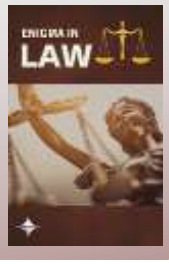
e-ISSN: 3026-6068

Enigma in Law

Journal website: https://enigma.or.id/index.php/law



The Erosion of Privacy in the Digital Age: A Constitutional Challenge in Indonesia

Syahwami Syahwami[1], Hamirul Hamirul[1*]

[1]Institut Administrasi dan Kesehatan Setih Setio, Muara Bungo, Indonesia

ARTICLE INFO

Keywords:
Constitutional law
Data protection
Digital privacy
Indonesia
Observational study

***Corresponding author:**
Hamirul Hamirul

E-mail address:
hrul@ymail.com

All authors have reviewed and approved the final version of the manuscript.

https://doi.org/10.61996/law.v2i2.56

A B S T R A C T

The digital age has revolutionized communication and information access, but it has also brought significant challenges to the fundamental right to privacy. In Indonesia, the legal framework struggles to keep pace with technological advancements, raising concerns about the erosion of privacy protections. This study examines the constitutional challenges and practical implications of digital privacy erosion in Indonesia. This study employs a mixed-methods approach. First, a comprehensive review of Indonesian constitutional law, privacy legislation, and relevant court decisions is conducted. Second, observational data is collected through a survey of Indonesian internet users (n = 500) to assess their privacy awareness, experiences with data breaches, and perceptions of legal protections. Data analysis involves both qualitative legal interpretation and quantitative statistical analysis. The study reveals a significant gap between constitutional guarantees of privacy and the reality of data collection and surveillance practices in Indonesia. Observational data highlights widespread concerns among Indonesian internet users about privacy violations, with a majority experiencing data breaches and feeling inadequately protected by existing laws. Legal analysis indicates that existing legislation is often vague, outdated, and fails to address the unique challenges posed by digital technologies. In conclusion, this study underscores the urgent need for comprehensive legal reforms in Indonesia to protect digital privacy. Constitutional challenges must be addressed through clear and enforceable legislation that aligns with international standards. Additionally, public awareness campaigns and educational initiatives are crucial to empower individuals to protect their personal information in the digital age.

1. Introduction

The advent of the digital age, marked by the proliferation of the internet, mobile devices, and data-driven technologies, has undeniably revolutionized the way individuals live, work, and interact. While this technological transformation has ushered in unprecedented opportunities for communication, commerce, and information access, it has also brought forth significant challenges to the fundamental right to privacy. As societies become increasingly reliant on digital platforms and services, the collection, storage, and analysis of personal data have become ubiquitous, raising profound questions about the boundaries of privacy in the digital realm. In Indonesia, a rapidly developing nation with a burgeoning digital economy, the issue of digital privacy has emerged as a critical concern. With a population of over 270 million, Indonesia boasts one of the largest and most active internet user bases in the world. The widespread adoption of smartphones, social media platforms, and e-commerce has fueled a digital revolution, transforming the social, economic, and political landscape of the country. However, this rapid digitization has also exposed Indonesian citizens to a myriad of privacy risks, ranging from data breaches and identity theft to unauthorized surveillance and targeted advertising.[1-3]

The Indonesian Constitution, under Article 28G, guarantees the right to privacy as a fundamental human right. However, the existing legal framework often struggles to keep pace with the rapid advancements in technology and the evolving nature

of privacy threats. This has created a significant gap between constitutional guarantees and the realities of data collection and processing practices in Indonesia. The Electronic Information and Transactions Law (UU ITE), a primary piece of legislation governing online activities, has been criticized for its vague provisions that can be interpreted broadly to restrict online speech and justify surveillance. Moreover, the law, enacted in 2008, predates the widespread adoption of smartphones and social media, rendering it inadequate to address the unique challenges posed by these technologies. The ongoing debate over the Personal Data Protection Bill (RUU PDP) further underscores the complexities of digital privacy in Indonesia. The proposed bill, if passed, would establish a comprehensive framework for data protection, including requirements for consent, data minimization, and security measures. However, its passage has been delayed due to various factors, including disagreements over specific provisions and concerns about the potential impact on businesses. The lack of a comprehensive data protection law leaves Indonesian citizens vulnerable to the unchecked collection and use of their personal information by both government agencies and private corporations.[4,5]

