Qonun: Jurnal Hukum Islam dan Perundang-Undangan, 9 (2), 2025: 359-388
https://journal.uinsi.ac.id/index.php/qonun/index
DOI: https://doi.org/10.21093/qj.v9i2.12656
E-ISSN: 2774-3209

DIGITAL ADVERTISING AS A THREAT TO CONSUMER PRIVACY: A COMPARATIVE LEGAL ANALYSIS

Nurlaily*
Universitas Internasional Batam
Lu Sudirman**
Universitas Internasional Batam
Mimi Sintia Mohd Bajury***
Universiti Teknologi MARA, Malaysia
Hari Sutra Disemadi****
Universitas Internasional Batam
Ninne Zahara Silviani*****
Universitas Internasional Batam

Abstract

The rapid growth of digital advertising as a key component of the digital economy has intensified concerns over the protection of personal data and privacy rights. The primary legal problem addressed in this research is the inability of Indonesia's current data protection framework to adequately regulate data-driven digital advertising practices and prevent unlawful identification of individuals, particularly when compared to South Korea's more advanced regulatory regime. This study aims to comparatively analyze the legal frameworks governing personal data and privacy protection in digital advertising in Indonesia and South Korea and to propose a legal development model for Indonesia. This research employs a normative legal research method using a comparative statutory approach, focusing on Indonesia's Law on Personal Data Protection and South Korea's Personal Information Protection Act, along with its enforcement regulations. Legal norms are examined through statutory provisions and supported by relevant

* drnurlaily@uib.ac.id
** lu@uib.ac.id
*** mimisintia@uitm.edu.my
**** hari@uib.ac.id
***** ninne@uib.ac.id

legal and academic literature. The findings demonstrate substantial regulatory disparities between the two countries. South Korea has established a comprehensive and technologically responsive legal framework, incorporating detailed data classification, recognition of pseudonymized data, strict profiling limitations, and strong institutional enforcement. In contrast, Indonesia's legal framework remains structurally limited, relies heavily on undelivered implementing regulations, and insufficiently addresses indirect identification and advanced data-processing practices in digital advertising. This study proposes targeted legal reforms for Indonesia, including the integration of pseudonymization, enhanced data classification, criminalization of unlawful identification, and mandatory tracking notifications to strengthen privacy protection in the digital advertising ecosystem.

Keywords: Consumer Privacy; Digital Advertising; Consumer Protection;

A. Introduction

With the rise of digital transformation and consequently, digital economy, privacy becomes a serious concern for many people.[1] One common practice in digital economy is digital advertising, which leverages digital spaces to advertise many products and services.[2] This practice raises many concerns regarding the protection of consumer privacy within many digital spaces,[3] which necessitates a serious legal analysis. Indonesia and South Korea are particularly known in Asia and throughout the world for having a massive digital economy, with digital advertising as one of the main components. While Indonesia is still a middle-income country, its growing economy is expected to become of the biggest in the world, thanks to the existence of digital

[1] Mohammad Aslam Khan, "Mega Risks: Digital Transformation and Sustainability," in *Cities and Mega Risks: COVID-19 and Climate Change*, ed. Mohammad Aslam Khan (Cham: Springer International Publishing, 2022), 81–111, https://doi.org/10.1007/978-3-031-14088-4_4.

[2] Micael Dahlen and Sara Rosengren, "If Advertising Won't Die, What Will It Be? Toward a Working Definition of Advertising," *Journal of Advertising* 45, no. 3 (2016): 334–45, https://doi.org/10.1080/00913367.2016.1172387.

[3] Simone Aiolfi, Silvia Bellini, and Davide Pellegrini, "Data-Driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising," *International Journal of Retail & Distribution Management* 49, no. 7 (January 2021): 1089–1110, https://doi.org/10.1108/IJRDM-10-2020-0410.

technologies.[4] South Korea, on the other hand, is one of the leading countries in the world when it comes to technological advancements,[5] making it one of the earliest adopters of digital technologies, and now one of the most successful.[6] By delving into the intricacies of their respective legal systems, the study aims to uncover the effectiveness, strengths, and potential gaps in the protection mechanisms currently in place.

Advertising plays a key role in the success of many businesses around the world, as it helps spread the value of certain products and services to the market.[7] Not only that, advertising can be targeted to certain audience, who have a very high chance of becoming consumers. This significant role of advertising has made advertising itself an industry, where advertisers implement advertising strategies that are finely tuned to the extent that messages and experiences are customized for individual recipients.[8] The role of advertising is further enhanced with the advent of digital technologies, which allows advertisers reach wider audience, or target an even more specific audience with better accuracy.[9] However, digital technologies also

[4] Majid Khalaf Alshammari et al., "Social and Psychological Problems and Their Relationship with Several Variables among University Students," *Review of Economics and Finance* 21 (2023): 426–29, https://doi.org/10.55365/1923.x2023.21.44.

[5] Marina Reshetnikova, Irina Pugacheva, and Alina Evseevicheva, "China or South Korea: A Comparative Analysis of Innovative Development," in *E3S Web of Conferences*, vol. 295, 2021, 1–9, https://doi.org/10.1051/e3sconf/202129501060.

[6] John Nixon, "Digitalization Deployed: Lessons Learned from Early Adopters," in *Proceedings of the Annual Offshore Technology Conference*, vol. 2020-May, 2020, 1–7, https://doi.org/10.4043/30794-ms.

[7] Remziye Terkan, "Importance of Creative Advertising and Marketing According to University Students' Perspective," *International Review of Management and Marketing* 4, no. 3 (2014): 239–46.

[8] James F. Hamilton, "A New Take on Digital Advertising: Theory, History, and Society," *Advertising & Society Quarterly* 18, no. 1 (2017): 1–41, https://doi.org/10.1353/asr.2017.0006.

[9] John Sinclair, "Magazines and Advertising in the Digital Age," in *The Handbook of Magazine Studies*, 2020, 105–19, https://doi.org/10.1002/9781119168102.ch8.

introduce sophisticated methods of data collection and targeted advertising that pose unprecedented challenges to consumer privacy.[10] Indonesia and South Korea, despite their geographical proximity, exhibit varying degrees of regulatory robustness and enforcement efficacy in this context. The juxtaposition of these two legal environments offers a unique perspective on how differing legal traditions and societal values influence the evolution of privacy laws and their implementation.

