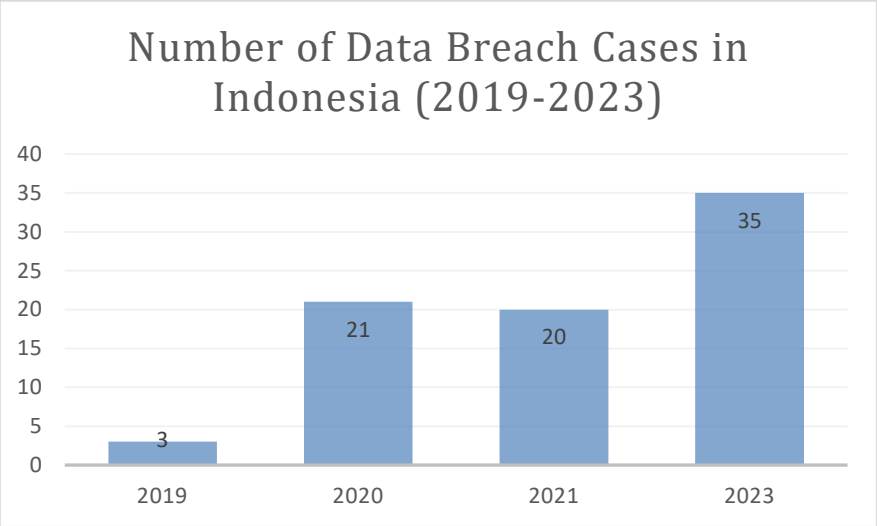

Figure 1. Data Breach Cases in Indonesia (2019–2023)

Source: ITS Media Centre. (2024, November 1). Graph of data leakage cases in Indonesia. Institut Teknologi Sepuluh Nopember.https://www.its.ac.id/news/2024/11/06/gelar-idsecconf-its-ajak-publik-sadar-keamanan-data-di-era-ai/

No	Country	Number of Leaked Accounts (millions)
1	United States	994,72
2	Russia	338,57
3	India	165,08
4	China	161,37
5	Iran	155,42
6	Brasil	134,67
7	France	100,92
8	Indonesia	94,22
9	United Kingdom	76,59
10	Philippines	65,13

Figure 2. Ten Countries with the Largest Data Breaches (January 2020–January 2024)

Source: Surfshark. (2024). 10 Countries with the Most Data Leaks (January 2020-January 2024). Accessed from Databoks by Katadata

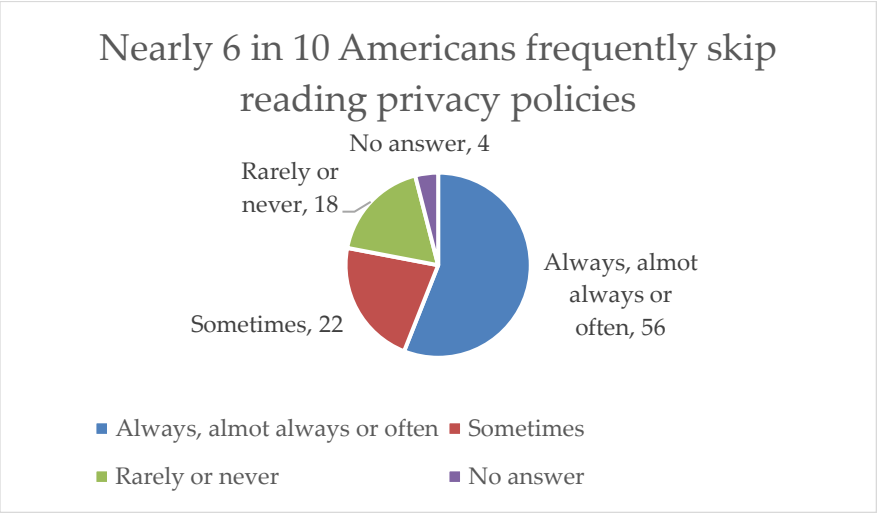

Figure 3. Nearly 6 in 10 Americans frequently skip reading privacy policies

Source: Pew Research Center. (May 15–21, 2023). How Americans View Data Privacy. Survey of U.S. adults.