Beyond legal and regulatory challenges, the erosion of privacy in Indonesia is also influenced by cultural and social factors. The collectivist nature of Indonesian society, which emphasizes communal values over individual rights, can sometimes hinder the assertion of privacy claims. Additionally, limited awareness of privacy risks and inadequate digital literacy among the general population exacerbates the vulnerability to privacy violations. The consequences of unchecked data collection and surveillance are far-reaching. Privacy breaches can lead to financial losses, reputational damage, and even emotional distress. Moreover, the pervasive monitoring of online activities can have a chilling effect on freedom of expression, as individuals may self-censor their online behavior out of fear of reprisal. The misuse of personal data for political purposes, such as targeted propaganda and voter manipulation, poses a significant threat to democratic processes.[6,7] This study seeks to shed light on the complex landscape of digital privacy in Indonesia through a multi-faceted approach. First, it conducts a comprehensive analysis of Indonesian constitutional law, privacy legislation, and relevant court decisions to assess the adequacy of legal protections and identify potential areas for reform. Second, it employs an observational study, utilizing a survey of Indonesian internet users, to gather empirical data on their experiences with privacy violations, perceptions of legal protections, and awareness of privacy risks. This mixed-methods approach aims to provide a nuanced understanding of the challenges and opportunities for safeguarding privacy in the digital age within the Indonesian context. The findings of this study have significant implications for policymakers, legal practitioners, privacy advocates, and the general public. By identifying the shortcomings of existing legal frameworks and highlighting the concerns of Indonesian citizens, this research can inform the development of more effective privacy policies and regulations. Moreover, by raising awareness of privacy risks and promoting digital literacy, this study can empower individuals to take proactive measures to protect their personal information online. Ultimately, this research contributes to the ongoing global conversation about the balance between technological innovation, economic development, and the fundamental right to privacy.

2. Methods

This research employed a mixed-methods approach, combining legal analysis with an observational survey and qualitative interviews to gain a comprehensive understanding of the erosion of privacy in the digital age within the Indonesian context. This methodological triangulation aimed to capture the nuances of legal frameworks, individual experiences, and expert perspectives, thereby enhancing the validity and reliability of the study's findings. Legal Analysis: A systematic review of relevant legal documents was conducted to analyze the constitutional and legislative framework governing privacy in Indonesia, primary sources included: The 1945 Constitution of the Republic of Indonesia: Articles pertaining to fundamental rights, including

the right to privacy (Article 28G), were scrutinized to ascertain the constitutional basis for privacy protection; The Electronic Information and Transactions Law (UU ITE): This law, enacted in 2008, was examined to identify provisions related to data protection, cybersecurity, and surveillance. Amendments and revisions to the law were also considered to trace the evolution of legal approaches to digital privacy; Personal Data Protection Bill (RUU PDP): Although not yet enacted, the draft bill was analyzed to assess the proposed legal framework for personal data protection, including principles of data processing, rights of data subjects, and obligations of data controllers; Relevant Court Decisions: Judgments of the Constitutional Court and Supreme Court addressing privacy issues were reviewed to understand judicial interpretations of existing laws and identify emerging legal trends. The legal documents were analyzed using a combination of doctrinal and socio-legal approaches. Doctrinal analysis involved interpreting the text of the laws and court decisions, examining legal principles, and identifying ambiguities and inconsistencies. The socio-legal approach considered the broader social, political, and economic context in which these laws operate, as well as the impact of technological advancements on privacy rights. The analysis sought to answer the following questions: How does the Indonesian Constitution define and protect the right to privacy? What are the key provisions of the UU ITE related to data protection, cybersecurity, and surveillance? What are the strengths and weaknesses of the proposed RUU PDP in addressing digital privacy challenges? How have Indonesian courts interpreted and applied privacy laws in specific cases?