An in-depth exploration of Indonesia's and South Korea's legal frameworks can reveal the nuances of their approaches to digital advertising and privacy protection, which are inherently affected by the economic and market conditions of each country. The comparison of Indonesia's and South Korea's legal framework can also show the level of legal developments from both countries, and how much those legal developments can contribute to the growing needs of protection for privacy in the digital age. The focus on primary law sources as the main object of comparison ensures a comprehensive understanding of the legal principles at play without necessitating the collection of primary data, thereby streamlining the research process and emphasizing the study's reliance on existing legal documents and scholarly commentary.

The culmination of this research can provide insightful findings into the bigger picture of Indonesia's and South Korea's legal developments, particularly around privacy protections in the digital advertising sphere. It can highlight the ways in which legal mechanisms are structured and deployed, shedding light on the broader implications for international privacy standards and the global digital economy. Through this comparative lens, the study contributes to the ongoing dialogue on the harmonization of privacy protections and the challenges of regulating digital advertising in a manner that respects and upholds the privacy data subjects.

[10] Dylan A Cooper et al., "Privacy Considerations for Online Advertising: A Stakeholder's Perspective to Programmatic Advertising," *Journal of Consumer Marketing* 40, no. 2 (January 2023): 235–47, https://doi.org/10.1108/JCM-04-2021-4577.

The literatures on privacy have grown over the years, as we go deeper into the digital age, with AI dominance in the horizon looking forward. Digital economy itself has long been associated with privacy concerns, particularly because of its heavy reliance on data, as highlighted by a study focusing on data and its economic values.[11] One of the key aspects of this study is the classification of data, which is essential in analyzing not only the values of data, but also the possible privacy risks in poses. The risks are then identified from many forms of data management practices, throughout many processes, from data collection to data maintenance. Another study also supports the same narrative, particularly on the reliance of data on the digital economy.[12] The study even suggests that the digital economy is becoming the economy itself, indicating that digital technologies would eventually take over the entirety of the economic system, which in the end increases the reliance on data even more.

From the legal standpoint, the legal implication of this reliance on data is important to be analyzed, particularly in the realm of privacy and data protection laws. A study analyzing this highlights the importance of upholding privacy laws and data protection measures, as many digital practices have helped the massive aggregation of data for digital advertising purposes, and subsequently threaten the privacy of many people.[13] The study also highlights the problematic network of digital advertising, which often involves third parties that might not be subject to adequate compliance for data protection. Another study also supports these findings, by crucially highlighting the lack of comprehensive regulation for tackling issues relevant to digital advertising, despite the serious and easily identifiable ethical

[11] David Nguyeni and Marta Paczosi, "Measuring the Economic Value of Data and Cross-Border Data Flows : A Business Perspective," *OECD Digital Economy Papers*, no. 297 (2020): 1–47, https://doi.org/10.1787/20716826.

[12] L Narayana Swamy, "The Digital Economy: New Business Models and Key Features," *International Journal of Research in Engineering, Science and Management* 3, no. 7 (July 2020): 118–22.

[13] José Estrada-Jiménez et al., "Online Advertising: Analysis of Privacy Threats and Protection Approaches," *Computer Communications* 100 (2017): 32–51, https://doi.org/10.1016/j.comcom.2016.12.016.

implications.[14] Despite the emphasis on future legal development, the study itself doesn't provide the necessary foundation for future legal developments, as it doesn't outline the aspects that actually need to be covered by future legislative measures.

Ultimately, the literature analysis outlines the significant gap in fully understanding the legal implications of digital advertising, particularly in a country with growing digital economy like Indonesia and a country with one of the most advanced integration of digital technology like South Korea. While analyzing the legal implications of this particular topic is essential, the identification of these implications need to be utilized as a lens to analyze the relevant regulatory frameworks around data privacy in the context of e-commerce in Indonesia and South Korea. The novelty of this study stems mainly from its core objective of dissecting this highly specific legal topic, by narrowing the focus from data privacy as a general concern in the e-commerce environment to a more specific legal topic that needs to be dissected according to the relevant regulations. The study also aims to further fill the gap in the literature by identifying the existing gaps in the regulatory framework and how those gaps should be tackled. Additionally, this study also aims to provide a model of legal development to tackle the identified issues in regard to the legal implications, particularly for Indonesia as the less developed digital economy between the two.

The research method used is normative legal research method. Normative legal research method is a systematic approach to analyzing legal norms and principles to derive conclusions and recommendations based on legal standards and values.[15] This method focuses on examining legal texts, doctrines, and judicial decisions to

[14] Zaki Mahmed Channak et al., "Business Ethics in E-Commerce – Legal Challenges and Opportunities," *Access to Justice in Eastern Europe* 6, no. Special Issue (2023): 1–16, https://doi.org/10.33327/AJEE-18-6S007.

[15] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 289–304, https://doi.org/10.37253/jjr.v24i2.7280.

understand and interpret legal rules and their implications.[16] This research employs the comparative legal research method, focusing primarily on the examination of the legal frameworks in both Indonesia and South Korea. Through this method, the study scrutinizes the variations and disparities in the legal structures governing data protection and privacy in digital advertising practices between the two countries.

South Korea is specifically chosen as a comparison to Indonesia because of how developed the country already is in its adaptation of technology, along with its fairly reputable legal framework. Instead of the typical benchmark, the GDPR, the South Korean perspective can perhaps provide a more relevant Asian viewpoint, where the goal rapid growth is balanced with growing concerns regarding privacy.[17] Not to mention, South Korea is a prime example of successful transition from a developing economy to one of the most developed in the world, representing an adaptable roadmap of development that Indonesia can follow. By meticulously analyzing the legislative provisions, regulations, and judicial precedents in Indonesia and South Korea, the research aims to provide a comprehensive understanding of how each jurisdiction addresses and regulates privacy within the realm of digital advertising. Secondary data used in this research are Law No. 27 of 2022 on Personal Data Protection, Law No. 8 of 1999 on Consumer Protection, Personal Information Protection Act, and Enforcement Decree of the Personal Information Protection Act.

B. Discussion

[16] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463–78, https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601.

[17] Despite the strong prevalence of surveillance in the country for security-related purposes, the concerns regarding privacy rights continue to be raised by Koreans as the technology involved is getting more developed than ever. *See* Tonghoon Kim and David J. Atkin, "How Government Surveillance Policies Modify SNS Use in South Korea," *Journal of Information Policy* 9 (December 1, 2019): 214–37, https://doi.org/10.5325/jinfopoli.9.2019.0214.

