West Science Law and Human Rights
Vol. 3, No. 03, July 2025, pp. 286~291

Personal Data Privacy in Social Media Platform: Governance, Ethics, an Regulatory Measures.

Aprilia Dwi Santoso Putri[1], Rina Arum Prasastyanti[2]
[1,2]Duta Bangsa University

Article Info

Article history:

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

Keywords:

Personal Data Privacy
Social Media Platform
Data Governance
Platform Responbility

ABSTRACT

This study explores the complexities of personal data privacy in the context of social media platforms, and existing regulatory frameworks. Trough a multidisciplinary analytical approach, this study evaluates the relationshipbetween users privacy rights, data management practies by platforms, and corporate legal liability. As a theoretical frameworks, the theory of privacy rights, data governance theory, and the concept of platforms responbilityare used toanalyze this problem. The results of the study revealed that there is a significant gap between the business model of platforms that rely on data extraction and user privacy expectations. Also identified are the limitations of current regulations in the face of rapid technological dynamics. This research contributes to the literature by introducing an integrated privacy governance model, which seeks to accommodate the needs of a more adaptive regulatory stakeholder. These findings have important implications for policy development, industry practices, and improved digital literacy for users.

Corresponding Author:

Name: Rina Arum Prastyanti
Institution Address: Jl. Ki Mangun Sarkoro No. 20, Nusukan, Banjarsari, Surakarta, Indonesia
e-mail: rina_arum@udb.ac.id

1. INTRODUCTION

The advancement of digital technology and the rapid growth of social media platforms has changed the way we socialize, communicate and share information. Behind the convenience and connectivity offered, there are complex challenges related to the privacy of users' personal data that are increasingly becoming a global concern. This research arises from concerns about the power imbalance between users and large technology platforms in regulating personal information. Through this research, we seek to not only recognize the problems, but also provide solutions that can connect the interests of various parties, from individual users to technology platforms, regulators, and civil society. A diverse approach is expected to provide a comprehensive and balanced perspective on data privacy management in the digital era. We hope that this research can contribute to academic discussions, policy development, and increase public awareness about the importance of protecting personal data

privacy on social media platforms. Fundamentally, our goal is to foster an innovative and dynamic digital ecosystem, while respecting the privacy rights and dignity of users.

The rapid growth of social media platforms in the past decade has brought about profound changes in the global information ecosystem. With more than 4.8 billion social media users worldwide [13], the amount of personal data collected, processed and monetized has reached unprecedented levels. The "data as the new oil" paradigm has fueled platform business models that rely on the extraction, analysis, and commercialization of users' personal data, often with devastating repercussions.users themselves are unaware of.

In this study, we seek to answer a number of important questions, namely: (1) How to achieve a balance between the privacy rights of users and the business interests of the platform? (2) What is the most effective data governance framework that benefits from protecting privacy while still supporting innovation? (3) How can platform responsibilities be defined and enforced in the context of varying regulations at the global level?

The research aims to analyze the practices of personal data management by social media platforms, evaluate the effectiveness of existing regulatory frameworks, and develop a privacy governance model that is user-centric but still sensitive to the interests of various stakeholders. This research offers an important contribution in the context of increasing global attention to digital privacy, the emergence of new regulations such as GDPR in Europe, CCPA in California, and PDPA in various Asian countries, as well as public debates about the responsibilities of large tech platforms. The results of this study are expected to inform policy development, industry practices, and public awareness about data privacy.

The theory of the right to privacy has evolved from the idea of "the right to be left alone" to a more comprehensive understanding of control over personal data. In the digital world, it is important to have clear consent, transparency, and control over users over their information. A contextual privacy approach also helps us understand how information should be flowed according to the social context, especially in an era of social media that blurs traditional boundaries.

Data governance discusses the structure and practices of data management throughout its lifecycle. The existing model includes hierarchical approaches, markets, and self-governance. On social media platforms, a co-regulatory approach that combines formal regulation and self-governance is increasingly being considered. Previous studies have identified challenges in implementing effective data governance principles on social media platforms, including information asymmetry, technical complexity, and conflicts of interest [1].

Platform responsibility has been the focus of academic and policy debate in policy in recent years, with perspectives ranging from libertarian approaches that prioritize self-regulation to advocacy for stricter regulation [2], [3]. Platform liability theory combines elements from media law, technology ethics, and the political economy of communication to articulate the platform's obligations to users and society at large [4]. Contemporary debates about platform responsibility also encompass the concept of "algorithmic justice" and accountability for automated decision-making systems that affect user privacy [5].

2. LITERATURE REVIEW

2.1 Privacy Rights Theory and Digital Governance

Privacy rights theory has evolved from Warren and Brandeis's [6] "right to be left alone" to complex frameworks addressing digital governance. Westin [7] established informational self-determination as a core principle, defining privacy as individuals' claim to control when, how, and to what extent their information is communicated.