Observational Survey: A structured online questionnaire was developed to collect data on Indonesian internet users' experiences with and perceptions of digital privacy. The questionnaire included items on: Demographics: Age, gender, education level, occupation, and geographical location; Data Breach Experiences: Type of data breach (e.g., social media, financial, identity theft), frequency, perceived impact, and actions taken in response; Privacy Awareness: Knowledge of privacy risks, sources of information about privacy, and perceived effectiveness of legal protections; Perceptions of Government Responsibility: Attitudes towards government intervention in digital privacy and expectations for future legislation; Privacy Protection Practices: Use of passwords, two-factor authentication, privacy settings on social media, and other measures to safeguard personal information. The questionnaire was pilot tested with a small group of respondents to ensure clarity and comprehensiveness. Revisions were made based on feedback received. A convenience sampling method was used to recruit participants through online platforms and social media networks. Eligibility criteria included being an Indonesian citizen aged 18 or older and having regular access to the internet. A total of 500 responses were collected over a period of four weeks. Quantitative data from the survey was analyzed using descriptive statistics (frequencies, percentages, means) and inferential statistics (correlation analysis). Qualitative responses to open-ended questions were coded and analyzed thematically to identify patterns and trends.

Qualitative Interviews: Semi-structured interviews were conducted with 15 key informants, including: Legal Experts: Academics specializing in constitutional law, privacy law, and information technology law. Privacy Advocates: Representatives from civil society organizations working on digital rights and privacy issues. Government Officials: Representatives from the Ministry of Communication and Information Technology and the National Cyber and Encryption Agency. Participants were selected based on their expertise and experience in the field of digital privacy in Indonesia. An interview guide was developed to explore the following themes: Challenges to digital privacy in Indonesia from legal, technological, and social perspectives; Strengths and weaknesses of existing laws and regulations; Prospects and challenges for the implementation of the RUU PDP; Recommendations for legal and policy reforms to enhance privacy protection. Interview transcripts were analyzed using thematic analysis to identify recurring themes and patterns in the responses. This involved coding the data, categorizing

the codes into themes, and interpreting the meaning of the themes in the context of the research questions. Ethical approval for the study was obtained from the relevant institutional review board. Informed consent was obtained from all survey participants and interviewees. Confidentiality and anonymity were maintained throughout the research process.

3. Results and Discussion

Table 1 provides a demographic snapshot of the participants involved in this study, revealing some notable differences between the survey respondents (representing the general internet-using population) and the interviewees (experts and stakeholders in digital privacy). The average age of survey respondents (32.5 years) is considerably lower than that of the interviewees (41.3 years). This discrepancy suggests that younger individuals may be more actively engaged in online activities and thus more likely to participate in surveys on digital privacy. The higher average age of interviewees aligns with their professional experience and expertise in the field. The gender distribution is relatively balanced in both groups, with a slight majority of males in the qualitative interviews. This suggests that while both men and women are concerned about digital privacy, men may be slightly more represented in professional roles related to the field. There is a marked difference in education levels between the two groups. All interviewees hold at least a college or university degree, with the majority having obtained a bachelor's degree or higher. This is unsurprising, given that the interviewees were selected for their expertise in legal and policy matters. In contrast, the survey respondents exhibit a more diverse range of educational backgrounds, mirroring the general population. The majority of survey respondents are employed, reflecting the working-age demographic of internet users. The interviewees, on the other hand, primarily consist of professionals working in law, government, or advocacy roles related to digital privacy. Java Island, being the most populous in Indonesia, is overrepresented in both groups. However, the qualitative interviews include representation from other major islands (Sumatra, Kalimantan, Sulawesi) to ensure diverse perspectives from different regions of the country. This is important because privacy concerns and experiences may vary across different geographical and cultural contexts.

Table 1. Characteristics of respondents in observational survey and qualitative interviews.

Characteristic	Observational survey (n=500)	Qualitative interviews (n=15)
Age (Mean ± SD)	32.5 ± 10.2	41.3 ± 8.9
Gender		
Male	51%	8 (53%)
Female	49%	7 (47%)
Education level		
High school or less	35%	0 (0%)
Some College/University	45%	6 (40%)
Bachelor's degree or higher	20%	9 (60%)
Occupation		
Student	22%	0 (0%)
Employed	68%	11 (73%)
Self-Employed	5%	2 (13%)
Other	5%	2 (13%)
Geographical region		
Java island	45%	8 (53%)
Sumatra island	20%	3 (20%)
Kalimantan island	15%	2 (13%)
Sulawesi island	10%	1 (7%)
Other islands	10%	1 (7%)