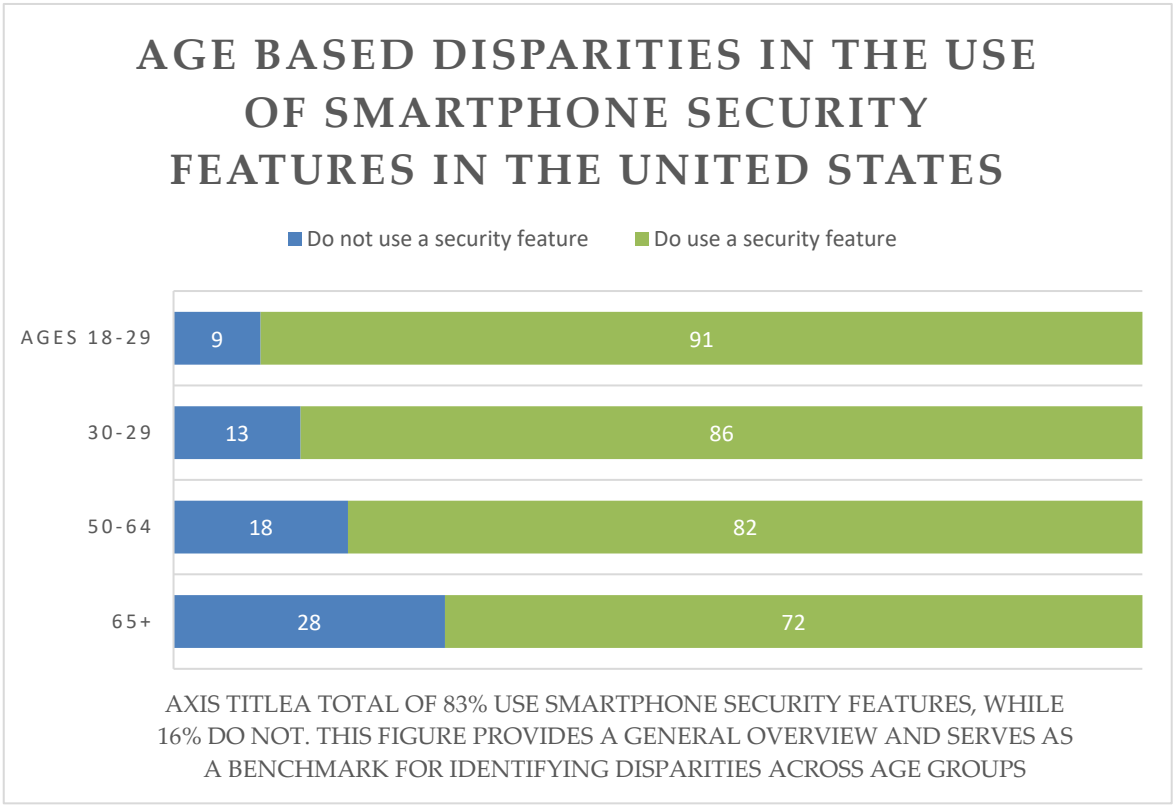

Figure 4. Use of Security Features by U.S. Adult Smartphone Owners by Age Group (% of respondents who use or do not use security features such as passcode, fingerprint, or facial recognition)

Source: Pew Research Center. (2023). "How Americans View Data Privacy." Survey conducted May 15–21, 2023.

5. CONCLUSION

Based on the established research objectives, namely to analyze the forms, causes, and consequences of the inequality of personal data protection in Indonesia, especially for vulnerable groups, it can be

concluded that this inequality is a structural symptom that is exacerbated by the lack of digital literacy, unprepared legal infrastructure, and weak public awareness of their privacy rights. This research confirms that personal data protection in Indonesia is still exclusive and unequal, especially for groups that do not have equal access to technology and information.

The findings show that vulnerable groups such as rural communities, informal workers, the elderly, and individuals with limited education experience double vulnerability to data exploitation.