This foundation remains central to modern privacy law.

Nissenbaum's [8] contextual integrity theory revolutionized privacy scholarship by arguing that privacy expectations are contextual rather than universal. Information flows are appropriate when they conform to specific contextual norms defined by actors, information types, and transmission principles. This framework is particularly relevant to social media platforms where users navigate multiple overlapping contexts within single digital spaces.

Recent scholarship expanded to collective privacy dimensions. Marwick and Boyd (2014) introduced "networked privacy," recognizing that individual privacy decisions affect entire social networks through social graphs and inferential analytics. Kumar et al. (2018) argued that privacy should be understood as a collective good, demonstrating how aggregated individual data can reveal sensitive group information.

Zuboff's [9] surveillance capitalism framework provides critical insight into platform business models, arguing that platforms extract behavioral data to create "behavioral futures markets." This creates "instrumentarian power"—the ability to shape behavior through environmental modification—highlighting structural power imbalances that traditional privacy protections may inadequately address.

2.2 Data Governance Models and Platform Rresponsibility

Data governance literature identifies three primary models: hierarchical (government-led), market-based (industry self-regulation), and network-based (multi-stakeholder collaboration) [10]. Co-regulatory approaches combining formal regulation with industry self-governance have gained prominence as frameworks addressing limitations of pure regulatory and market-based approaches (Marsden, 2011).

Platform responsibility theory emerged as platforms evolved into quasi-governmental entities requiring new governance frameworks. Gillespie [11] reveals how platforms navigate tension between being neutral conduits and active mediators through strategic ambiguity. Van Dijck, Poell, and de Waal [3] propose the "platform society" concept, arguing that platforms have become fundamental infrastructure extending responsibility goes beyond technical aspects to broader social impacts. The literature on algorithm accountability explains how algorithmic systems affect individual privacy and freedom. Pasquale [5] criticizes algorithmic systems that function as “black boxes”, arguing that opacity undermines accountability.

Diakopoulos (2016) proposes a model of accountability based on transparency, clarity, and auditability, although he recognizes the conflict between transparency and competitive advantage. The idea of fiduciary responsibility for data management on platforms has attracted attention. Balkin (2016) argues that platforms should be viewed as “information fiduciaries” who have a legal responsibility to maintain fidelity, care and confidentiality. McDonald and Cranor (2021) argue that fiduciary responsibility can provide more effective privacy protection than models that rely on consent, although major changes in the legal framework are required.

2.3 Comparative Regulatory Frameworks and Implementation Challenges

Regulatory responses internationally show diverse philosophical approaches in seeking a balance between privacy protection and economic progress. The GDPR in the European Union is a comprehensive rights-based regulation with international reach. Hoofnagle and colleagues (2019) note the so-called “Brussels effect” of the GDPR, whereby EU regulations become global standards through market mechanisms. Bradford (2020) examines how European privacy standards became an international norm thanks to the spillover effect of regulation. Meanwhile, the United States implements sectoral regulations with different provisions for each industry. Solove and Hartzog [12] reveal consistent principles as well as problems in the existing legal framework.

The California Consumer Privacy Act (CCPA) represents a major shift in privacy regulation at the state level. Determann (2021) observes that state-level regulation brings challenges to compliance, while potentially being more aligned with US legal traditions. In Asia, jurisdictions are developing hybrid strategies that combine aspects from Europe and America. Greenleaf (2021) mentions several recurring themes, including provisions for government access to data localization requirements, and emphasis on economic development. Singapore's PDPA exemplifies hybrid approaches incorporating European-style principles while maintaining business innovation flexibility.

User behavior research reveals complex relationships between privacy concerns and actual behavior. The "privacy paradox" (Norberg et al., 2007) describes users expressing strong privacy concerns while continuing to share personal information. Solove [12] argues that apparent behavioral inconsistencies may reflect rational responses to limited choices rather than inconsistent preferences.

Digital literacy research emphasizes its importance in enabling meaningful privacy choices. Hargittai and Marwick (2016) find that higher digital literacy correlates with privacy-protective behaviors, though even digitally literate users struggle with complex privacy settings. Park (2019) proposes privacy literacy frameworks encompassing technical knowledge and critical thinking skills.

3. METHODS

3.1 Research Approach

The study adopts a mixed methodological approach that combines policy analysis, comparative case studies, and qualitative content analysis. This multidisciplinary approach allows for a comprehensive understanding of the complex dynamics of data privacy on social media platforms.

3.2 Data Collection

Data for this study were obtained from various sources: (1) privacy policy documents from the five largest social media platforms; (2) regulatory frameworks from different jurisdictions (the European Union, the United States, and five Asian countries); (3) case studies of data breach and privacy litigation (2018-2023); and (4) semi-structured interviews with 25 privacy experts, regulators, and industry executives.