1. Privacy Risks of Digital Advertising and Their Legal Implications

Digital advertising has become an inseparable aspect of e-commerce, as it has helped many business actors promote their products and services to many potential consumers.[18] The numerous potentials brought by digital advertising has also unlocked many potentials of business that are otherwise struggling to reach many potential customers and compete with other businesses that already have certain amount of influence in their relevant market. Digital advertising has become so advanced that it can be done in many digital platforms simultaneously in a very fast manner, significantly improving productivity, brand awareness, and sales.[19] Data is the main driver of these developments, as it fuels all kinds of digital technology utilization, subsequently making it an important commodity in Industry 4.0. Data is even considered more important than some of the most valuable traditional commodities, like oil, indicating its significant economic value.[20]

Therefore, it's of paramount importance to understand the nature of data utilization in order to truly understand the implications of digital advertising. This is even more important when the legal aspects of such technical acts are taken into account, outlining the interplay between many legal spheres. The very first aspect of data is the collection of data itself. Data is collected from many sources, including user interactions on websites, social media platforms, mobile applications, which can affect even the physical-world of data

[18] Reza Nur Rosiyana et al., "A New Digital Marketing Area for E-Commerce Business," *International Journal of Research and Applied Technology (INJURATECH)* 1, no. 2 (December 2021): 370–81, https://doi.org/10.34010/injuratech.v1i2.6765.

[19] Yogesh K Dwivedi et al., "Setting the Future of Digital and Social Media Marketing Research: Perspectives and Research Propositions," *International Journal of Information Management* 59 (2021): 1–37, https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102168.

[20] Jan Michael Nolin, "Data as Oil, Infrastructure or Asset? Three Metaphors of Data as Economic Value," *Journal of Information, Communication and Ethics in Society* 18, no. 1 (2020): 54–69, https://doi.org/10.1108/JICES-04-2019-0044.

subjects.[21] This data can range from basic information such as names and email addresses to more sensitive details like browsing habits, location data, and purchasing behavior. The aggregation of this data allows advertisers to create detailed consumer profiles, which can then be used to deliver highly targeted advertisements.

The significance of data in the current state of society is nothing less than essential. Data is used in many facets of life, and is increasingly getting more and more importance, as the integration of digital technologies continue to be supported. In digital advertising, data can provide relevant information for electronic systems, to ensure that the advertising is shown to the relevant users of that electronic systems. This ability to target the correct audience for an advertising can significantly increase the chances that the advertised products and services are going to be looked at and eventually bought. Ultimately, these potentials positioned data at the very center of Industry 4.0, as an essential commodity. However, much like other commodities, the utilization of data can also raise concerns over illicit practices, from the how the data is collected and how it's being utilized.

Regulatory philosophies concerning privacy risks in digital advertising fundamentally revolve around balancing the protection of individual privacy rights with the promotion of innovation and economic growth. At the core of these philosophies is the principle of informed consent, which asserts that individuals should have clear, comprehensible information about users' data that are going to be collected, processed, and utilized. Informed consent therefore needs to be critically analyzed and undergo intense scrutiny to ensure that privacy of data subjects is adequately protected.[22] Additionally, the principle of transparency requires data controllers to be open about their data handling practices, providing consumers with easy access to

[21] Yinhao Jiang et al., "Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures," *Cryptography*, 2024, https://doi.org/10.3390/cryptography8010005.

[22] Anna Sexton et al., "The Role and Nature of Consent in Government Administrative Data," *Big Data and Society* 5, no. 2 (2018): 1–17, https://doi.org/10.1177/2053951718819560.

their own data and the ability to correct inaccuracies.[23] Accountability is also a crucial component in ensuring that organizations are held responsible for protecting personal data and adhering to established privacy regulations. Finally, the regulatory approach often emphasizes the need for robust security measures to protect against data breaches and unauthorized access. Together, these principles form a comprehensive framework designed to safeguard consumer privacy while enabling the benefits of digital advertising.

The dynamics around this topic ultimately highlights the ongoing race between technology and legislation.[24] Technology itself is important for the better of humanity, but the power it can give can also be dangerous when left unchecked. Therefore, legislation must be able to continuously adapt to the advancement of technology and how it affects the lives of many people. From the legal sphere of privacy, the utilization of data in digital advertising outlines a serious but often overlooked paradox. The paradox is how consumers as users of many electronic systems express concerns over privacy but often provide personal information for conveniences or benefits.[25] This is hugely attributed to the fact that tech companies have deep knowledge on human psychology gathered from various studies, enabling them to create electronic systems that can take advantage of human behavior tendencies.[26] However, from the legal standpoint, this must be analyzed from different perspectives. On one hand, it shows the

[23] Claudia Quelle, "Not Just User Control in the General Data Protection Regulation," in *Privacy and Identity Management. Facing up to Next Steps*, ed. Anja Lehmann et al. (Cham: Springer International Publishing, 2016), 140–63, https://doi.org/10.1007/978-3-319-55783-0_11.

[24] Monique Kalsi, "Still Losing the Race with Technology? Understanding the Scope of Data Controllers' Responsibility to Implement Data Protection by Design and by Default," *International Review of Law, Computers & Technology*, 2024, 1–23, https://doi.org/10.1080/13600869.2024.2324546.

[25] Ruwan Bandara, Mario Fernando, and Shahriar Akter, "Explicating the Privacy Paradox: A Qualitative Inquiry of Online Shopping Consumers," *Journal of Retailing and Consumer Services* 52 (2020): 1–9, https://doi.org/10.1016/j.jretconser.2019.101947.

[26] Hagar Afriat et al., "'This Is Capitalism. It Is Not Illegal': Users' Attitudes toward Institutional Privacy Following the Cambridge Analytica Scandal," *Information Society* 37, no. 2 (2020): 115–27, https://doi.org/10.1080/01972243.2020.1870596.

dependency and reliance on technologies, particularly digital technologies, which can be detrimental to many aspects of personal freedom and security. On the other hand, it also shows how developed current society is, especially within the context of e-commerce, where productivity has increased significantly and also contributed to the increase in trade volumes.

Therefore, the legal system must be able to balance the rights of consumers as users of electronic systems, while also ensuring that they're aware of what they're giving consent to regarding their data and how those data are going to be utilized for their own benefits along with the benefits of electronic system providers. It must also be capable of continuously adapting to the changes in the development of the relevant technologies, which can tip the balance between privacy, convenience, and economic growth.[27] The legal system must also be able to promote growth, particularly in the digital sector, as many different types of technologies are continuously being developed. This is even more important the world is transitioning from Industry 4.0 era into the Society 5.0 era, with the utilization of artificial intelligence, which also relies on the collection and utilization of data in training its model.[28]

Both Indonesia and South Korea are no strangers to data privacy issues.[29] However, Indonesia has a significantly worse track record regarding the protection of privacy rights in the digital space, due to the scale of the data breach and how it often targets the public sector,

[27] Larry Ozeran, Anthony Solomonides, and Richard Schreiber, "Privacy versus Convenience: A Historical Perspective, Analysis of Risks, and an Informatics Call to Action," *Applied Clinical Informatics* 12, no. 2 (2021): 274–84, https://doi.org/10.1055/s-0041-1727197.