They not only have minimal understanding of the consequences of digitalization but also lack bargaining power in the processes of data collection and use. This inequality is further clarified by an intersectionality approach and Critical Legal Studies, which position the law not as a neutral tool but as a product of power relations that do not favor marginalized groups.

In response to this inequality, this study recommends the establishment of more inclusive and responsive policies to the needs of vulnerable groups. This can be realized through three main steps: first, systematic public education on digital rights and data protection mechanisms; second, the establishment of independent oversight institutions that ensure fair distribution of technology and regulation; third, the revision of data protection regulations with a distributive justice approach, rather than merely a procedural legal approach. This procedure must involve the active participation of affected communities in the policy formulation process.

Thus, personal data protection should not be understood solely as a legal or technical issue, but rather as a social right that requires the state's commitment to marginalized groups. This research is expected to serve as an initial foundation in building a data protection system that is not only administratively effective but also socially just, ensuring that no group is left behind in the ever-evolving digital ecosystem.

ACKNOWLEDGEMENTS

The author expresses heartfelt thanks to the course instructor for International Law, Assoc. Prof. Dr. Rina Arum Prastyanti, S.H., M.H., who has guided and provided significant direction in the learning process and the preparation of this research. Thanks, are also extended to ITS Media Center for providing data related to data breaches in Indonesia on November 24, as well as to the party that supplied the data "Ten Countries with Largest Data Breaches (January 2020 - January 2024)" which greatly supports the analysis in this research. Additionally, I would like to thank Surfshark 2024 and Databoks by Katadata for the relevant and accurate data and information, as well as Pew Research Center for the survey results titled "How America Views Data Privacy" conducted from May 15 to 21, 2023, which provides important perspectives regarding the views of the American public on data privacy issues. Lastly, I express my deep gratitude to Muhammad Faisal Khairul Rijal who has faithfully accompanied and supported me throughout the research process.

REFERENCES

Journal

[1] L. Judijanto, N. Solapari, and I. Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," vol. 3, no. 01, pp. 20–29, 2024, doi: 10.58812/eslhr.v3i01.

[2] C. H. I. H. Arris, I. H. Arvard, L. A. W. R. Eview, D. W. Carbado, and C. I. Harris, "APPINPublic Law & Legal Theory Research Paper No . 19-52 I NTERSECTIONALITY AT 30 : M G THE M ARGINS OF A NTI -E SSENTIALISM , I NTERSECTIONALITY , AND D OMINANCE T HEORY A ND ESSAY INTERSECTIONALITY AT 30 : MAPPING THE MARGINS," vol. 2193, no. 19, 2019.

[3] A. S. Kriswandaru *et al.*, "Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus," vol. 2, no. 4, pp. 740–755, 2024, doi: 10.51903/hakim.v2i04.2157.

[4] L. Effendi, R. S. Darwis, and N. C. Apsari, "DAN KEBUTUHANNYA (Sebuah Kajian Hasil Pemetaan Sosial CSR PT Indonesia Power UPJP Kamojang)KELOMPOK RENTAN," *Share Soc. Work J.*, vol. 10, no. 1, p. 51, 2020, doi: 10.24198/share.v10i1.26896.

[5] J. A. G. M. Van Dijk, "Digital Divide: Impact of Access," *Int. Encycl. Media Eff.*, pp. 1–11, 2017, doi: 10.1002/9781118783764.wbieme0043.

[6] M. Madden, M. Gilman, K. Levy, and A. Marwick, "Prcy, Poverty and Big Data: A Matrix of Vivaulnerabilities for Poor Americans," *Wash. Univ. Law Q.*, vol. 95, no. 1, pp. 053–125, 2017.

[7] R. Natamiharja and I. Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law J.*, vol. 7, no. 1, pp. 233–251, 2024, doi: 10.22437/home.v7i1.349.

[8] D. Pöhn, N. Mörsdorf, and W. Hommel, "Needle in the Haystack: Analyzing the Right of Access According to GDPR Article 15 Five Years after the Implementation," *ACM Int. Conf. Proceeding Ser.*, 2023, doi: 10.1145/3600160.3605064.