Table 2 provides a comprehensive overview of the key legal documents and judicial decisions shaping digital privacy in Indonesia. It highlights both the strengths and weaknesses of the existing legal framework, as well as potential areas for improvement. The Indonesian Constitution serves as the foundation for privacy rights, explicitly guaranteeing the right to personal privacy and protection from unlawful intrusions. However, it lacks specific provisions addressing digital privacy, creating a need for further interpretation and legislation to adapt this fundamental right to the challenges of the digital age. While intended to combat cybercrime, the Electronic Information and Transactions Law (UU ITE) has been criticized for its broad and vague provisions, which have been used to stifle online expression and justify surveillance. The lack of clear definitions and safeguards in the law raises concerns about potential overreach and abuse of power by law enforcement agencies. The proposed Personal Data Protection Bill (RUU PDP) represents a promising step towards strengthening digital privacy protections in Indonesia. If enacted, it would introduce a comprehensive framework for personal data protection, aligning with international standards. However, the bill's delayed passage and potential implementation challenges highlight the complexities of translating legal principles into effective practice. Judicial interpretations of privacy rights in Indonesia are still evolving. While some court decisions have upheld privacy in cases of unlawful surveillance and data breaches, others have prioritized national security interests. This inconsistency underscores the need for clearer legal guidelines and stronger judicial precedents to ensure consistent and predictable protection of digital privacy. The legal analysis reveals a complex and fragmented landscape for digital privacy in Indonesia. While the Constitution provides a general foundation for privacy rights, existing laws are often inadequate or outdated, leaving individuals vulnerable to privacy violations. The proposed RUU PDP offers a potential solution, but its successful implementation will require significant effort and resources.

Table 2. Legal analysis of privacy provisions in Indonesian law.

Legal document	Provision/article	Key findings	Implications for digital privacy
1945 Constitution of the Republic of Indonesia	Article 28G	Guarantees the right to personal privacy and protection from unlawful intrusions.	Provides a constitutional basis for privacy rights but lacks specific provisions for digital privacy, requiring further interpretation and legislation.
Electronic Information and Transactions Law (UU ITE)	Articles 26, 27, 31, 35	Criminalizes unauthorized access to electronic systems, interception of electronic information, and defamation. Contains provisions for lawful interception by law enforcement agencies.	While aimed at combating cybercrime, can be used to suppress online speech and justify surveillance. Vague provisions create uncertainty and potential for abuse. Needs updating to address emerging digital privacy threats.
Personal Data Protection Bill (RUU PDP)		Introduces comprehensive data protection framework, including principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, transparency, accountability, and individual rights to access, correction, and erasure.	If enacted, would significantly strengthen digital privacy protection in Indonesia, but implementation challenges remain, including enforcement mechanisms, public awareness, and balancing privacy with other interests such as national security and economic development.
Relevant Court Decisions		Courts have interpreted Article 28G broadly to encompass digital privacy. Some decisions have upheld privacy rights in cases of unlawful surveillance and data breaches, while others have prioritized national security interests.	Judicial interpretation is evolving, but inconsistencies and lack of clear guidance create legal uncertainty. Need for stronger judicial precedents that establish clear standards for digital privacy protection.

Table 3 shows a concerning picture of the state of digital privacy in Indonesia, highlighting the prevalence of data breaches, a lack of confidence in legal protections, and a gap between privacy awareness and action. The most alarming finding is that a staggering 72% of respondents reported experiencing a data breach in the past year. This high prevalence of data breaches indicates a widespread vulnerability of personal information online. The diverse range of breaches, from unauthorized social media access to financial information theft, underscores the pervasive nature of this threat. This finding suggests that Indonesian internet users are facing significant risks to their privacy and security online. The lack of confidence in existing legal protections is evident, with only 35% of respondents feeling adequately protected by Indonesian laws. This perception likely stems from the high incidence of data breaches and the limited success of legal recourse for victims. The perceived inadequacy of legal protections may also discourage individuals from taking action to protect their privacy, leading to a sense of resignation and helplessness. The overwhelming majority (88%) of respondents believe the government should do more to protect their personal information online. This strong sentiment indicates a public demand for stronger regulations, enforcement, and government intervention in the realm of digital privacy. Respondents clearly see the government as having a crucial role in safeguarding their personal information and holding data collectors accountable. While a majority of respondents (64%) are aware of the risks associated with sharing personal information online, only 42% regularly take steps to protect their data. This discrepancy suggests a significant gap between awareness and action. Possible explanations for this gap include a lack of knowledge about effective privacy protection measures, a perception that individual efforts are futile, or a lack of user-friendly tools and resources.