[28] Etieno Enang, Mahdi Bashiri, and David Jarvis, "Exploring the Transition from Techno Centric Industry 4.0 towards Value Centric Industry 5.0: A Systematic Literature Review," *International Journal of Production Research* 61, no. 22 (2023): 7866–7902, https://doi.org/10.1080/00207543.2023.2221344.

[29] South Korea has faced numerous data breaches to its digital spaces, showing that despite the overall robust system against issues that can be exploited, the country is not immune to privacy-threatening problems. *See* Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10, no. 1 (January 3, 2024): 1–20, https://doi.org/10.20956/halrev.v10i1.5016.

which holds a much bigger volume of sensitive data.[30] For example, in November 2023, the General Elections Commission (KPU) suffered a massive cyberattack that reportedly compromised the personal data of over 204 million voters, which included National Identification Numbers (NIK) and family card details.[31] Furthermore, in June 2024, Indonesia's digital sovereignty faced a massive blow when the Temporary National Data Center (PDNS) was paralyzed by a 'Brain Cipher' ransomware attack, locking critical data from 282 central and regional agencies and disrupting immigration services for weeks due to a systemic absence of backup protocols, while also solidifying Indonesia's position as one of the worsts in the world against data breaches.[32] These cases provide an even bigger threat in the context of e-commerce today, as it can provide a massive source of illegally-obtained data that can easily be bought by advertisers, which in turn can be used to negatively affect consumer's autonomy in the e-commerce spaces through various methods of advanced data analytics.

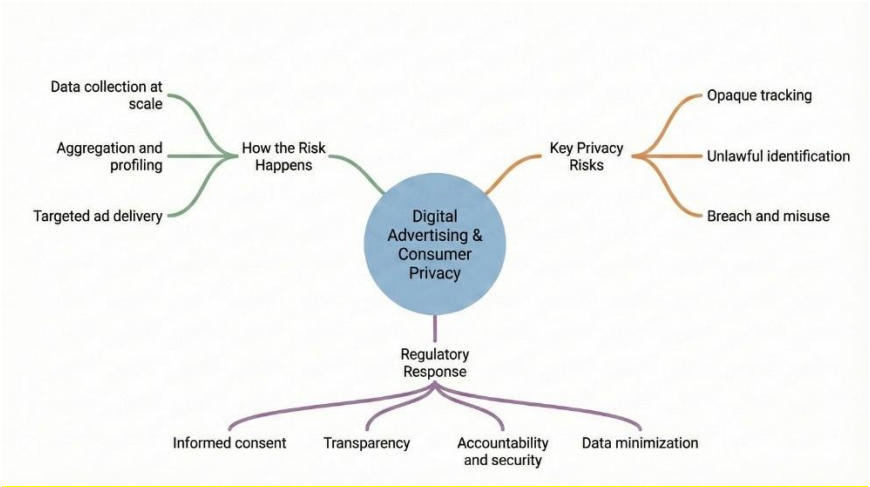
Below is an overview of the privacy implications and how the ideal normative structures should respond to them, in the form of mind map.

Figure 1. Mind Map of Digital Advertising, Privacy Risks, and Regulatory Needs

[30] Imanuel Toding Bua and Nur Isdah Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024," *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 2 (May 23, 2025): 100–114, https://doi.org/10.62383/desentralisasi.v2i2.653.

[31] Muhamad Rizki and Surgana Surgana, "Data Breach of General Elections Commission: Causes and Prevention Efforts," *Jurnal Sistem Informasi Dan Teknologi Informasi* 2, no. 1 (January 1, 2025): 157–60, https://doi.org/10.33197/justinfo.v2i1.1793.

[32] Fariz Fadliansyah et al., "Evaluasi Pembelajaran Dari Kasus Kebocoran Data Di Indonesia Sebagai Negara Dengan Data Breach Terbesar Ke-8 Dunia," *TEKNOBIS: Jurnal Teknologi, Bisnis Dan Pendidikan* 3, no. 2 (October 19, 2025): 272–77, https://jurnalmahasiswa.com/index.php/teknobis/article/view/3025.



Source: Researchers' illustration

An effective regulatory framework regarding this would be the kind that can align many aspects of concerns within the digital sphere, to create a wall of legal compliance that can guarantee the balance between those aspects. Within the context of digital advertising, the legal framework must be able to create a mechanism of compliance that can promote ethical digital advertising practices.[33] Transparency, as highlighted by the broader philosophical implication of regulatory development, also remains as one of the essential aspects of the legal framework for privacy and data protection, to eventually promote it as a part of ethical digital advertising practices. Additionally, ethical advertising should adhere to data minimization principles, ensuring that only the necessary data is collected and retained for the shortest time possible.[34]

As advancements in artificial intelligence and machine learning continue to enhance the precision and personalization of digital advertisements, the urgency to regulate the utilization of data for

[33] Kelly D. Martin and Patrick E. Murphy, "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science* 45, no. 2 (2017): 135–55, https://doi.org/10.1007/s11747-016-0495-4.

[34] Brahmantyo Suryo Satwiko, "Privacy and Data Protection: Indonesian Legal Framework," *Corporate and Trade Law Review* 1, no. 2 (2021): 98–118, https://doi.org/10.21632/ctlr.1.2.98-118.

digital advertising becomes even more crucial.[35] The rapid evolution of artificial intelligence, machine learning, and data analytics can significantly outdo the speed at which legislation is developed and implemented. This can create a serious risk for consumer privacy as it can be exploited by certain digital advertising practices such as behavioral targeting and cross-device tracking, among many others. Lawmakers must proactively anticipate these technological trends and implement forward-thinking regulations that can accommodate growth while robustly protecting consumer privacy. Therefore, normative analysis is crucial to evaluate the adequacy of current regulations in addressing these rapid advancements. By systematically assessing and updating the relevant legal frameworks, a legal system can reflect upon the shortcomings and future challenges that it must be able to face, to ensure the continued harmony between technological and societal development.