3.3 Data Analysis

Data were analyzed using a thematic approach to identify patterns, tensions, and best practices in privacy governance. Framework analysis is used to map regulatory approaches across jurisdictions, while critical discourse analysis is applied to platform privacy policies to uncover inherent assumptions and positions of power.

3.4 Research Limitations

The study has several limitations, including a focus on dominant social media platforms that may not represent the entire landscape, data access challenges due to information ownership, and rapidly changing regulatory dynamics that may affect the long-term relevance of the findings.

4. RESULTS AND DISCUSSION

Analysis of how data is managed by social media shows a difference between what they claim about privacy and the reality in the field regarding data collection. Although they stated that they protect user privacy, these platforms still collect more data both in number and type, with an average increase of 40% in data variation from 2018 to 2023. Many of these platforms implement complex consent methods, which force users to agree to extensive data collection. In addition, there are 127 technical terms in the privacy policy that are not clearly explained.

The platform also implements location tracking through non-transparent methods, such as the use of photo metadata, WiFi triangulation, and network pattern analysis. Face technology known as facial recognition brings challenges to privacy, with the potential misuse of biometric data for advertising and monitoring. A review of the international regulatory framework shows

that there are three dominant regulatory models: the rights-based model in the European Union guided by the GDPR, the intermittent sectoral model in the United States, and the mixed model in Asia-Pacific that is highly dependent on the local context.

Obstacles in the implementation of regulations include limited resources for enforcement and difficulties in understanding the latest technology. The results of interviews with a number of stakeholders indicate that many regulators consider the current regulations to be inadequate and more supportive of the co-regulation approach. Executives in the industry are aware of the tension between their business and privacy protection. Privacy experts argue that the current consent mechanism is ineffective and propose the need for a better privacy plan.

This study concludes that the traditional concept of consent is no longer relevant for data management on social media. There is a need to switch to "dynamic agreement" that can adapt to technological advances and changing user demands. This research also highlights the responsibility of the platform as a development in legal doctrine, including the obligation to maintain and clarity regarding algorithm accountability. The power imbalance between users and platforms is also a concern, with asymmetric information and technology identified as the main issue.

From the results of this research, an integrated privacy governance model was developed, which includes principle-based regulation, improvement of self-management mechanisms, technical privacy tools, and user empowerment through education. The framework for implementation is divided into three stages, starting from building the basis, implementing experiments, to full implementation.

This study provides theoretical contributions in various aspects, such as the development of privacy theory for digital platforms, governance models involving many stakeholders, and responsibilities from platforms. The practical implications include the development of technical capabilities by regulators, the application of privacy principles by the platform, as well as the improvement of digital literacy and awareness of privacy rights among users.

5. CONCLUSION

This research confirms that data privacy on social media platforms is a complex challenge that requires a multidimensional approach. The findings point to significant gaps between platform practices and user privacy expectations, evolving regulatory frameworks that often lag behind technological innovation, and the potential value of multi-stakeholder governance approaches. Platform responsibilities need to be redefined to include not only legal compliance but also ethical obligations to users and society.

ACKNOWLEDGEMENTS

This research would not have been possible without the support and contributions from various parties who have taken the time, shared their knowledge, and placed their trust in us. From the bottom of our hearts, we would like to express our deepest gratitude to the respondents from authorities, social media platforms, and civil society organizations who have been willing to share their views, experiences, and valuable insights on the issue of personal data protection and digital governance.

We would also like to thank Dr. Rina Arum Prastyanti, S.H., M.H., as our academic supervisor, for her guidance, encouragement, and constructive input during the research and writing process of this article. The participation and support of various parties has enriched our understanding of this complex topic. We recognize that any errors that may be contained in this article are the sole responsibility of the authors.

REFERENCES

[1] Zubof, S. (2019). The age of surveillance capitalism: The flight for a human future at the new frontier of

power. PublicAffairs.
[2] Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press.
[3] Van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world.* Oxford University Press.
[4] Helberger, T. (2018). Governing online platform: From conteted to cooperative responsibility. The Information Society, 34(1), 1-14. https://doi.org./.10.1080/1369118X.2019.1573914
[5] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Harvard University Press.
[6] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193-220.
[7] Westin, A.F. (1967). Privacy and freedom. Atheneum.
[8] Nisenbaum, H. (2010). *Privacy in Context: Technology, policy, and the integraty of social life.* Stanford University Press.
[9] Zubof, S. (2019). The age of surveillance capitalism: The flight for a human future at the new frontier of power. PublicAffairs.
[10] Webber, R. H. (2018). Governance of data and artifical intelligence. *Journal of the Internet Law, 22*(3), 3-14.
[11] Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press.
[12] Solove, D. J. (2021). The myth of the privacy paradox. *George Washington Law Review, 89*(1), 1-51.
[13] Kemp,S. (2023). Digital 2023: *Global digital overview.* DataReportal. https://datareportal.com/reports/digital-2023-global-overview-report