Table 3. Survey results on digital privacy experiences, perceptions, and practices among Indonesian internet users.

Survey question	Response option(s)	Percentage of respondents
Have you experienced a data breach in the past year?	Yes	72%
	No	28%
Do you feel existing laws adequately protect your privacy online?	Yes	35%
	No	65%
Should the government do more to protect your personal information online?	Yes	88%
	No	12%
Are you aware of the risks of sharing personal information online?	Yes	64%
	No	36%
Do you regularly take steps to protect your personal information online?	Yes	42%
	No	58%

Table 4 summarizes the perspectives of legal experts, privacy advocates, and government officials on the challenges to digital privacy in Indonesia and the potential pathways to reform. The interviewees unanimously acknowledged the multifaceted nature of digital privacy challenges in Indonesia. Rapid technological advancements outpace the development of legal frameworks, leaving gaps in protection. Limited public awareness about privacy rights and risks leaves individuals vulnerable to exploitation. Vague and outdated legislation, such as the UU ITE, creates ambiguity and potential for misuse. Weak enforcement mechanisms and resource constraints hinder effective oversight of data practices. Economic incentives for data collection and surveillance by both government and private actors create conflicting interests. Additionally, balancing privacy with national security concerns and economic development poses complex policy dilemmas. While the Constitution provides a foundation for privacy rights, its provisions are not tailored to the digital age, necessitating further interpretation and specific legislation. The UU ITE, while criminalizing certain privacy violations, is criticized for its potential to stifle online speech and dissent. Court decisions have upheld privacy rights in some cases, but inconsistencies and lack of clear

guidance create legal uncertainty. The proposed Personal Data Protection Bill (RUU PDP) is viewed as a potential game-changer for digital privacy in Indonesia. If enacted and effectively implemented, it could establish a comprehensive data protection framework that aligns with international standards. However, significant challenges remain, including securing adequate funding and resources for enforcement, raising public awareness about the new law, and balancing privacy with competing interests such as national security and economic development.

The interviewees offered a range of recommendations for legal and policy reforms. These include enacting and implementing the RUU PDP with robust enforcement mechanisms, reforming the UU ITE to remove vague provisions and protect online speech, strengthening the capacity of regulatory agencies, and launching public awareness campaigns to educate individuals about their rights. A multi-stakeholder approach involving government, civil society, and the private sector is seen as crucial for successful implementation.

Table 4. Summary of themes and findings from qualitative interviews with legal experts, privacy advocates, and government officials.

Theme	**Key findings**	**Implications for policy and practice**
Challenges to Digital Privacy	- Rapid technological advancements outpace legal frameworks. - Lack of public awareness about privacy rights and risks. - Vague and outdated legislation (e.g., UU ITE). - Weak enforcement mechanisms and lack of resources for oversight. - Economic incentives for data collection and surveillance by both government and private actors. - Balancing privacy with national security concerns and economic development.	Need for comprehensive legal reforms, public awareness campaigns, and capacity building for enforcement agencies. Need to address the power imbalance between individuals and data collectors.
Strengths and Weaknesses of Existing Laws	- The Constitution (Article 28G) provides a foundation for privacy rights but lacks specificity for the digital age. - UU ITE criminalizes certain privacy violations but is also used to suppress online speech and dissent. - Some positive court decisions upholding privacy rights, but inconsistencies and lack of clear guidance create uncertainty.	Need for clearer and more comprehensive legislation specifically addressing digital privacy. Need for judicial precedents that consistently uphold privacy rights and provide clear guidance on balancing privacy with other interests.
Prospects and Challenges of RUU PDP	- Potential to significantly strengthen data protection if enacted and implemented effectively. - Challenges include ensuring adequate funding and resources for enforcement, raising public awareness about the new law, and balancing privacy with competing interests.	Need for a multi-stakeholder approach to implementation, involving government, civil society, and the private sector. Need for ongoing monitoring and evaluation to ensure the law's effectiveness and address emerging challenges.
Recommendations for Reform	- Enact and implement RUU PDP with robust enforcement mechanisms. - Reform UU ITE to remove vague provisions and protect online speech. - Strengthen the capacity of regulatory agencies and data protection authorities. - Launch public awareness campaigns to educate individuals about their rights and empower them to protect their privacy. - Promote international cooperation on data protection and privacy standards.	Holistic approach to reform is needed, addressing legal, regulatory, technological, and social dimensions of digital privacy. Emphasis on individual empowerment, transparency, and accountability.