From the perspective of Indonesian consumer law, these issues are inherently relevant, as the privacy of consumers in e-commerce spaces are part of their rights in the modern context of commerce. The implication is that the mismanagement or unauthorized dissemination of personal data constitutes a direct violation of the consumer's statutory right to security and comfort. Therefore, legal liability for e-commerce platforms extends beyond mere transactional disputes to encompass the protection of the consumer's digital identity as a fundamental component of the service itself. As the technology utilized for advertising is getting even more advanced, the volume of data needed also grows, which in turn creates even more implications on data privacy. Therefore, a robust regulatory framework must be able to address these challenges by applying the concept of "privacy by design",[36] where the core objective of ensuring privacy is embedded

[35] Sheshadri Chatterjee and N. S. Sreenivasulu, "Personal Data Sharing and Legal Issues of Human Rights in the Era of Artificial Intelligence: Moderating Effect of Government Regulation," *International Journal of Electronic Government Research* 15, no. 3 (2019): 21–36, https://doi.org/10.4018/IJEGR.2019070102.

[36] Cristina Del-Real, Els De Busser, and Bibi van den Berg, "A Systematic Literature Review of Security and Privacy by Design Principles, Norms, and Strategies for Digital Technologies," *International Review of Law, Computers & Technology* 39, no. 3 (September 2, 2025): 374–405, https://doi.org/10.1080/13600869.2025.2457227.

within every part of data ecosystems for e-commerce and digital advertising, from data collection to data processing.

2. Comparative Analysis of Data Protection and Privacy In Indonesian and South Korean Digital Advertising

Indonesia has tried to accommodate the development of digital technology many times by introducing key regulations. This effort started as early as 2008, with the enactment of Law No. 11 of 2008 on Electronic Information and Transaction (EIT Law). This law was the first step in acknowledging what was to come from the development of digital technology in Indonesia.[37] This law has been revised twice, with the first revision through Law No. 19 of 2016 on Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (First Revision of EIT Law) and the latest one through Law No. 1 of 2024 on Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions (Second Revision of EIT Law). The EIT Law, along with its provisions, provides the basic framework for digital governance, with provisions covering many aspects of the digital world, including privacy, data transmission, and basic conducts within the digital space.

However, it wasn't until the enactment of Government Regulation No. 71 of 2019 on Implementation of Electronic Systems and Transactions (Government Regulation on EIT Implementation) did Indonesia have concrete set of provisions regarding data and privacy for digital environments. This regulation brought forth many concrete provisions that the EIT Law lacked, such as the responsibilities and the key principles for data collection, processing, and protection, along with data security.[38] However, the set of provisions from this regulation still didn't meet the dire need for a comprehensive legal framework for data privacy and protection, which was then fulfilled by the enactment of Law No. 27 of 2022 on

[37] Franciscus Xaverius Wartoyo and Yuni Priskila Ginting, "Convergence of Law and Technology Through Optimization of Pancasila," *Journal of Digital Law and Policy* 1, no. 2 (2022): 61–72, https://doi.org/10.58982/jdlp.v1i2.139.

[38] Zawil Fadhli, Sri Walny Rahayu, and Iskandar A. Gani, "Perlindungan Data Pribadi Konsumen Pada Transaksi Paylater," *Jurnal Hukum Magnum Opus* 5, no. 2 (2022): 119–32.

Personal Data Protection (PDP Law). The PDP Law, as the first comprehensive legal framework for personal data protection in Indonesia,[39] provides a more robust set of provisions, focusing solely on the data as the core object of protection. To date, PDP Law remains the main legal framework for data protection in Indonesia, while it's expected to be supported by an implementing regulation in the near future.

South Korea is also a country that has been grappling with the legal needs to regulate its digital environments, as the market for e-commerce in South Korea is one of the most advanced in the world. South Korea marked its legislative commitment to accommodate the development of digital technologies through the enactment of Act on Promotion of Information and Communications Network Utilization and Information Protection (Network Act) in 2001. Network Act has undergone many amendments, with the latest one in 2024. As Network Act continued to receive many amendments, in early 2020, South Korea ended up consolidating the provisions regarding data protection into Personal Information Protection Act (PIPA) which was enacted in 2011 and had also undergone many amendments.[40] This was done to make the legal norms regarding data protection in South Korea more streamlined and efficient. To date, South Korea still relies on PIPA as its main legal framework for data protection. PIPA, as mentioned before, has received many amendments, with the latest one in 2023.

From basic definitions, PIPA provides a much more comprehensive understanding of the nature of data and its implication to privacy. Article 1 of PIPA stipulates that: *"Personal information is any of the following information relating to a living individual: (a) Information that identifies a particular individual by his or her full name, resident registration number, pictures, etc.; (b) Information which, even*

[39] Luh Anastasia Trisna Dewi, Ni Putu Suci Meinarni, and I Dewa Gede Dana Sugama, "Analisis Ekonomi Terhadap Hukum Dalam Kegagalan Perlindungan Data Pribadi Pengguna E-Commerce," *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 3 (December 2021): 698–708, https://doi.org/10.29303/ius.v9i3.976.

[40] Changhee Lee, "National Informatization Policy in Korea: A Historical Reflection and Policy Implications," *Korean Journal of Policy Studies* 36, no. 1 (2021): 27–43, https://doi.org/10.52372/kjps36103.

if it by itself does not uniquely identify an individual, may be easily combined with other information to uniquely identify an individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured; (c) Information under items (a) or (b) above that is pseudonymized in accordance with subparagraph 1-2 below and thereby becomes incapable of uniquely identifying an individual without the use or combination of information for restoration to the original state (hereinafter referred to as "pseudonymized information"); 1-2. The term "pseudonymization" means a procedure to process personal information so that the information cannot uniquely identify an individual without additional information, by erasing in part, or replacing in whole or in part, such information."

On the other hand, the PDP Law only defines personal data as: *"Personal data is data on individual persons who are identified or can be identified individually or in combination with other information either directly or indirectly through electronic or non-electronic systems."*

The definition of personal information or personal data as the main object of data protection plays a crucial part in how the dynamics of data governance are going to be regulated. PIPA's definition constructs a normative framework that meticulously categorizes personal information to include data that does not immediately identify an individual but can do so when combined with other data or when de-pseudonymized. This level of comprehensiveness is only partly covered by the PDP Law's definition of personal data. This normative stance is critical in digital advertising, where disparate datasets are often integrated to profile consumers.[41] By explicitly regulating not just direct identifiers like names or photos but also the combinatory processes that can lead to identification, PIPA establishes a more protective norm for personal data.