[9] S. S. Lima Filho and B. C. S. Peixe, "Análise de eficiência na gestão de recursos das Instituições Federais de Ensino Superior à luz da nova administração pública," *Rev. Contemp. Contab.*, vol. 17, no. 43, pp. 88–103, 2020, doi: 10.5007/2175-8069.2020v17n43p88.

[10] T. Bolca, "Can PIPEDA 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation against Facial Recognition Technology," *Can. J. Law Technol.*, vol. 18, no. 1, 2020, [Online]. Available: www.zdnet.com/article/

[11] A. Issaoui, J. Örtensjö, and M. S. Islam, "Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance," *Futur. Bus. J.*, vol. 9, no. 1, 2023, doi: 10.1186/s43093-023-00285-2.

[12] R. Rughiniș, C. Rughiniș, S. N. Vulpe, and D. Rosner, "From social netizens to data citizens: Variations of GDPR awareness in 28 European countries," *Comput. Law Secur. Rev.*, vol. 42, pp. 36–46, 2021, doi: 10.1016/j.clsr.2021.105585.

[13] L. A. Sihombing and Y. Nuraeni, "Norms and Ethics in Criminal Justice: Assessing Contemporary Legal Policy," *J. Info Sains Inform. …*, vol. 13, no. 03, pp. 1088–1099, 2023, [Online]. Available: https://ejournal.seaninstitute.or.id/index.php/InfoSains/article/view/3693%0Ahttps://ejournal.seaninstitute.or.id/index.php/InfoSains/article/download/3693/2885

[14] D. J. Solove, "Murky Consent: an Approach To the Fictions of Consent in Privacy Law," *Bost. Univ. Law Rev.*, vol. 104, no. 2, pp. 593–639, 2024, doi: 10.2139/ssrn.4333743.

[15] M. J. Amiradakis, "Surveillance capitalism and the derision of the digital denizen," *Acta Acad.*, vol. 52, no. 2, pp. 52–75, 2020, doi: 10.18820/24150479/aa52i2/4.

[16] G. A. Pimenta Rodrigues *et al.*, "Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review," *Data*, vol. 9, no. 2, pp. 1–24, 2024, doi: 10.3390/data9020027.

[17] T. N. Suciati, "Sinisme Privasi, Diskriminasi Dan Komoditas Data: Paradoks Media Sosial Di Era Kapitalisme Pengawasan," *J. Acta Diurna*, vol. 15, no. 2, p. 145, 2019, doi: 10.20884/1.actadiurna.2019.15.2.2138.

[18] V. Papakonstantinou and P. De Hert, "The Regulation of Digital Technologies in the EU," *Regul. Digit. Technol. EU*, no. May, 2024, doi: 10.4324/9781032630175.

News Article:

- AwanApps Team. (2024, November 1). Indonesia Wajib Contoh! Berikut 8 Negara dengan
- ITS Media Center. (2024, November 1). *Grafik kasus kebocoran data di Indonesia*. Institut Teknologi Sepuluh Nopember. https://www.its.ac.id/news/2024/11/06/gelar-idsecconf-its-ajak-publik-sadar-keamanan-data-di-era-ai/
- Perlindungan Data Terbaik. AwanApps. https://www.awanapps.com/technologies/indonesia-wajib-contoh-berikut-8-negara-dengan-perlindungan-data-terbaik/
- Pew Research Center, survei terhadap orang dewasa di AS yang dilakukan pada 15–21 Mei 2023. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/
- Santosa, L. W. (2023). *Kominfo tangani 94 kasus kebocoran data pribadi sejak 2019, 62 kasus melibatkan PSE privat*. ANTARA News. https://www.antaranews.com/berita/3584103/kominfo-tangani-94-kasus-kebocoran-data-pribadi-dalam-tiga-tahun
- Surfshark. (2024). 10 Negara dengan Kebocoran Data Terbesar (Januari 2020–Januari 2024). Diakses dari Databoks by Katadata
- Pew Research Center, survei terhadap orang dewasa di AS yang dilakukan pada 15–21 Mei 2023.

https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/