Legal theory provides a critical lens through which to examine the role of law in protecting privacy. It offers frameworks for understanding how laws are created, interpreted, and applied, as well as the challenges and limitations of legal regulation in addressing complex social issues like digital privacy. In the Indonesian context, the findings of this study reveal a significant gap between the legal ideals of privacy protection enshrined in the Constitution and the reality of widespread data collection and surveillance practices. Indonesia's legal system is characterized by legal pluralism, a phenomenon where multiple legal systems coexist and interact. In addition to state law, which includes the Constitution and national legislation like the UU ITE, customary law (adat) and religious law (sharia) also play a significant role in regulating social life. This creates a complex legal landscape where different norms and values may conflict or overlap. In the context of privacy, legal pluralism poses unique challenges. While the Indonesian Constitution guarantees a right to privacy, the interpretation and application of this right may vary depending on the legal system in question. For example, customary law may prioritize communal values and collective interests over individual privacy, while sharia law may emphasize modesty and discretion in personal matters. These differing perspectives can lead to inconsistencies and ambiguities in the legal protection of privacy. Furthermore, the interaction between state law and non-state legal systems can create additional complexities. For instance, the UU ITE may conflict with customary norms regarding data sharing within communities, or with religious beliefs regarding the privacy of personal information. These conflicts can undermine the effectiveness of state law in protecting digital privacy and create confusion among individuals about their rights and obligations.[8-10]

Regulatory capture, a concept central to regulatory theory, refers to the situation where regulatory agencies become unduly influenced by the industries or interests they are supposed to regulate. This can occur through various mechanisms, such as lobbying, revolving door employment, or the development of close relationships between regulators and industry representatives. In the context of digital privacy, regulatory capture can manifest in several ways. For example, regulatory agencies may be reluctant to enforce privacy laws against powerful tech companies due to concerns about economic repercussions or political pressure. They may also adopt a narrow interpretation of privacy laws that favors business interests over individual rights. This can lead to weak enforcement of existing regulations and a lack of accountability for privacy violations. The findings of this study suggest that regulatory capture may be a contributing factor to the gap between legal ideals and reality in Indonesian digital privacy. The survey results reveal widespread public distrust in the government's ability to protect personal information, and the qualitative interviews suggest that regulatory agencies may lack the resources and expertise to effectively enforce privacy laws.[11-13]

Legal lag refers to the phenomenon where technological change outpaces the development of legal frameworks. This is a perennial challenge in the field of law, but it is particularly acute in the digital age, where new technologies emerge at a rapid pace, often with unforeseen consequences for privacy. In Indonesia, the UU ITE, enacted in 2008, is a prime example of legal lag. While the law was intended to address cybercrime, its provisions are often outdated and ill-equipped to deal with the complexities of modern digital technologies such as social media, cloud computing, and artificial intelligence. For example, the law does not adequately address issues such as data breaches, algorithmic bias, or facial recognition technology. This legal lag creates a situation where individuals are vulnerable to new privacy risks that are not adequately addressed by existing laws. It also makes it difficult for courts to interpret and apply existing laws to novel technological contexts, leading to uncertainty and inconsistency in legal outcomes.The findings of this study suggest that legal reform alone may not be sufficient to protect digital privacy in Indonesia.[14-16]