Consequently, PIPA provides a more robust framework of provision regarding the identification of persons through data, which is crucial in digital advertising. Article 24 restricts the processing of

[41] Jaap Wieringa et al., "Data Analytics in a Privacy-Concerned World," *Journal of Business Research* 122 (January 2021): 915–25, https://doi.org/10.1016/j.jbusres.2019.05.005.

personally identifiable information unless certain conditions are met. It allows processing if the controller informs the data subject about specific matters and obtains their consent, or if other laws require or permit it. The controller must also implement safety measures, such as encryption, to protect the data. Regular inspections by the Protection Commission ensure compliance, and specialized institutions may conduct these inspections. Gravely, the PDP Law permits the data controller to profile data subjects using data that can be identifiable, with little to no layer of protection or justification. The only legal remedy for this problem is the provision of Article 10 paragraph (1) of the PDP Law, which governs that data subjects can file an objection against such act. Furthermore, paragraph (2) of Article 10 governs that the mechanism for the objection is to be regulated by a government regulation (as an implementing regulation). However, this has not yet seen the light of the Indonesian legal system, which essentially renders the provision entirely ineffective.

Furthermore, South Korea's PIPA framework incorporates specific articles that enhance the clarity and enforceability of its data protection provisions. For example, Article 23 of PIPA mandates explicit consent for the processing of sensitive information, including categories such as political opinions, health status, sex life, and ideology, among many others. This requirement is embedded directly within the primary legislation, providing clear and immediate guidelines on how sensitive data should be handled. Additionally, Article 24 specifies protective measures for juvenile information, emphasizing the need for stringent safeguards for data related to minors. Conversely, Indonesia's PDP Law outlines a broad framework that categorizes personal data into specific and general types under Article 4. While this classification acknowledges the need for differentiated handling of various data types, it falls short of specifying the procedural details within the law itself. Instead, it indicates that further regulations will elaborate on these details, potentially leading to a lag in the law's effective implementation and clarity.

Furthermore, South Korea's framework for privacy is also supported by PIPA's enforcement decree, which sets an even more comprehensive standard for data protection in the digital space. For example, Article 15-2 requires personal information controllers

handling large data volumes to follow strict notification rules. Controllers must notify data subjects within three months of collecting data if they handle sensitive information or personally identifiable information of at least 50,000 subjects, or any personal information of over one million subjects. Notifications can be made through various accessible methods like email, telephone, or text messages. Furthermore, these controllers are required to maintain records of when and how each notification was made until the information is officially destroyed, ensuring ongoing compliance with data protection regulations. In the context of digital advertising, this can help raise awareness among data subjects, which can substantially help them make purchasing decisions that are more reasonable, and not fully based on suggestions that essentially take advantage of their behavior.[42]

Another advantage that South Korea's framework for consumer privacy has over Indonesia is the fact that it provides the legal basis for a watchdog body that has the authority to oversee all the dynamics of data protection and privacy. Indonesia currently doesn't have a concrete legal basis for such comprehensive network of data protection. South Korea, through PIPA and PIPA's Enforcement Decree, provides a comprehensive set of provisions regarding the role of Personal Information Protection Commission (PIPC), who plays a crucial part in making sure that the privacy of South Koreans are protected under strict implementation of legal compliance. Article 7 establishes the Personal Information Protection Commission (Protection Commission), which is positioned under the Prime Minister to independently handle affairs related to personal information protection. This commission is designated as a central administrative agency per Article 2 of the Government Organization Act, with an exemption from Article 18 of the same act for certain matters. These exemptions specifically include business affairs outlined in subparagraphs 3 and 4 of Article 7-8, which concern the establishment of necessary measures to ensure the safety of personal

[42] Rina Arum Prastyanti and Ridhima Sharma, "Establishing Consumer Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India," *Journal of Human Rights, Culture and Legal System* 4, no. 2 (May 2024): 354–90, https://doi.org/10.53955/jhcls.v4i2.200.

information and to handle grievances and resolve disputes related to personal information breaches, and deliberations under Article 7-9 (1), which governs the processes for assessing factors that could lead to personal information breaches and the development of procedures to prevent these breaches.

Furthermore, Indonesia's consumer protection framework is largely archaic, as it was enacted in 1999 through Law No. 8 of 1999 on Consumer Protection (Consumer Protection Law), which has not received any amendments since. Unlike South Korea's direct consumer-privacy statutory language, Indonesia's Consumer Protection Law has remained as a framework that is too broad to specifically and clearly connect consumer protection dynamics with data protection and data privacy issues. The only relevant part of this framework is perhaps Article 4 letter c, which governs the right to information, a key principle that naturally extends to the digital context. Another potentially relevant, yet mostly vague provision is Article 4 letter a, regarding "the right to comfort, security, and safety in consuming goods and/or services". While this provision can potentially be tied to data privacy as the perception of privacy is inherently tied to safety, it is far to indirect to address a concern that has grown to become one of the biggest in modern legal scholarship around commerce.[43]

The analysis ultimately highlights why the reputation of PIPA as Asia's toughest regulatory framework for data protection and privacy[44] is indeed well-founded. As the case for Indonesia, it shows that the PDP Law lacks the acknowledgement of the technical aspects of data, which are important in the utilization of data for digital advertising purposes. It also shows that Indonesia is still heavily relying on the promise for a continued development of PDP legal framework through an

[43] This lack of direct acknowledgement regarding the issue of privacy in the digital space remains one of the biggest challenges in this overwhelmingly important and highly specific domain of legal scholarship. *See* Daniel J. Solove, "The Myth of the Privacy Paradox," *George Washington Law Review* 89, no. 1 (2021): 1–51, https://scholarship.law.gwu.edu/faculty_publications/1482/.

[44] Hannah K. Galvin and Paul R. DeMuro, "Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019," *Yearbook of Medical Informatics* 29, no. 1 (2020): 32–43, https://doi.org/10.1055/s-0040-1701987.

implementing regulation,[45] which has not yet been delivered. As Indonesia and South Korea edge closer to the transition to Society 5.0, it's important to note that legal developments are equally important for both countries. However, it can't be dismissed that the task for future legal developments in Indonesia is steeper, as the country's legal system has been identified to be behind in almost all aspects of privacy and data protection, particularly regarding the identification of persons using various kinds of data.