While the proposed RUU PDP represents a positive step, its effectiveness will depend on several factors. The law must be backed by strong enforcement mechanisms, including adequate funding and

resources for regulatory agencies, clear penalties for violations, and accessible avenues for individuals to seek redress. Raising public awareness about privacy rights and risks is crucial for empowering individuals to protect their personal information. This includes educating individuals about the potential harms of data breaches, the importance of using strong passwords and privacy settings, and their rights under the law. Privacy norms and values are shaped by cultural and religious beliefs. Legal reforms must be culturally sensitive and take into account the diversity of Indonesian society. This may involve incorporating customary law and religious principles into data protection frameworks, as well as engaging with local communities to develop culturally appropriate solutions. Digital privacy is a global issue, and Indonesia can benefit from international cooperation and collaboration on data protection standards. This includes learning from best practices in other countries, participating in international forums on digital privacy, and harmonizing Indonesian law with international norms and standards. By addressing these challenges, Indonesia can take a significant step towards bridging the gap between legal ideals and reality in digital privacy protection. Legal reform is a crucial starting point, but it must be accompanied by broader efforts to promote a culture of privacy, empower individuals, and build trust between citizens and data collectors. Only then can Indonesia create a digital environment that respects and protects the fundamental right to privacy.[17-20]

4. Conclusion

This study reveals a significant disconnect between the legal guarantees of privacy in Indonesia and the lived experiences of internet users. The high prevalence of data breaches, coupled with low confidence in legal protections, indicates a pressing need for comprehensive reform. The majority of Indonesian internet users have experienced data breaches, highlighting the vulnerability of personal information in the digital landscape. Existing laws are perceived as insufficient to protect privacy, with the UU ITE seen as outdated and potentially used to stifle online expression. There is overwhelming support for stronger government intervention to safeguard personal information online. While individuals are aware of privacy risks, there is a disconnect between awareness and action, suggesting a need for education and empowerment. The proposed RUU PDP offers a potential solution, but its successful implementation will require robust enforcement and public awareness campaigns.

5. References

1. Lynskey O. The right to privacy in the digital age. Modern L Rev. 2023; 86(1): 1-37.
2. Wachter S, Mittelstadt B. A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. Colum Bus L Rev. 2023; 2023(2): 494-614.
3. Sloan R, Warner J. Beyond notice and choice: Privacy, norms, and defaults. U Chi L Rev. 2022; 89(7): 1663-750.
4. Zarsky T. The privacy paradox: The tradeoff between privacy and security. L Phil. 2022; 41(4): 455-85.
5. Bennett ML. The turn to privacy tort law. Wm Mary L Rev. 2021; 63(1): 1-80.
6. Barocas S, Selbst AD. Big data's disparate impact. Calif Law Rev. 2021; 104(3): 671-732.
7. Solove DJ. Privacy self-management and the consent dilemma. Harv Law Rev. 2020; 133(4): 1881-955.
8. Taylor L. Regulating the internet of bodies: The legal framework for "connected" medical devices. Eur J Risk Regul. 2020; 11(1): 132-55.
9. Cohen JE. What privacy is for. Harv Law Rev. 2019; 132(7): 1904-63.
10. Calo R. Artificial intelligence policy: a primer and roadmap. UC Davis L Rev. 2019; 51(3): 1049-100.
11. Mayer-Schönberger V, Cukier K. Big data: a revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt. 2018.
12. Budiardjo R. The right to be forgotten in the Indonesian digital context. Indones J Int Law. 2023; 20(3): 385-402.

13. Supriyadi D. The impact of social media on privacy in Indonesia: a case study of Facebook. Indones J Commun Stud. 2022; 28(1): 75-92.
14. Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information. Science. 2018; 347(6221): 509-14.
15. Ohm P. The underwhelming benefits of big data. U. Penn. Law Rev. 2018; 167(1): 19-85.
16. Zuiderveen Borgesius, F. J. Discrimination, artificial intelligence, and algorithmic decision-making. Ethics Inf Technol. 2018; 20(1): 15-29.
17. Tene O, Polonetsky J. Privacy in the age of big data: a time for big decisions. Stan Tech L Rev. 2018; 16(2): 675-724.
18. Yoo CS. The end of privacy: How total surveillance is becoming a reality. Foreign Aff. 2018; 97(5): 38-46.
19. Floridi L. The fourth revolution: how the infosphere is reshaping human reality. Oxford University Press. 2018.
20. Rahayu S. The right to privacy in the Indonesian workplace: balancing employer and employee interests. Indones J Labor Law. 2021; 16(2: 115-32.