3. Future Legal Developments

As comprehensively highlighted by the normative analysis, it's clear that South Korea has a much more advanced legal framework to support the protection and privacy of personal data, which plays a crucial role in guaranteeing consumer's privacy. Less comprehensive data classification, along with the lack of provisions regarding their direct and unique legal implications, highlighted the problem of Indonesia's legal framework which to date, still relies on the undrafted implementing regulation. A deeper look on the basic norms also implied that the PDP Law does not adequately recognize the wider variety of data and how they can be used to identify individuals. It also fails in acknowledging the significant breach of privacy that can come from the identification of individuals from various kinds of data that, as highlighted before, are not properly classified and regulated.

Therefore, this paper provides a model of legal development specifically made for Indonesia, as it is important to continuously develop the necessary legal norms to facilitate growth within the digital environment, which instead of being just a part of the economy, can actually become the economy itself.[46] In essence, this model of legal development aims to fill the gaps within Indonesia's legal framework for data protection and privacy, to ensure that the utilization of digital technologies for advertising purposes don't breach the privacy rights of Indonesians. This model is made based on the identified gaps within the previous normative analysis, to accommodate to the specific needs

[45] Andreas Kris Sang Hanajati, "Siapkan Aturan Pelaksana UU PDP, Kominfo Libatkan Publik," Direktorat Jenderal Aplikasi Informatika - KOMINFO, February 2023.

[46] Swamy, "The Digital Economy: New Business Models and Key Features."

that Indonesia needs in order to enhance its data privacy norms in the face of growing extensive digital advertising practices that can potentially threaten the privacy rights of many users. The table below specifically positions the model as a strategic blueprint for legal reform, synthesizing the comparative strengths of the South Korean framework into actionable norms that directly address the specific vulnerabilities of Indonesian consumers.

Table 1: Model of privacy and data protection legal development for Indonesia.

Normative Aspects	Description
Pseudonymization to prevent unlawful identification.	Pseudonymization needs to be added into the PDP legal framework of Indonesia, to ensure that prevents unlawful identification.
More complex data classification, which includes socio-cultural and economic aspects of person.	Complex data classification can provide a pathway for better framework of legal compliance of many different types of data, which has its own unique characteristics and implications.
Criminalization of unlawful identification	Unlawful identification should be punishable by law, to ensure that the framework of digital advertising practices doesn't become predatory and take advantage of users' behavior.
Tracking notification	Tracking notification is crucial in providing clarity for users of electronic systems that the products/services that they're being offered to right now are based on their activities.

Source: Researchers' analysis

Pseudonymization is perhaps the most distinct advantage that South Korea's framework for data protection and privacy has over Indonesia's. This mechanism needs to be integrated into Indonesia's legal framework as a layer of protection against unlawful

identification, which significantly threatens the privacy of Indonesians in the digital environment. Consequently, Indonesia also needs to develop a more complex data classification, along with the provisions their direct and unique legal implications, much like South Korea's PIPA framework. Additionally, the effort to prevent unlawful identification needs to be supported by criminal provisions, to hold actors behind digital advertising responsible for the breach of privacy rights. Lastly, tracking notification can also be added into Indonesia's PDP framework to ensure that users of electronic systems, particularly as consumers, are aware that the advertisements that are provided to them are based on data that are collected from their activities. This can improve data and privacy awareness among consumers, improve transparency from electronic system providers, and help consumers make better purchasing decisions.

Indonesia can also benefit from the establishment of a watchdog body that can oversee the dynamics and enforcement of these norms, which can significantly improve regulatory delivery and inspection. This aspect of development is proposed separately due to its higher importance and broader implications for data protection and privacy in Indonesia. Much like South Korea's PIPC, Indonesian can better oversee the problems and detect violations of privacy and data protection compliance. Most importantly, it can also help determine the future of relevant legal developments as the problems and needs regarding privacy and data protection are directly overseen by a government body. Ultimately, these developments are necessary for Indonesia's legal system and the continuation of growth in different sectors that are increasingly affected by digital technologies.

C. Conclusion

Analyses have conclusively revealed the urgency for legal reforms in Indonesia in the face of growing, more privacy-invasive practices of digital advertising. The reliance on large-scale data collection, aggregation, and profiling, present significant privacy risks to the personal data of many users in e-commerce spaces. The significant disparity between Indonesia's and South Korea's legal frameworks governing data protection and privacy in digital advertising further heightens the urgency to tackle this legal problem.

South Korea's Personal Information Protection Act demonstrates a structurally robust and technologically responsive approach through its comprehensive data definition, explicit regulation of pseudonymized data, and the existence of an independent supervisory authority, among many other legal safeguards. In contrast, Indonesia's consumer protection regime largely irrelevant due to its broad nature, while the country's Personal Data Protection Law is inadequate due to vague data classification, limited restrictions on profiling activities, reliance on yet-to-be-enacted implementing regulations, and the absence of an empowered oversight body.

Based on the identified normative gaps, this research finds that future legal development in Indonesia must move beyond incremental reform and adopt a more systemic and anticipatory regulatory model. The proposed framework emphasizes the integration of pseudonymization, expanded data classification, criminal liability for unlawful identification, mandatory tracking notification, and the establishment of an independent supervisory authority, which are all essential not only to strengthen consumer privacy protection but also to ensure legal certainty and ethical integrity in the digital advertising market. Future research can focus more on the specific empirical evidence regarding enforcement failures and the prevaling patterns of privacy-invasive practices in digital advertising, to further support the proposed model or challenge it, expanding the necessary legal scholarship for future legal developments.

References

Afriat, Hagar, Shira Dvir-Gvirsman, Keren Tsuriel, and Lidor Ivan. "'This Is Capitalism. It Is Not Illegal': Users' Attitudes toward Institutional Privacy Following the Cambridge Analytica Scandal." *Information Society* 37, no. 2 (2020): 115–27. https://doi.org/10.1080/01972243.2020.1870596.

Aiolfi, Simone, Silvia Bellini, and Davide Pellegrini. "Data-Driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising." *International Journal of Retail & Distribution Management* 49, no. 7 (January 2021): 1089–1110. https://doi.org/10.1108/IJRDM-10-2020-0410.

Alshammari, Majid Khalaf, Mohamad Hashim Othman, Yasmin Othman Mydin, and Badiea Abdulkarem Mohammed. "Social and

Psychological Problems and Their Relationship with Several Variables among University Students." *Review of Economics and Finance* 21 (2023): 426–29. https://doi.org/10.55365/1923.x2023.21.44.

Bandara, Ruwan, Mario Fernando, and Shahriar Akter. "Explicating the Privacy Paradox: A Qualitative Inquiry of Online Shopping Consumers." *Journal of Retailing and Consumer Services* 52 (2020): 1–9. https://doi.org/10.1016/j.jretconser.2019.101947.

Bua, Imanuel Toding, and Nur Isdah Idris. "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024." *Desentralisasi: Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 2 (May 23, 2025): 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653.

Channak, Zaki Mahmed, Abdulkader Alkhateeb, Elham Saleh, Hanadi Aldeeb, and Sayed Alsharif. "Business Ethics in E-Commerce – Legal Challenges and Opportunities." *Access to Justice in Eastern Europe* 6, no. Special Issue (2023): 1–16. https://doi.org/10.33327/AJEE-18-6S007.

Chatterjee, Sheshadri, and N. S. Sreenivasulu. "Personal Data Sharing and Legal Issues of Human Rights in the Era of Artificial Intelligence: Moderating Effect of Government Regulation." *International Journal of Electronic Government Research* 15, no. 3 (2019): 21–36. https://doi.org/10.4018/IJEGR.2019070102.

Cooper, Dylan A, Taylan Yalcin, Cristina Nistor, Matthew Macrini, and Ekin Pehlivan. "Privacy Considerations for Online Advertising: A Stakeholder's Perspective to Programmatic Advertising." *Journal of Consumer Marketing* 40, no. 2 (January 2023): 235–47. https://doi.org/10.1108/JCM-04-2021-4577.

Dahlen, Micael, and Sara Rosengren. "If Advertising Won't Die, What Will It Be? Toward a Working Definition of Advertising." *Journal of Advertising* 45, no. 3 (2016): 334–45. https://doi.org/10.1080/00913367.2016.1172387.

David Nguyeni, and Marta Paczosi. "Measuring the Economic Value of Data and Cross-Border Data Flows : A Business Perspective." *OECD Digital Economy Papers*, no. 297 (2020): 1–47. https://doi.org/10.1787/20716826.

Del-Real, Cristina, Els De Busser, and Bibi van den Berg. "A Systematic Literature Review of Security and Privacy by Design Principles, Norms, and Strategies for Digital Technologies." *International Review of Law, Computers & Technology* 39, no. 3 (September 2,

2025): 374–405. https://doi.org/10.1080/13600869.2025.2457227.

Disemadi, Hari Sutra. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289–304. https://doi.org/10.37253/jjr.v24i2.7280.

Dwivedi, Yogesh K, Elvira Ismagilova, D Laurie Hughes, Jamie Carlson, Raffaele Filieri, Jenna Jacobson, Varsha Jain, et al. "Setting the Future of Digital and Social Media Marketing Research: Perspectives and Research Propositions." *International Journal of Information Management* 59 (2021): 1–37. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2020.102168.

Enang, Etieno, Mahdi Bashiri, and David Jarvis. "Exploring the Transition from Techno Centric Industry 4.0 towards Value Centric Industry 5.0: A Systematic Literature Review." *International Journal of Production Research* 61, no. 22 (2023): 7866–7902. https://doi.org/10.1080/00207543.2023.2221344.

Estrada-Jiménez, José, Javier Parra-Arnau, Ana Rodríguez-Hoyos, and Jordi Forné. "Online Advertising: Analysis of Privacy Threats and Protection Approaches." *Computer Communications* 100 (2017): 32–51. https://doi.org/10.1016/j.comcom.2016.12.016.

Fadhli, Zawil, Sri Walny Rahayu, and Iskandar A. Gani. "Perlindungan Data Pribadi Konsumen Pada Transaksi Paylater." *Jurnal Hukum Magnum Opus* 5, no. 2 (2022): 119–32.

Fadliansyah, Fariz, Muhammad Khusni Mubarok, Muhammad Dafa Aziz, and Annisa Elfina Augustia. "Evaluasi Pembelajaran Dari Kasus Kebocoran Data Di Indonesia Sebagai Negara Dengan Data Breach Terbesar Ke-8 Dunia." *TEKNOBIS: Jurnal Teknologi, Bisnis Dan Pendidikan* 3, no. 2 (October 19, 2025): 272–77. https://jurnalmahasiswa.com/index.php/teknobis/article/view/3025.

Galvin, Hannah K., and Paul R. DeMuro. "Developments in Privacy and Data Ownership in Mobile Health Technologies, 2016-2019." *Yearbook of Medical Informatics* 29, no. 1 (2020): 32–43. https://doi.org/10.1055/s-0040-1701987.

Hamilton, James F. "A New Take on Digital Advertising: Theory, History, and Society." *Advertising & Society Quarterly* 18, no. 1 (2017): 1–41. https://doi.org/10.1353/asr.2017.0006.

Hanajati, Andreas Kris Sang. "Siapkan Aturan Pelaksana UU PDP, Kominfo Libatkan Publik." Direktorat Jenderal Aplikasi

Informatika - KOMINFO, February 2023.

Jiang, Yinhao, Mir A Rezazadeh Baee, Leonie R Simpson, Praveen Gauravaram, Josef Pieprzyk, Tanveer Zia, Zhen Zhao, and Zung Le. "Pervasive User Data Collection from Cyberspace: Privacy Concerns and Countermeasures." *Cryptography*, 2024. https://doi.org/10.3390/cryptography8010005.

Kalsi, Monique. "Still Losing the Race with Technology? Understanding the Scope of Data Controllers' Responsibility to Implement Data Protection by Design and by Default." *International Review of Law, Computers & Technology*, 2024, 1–23. https://doi.org/10.1080/13600869.2024.2324546.

Khan, Mohammad Aslam. "Mega Risks: Digital Transformation and Sustainability." In *Cities and Mega Risks: COVID-19 and Climate Change*, edited by Mohammad Aslam Khan, 81–111. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-14088-4_4.

Kim, Tonghoon, and David J. Atkin. "How Government Surveillance Policies Modify SNS Use in South Korea." *Journal of Information Policy* 9 (December 1, 2019): 214–37. https://doi.org/10.5325/jinfopoli.9.2019.0214.

Lee, Changhee. "National Informatization Policy in Korea: A Historical Reflection and Policy Implications." *Korean Journal of Policy Studies* 36, no. 1 (2021): 27–43. https://doi.org/10.52372/kjps36103.

Martin, Kelly D., and Patrick E. Murphy. "The Role of Data Privacy in Marketing." *Journal of the Academy of Marketing Science* 45, no. 2 (2017): 135–55. https://doi.org/10.1007/s11747-016-0495-4.

Nixon, John. "Digitalization Deployed: Lessons Learned from Early Adopters." In *Proceedings of the Annual Offshore Technology Conference*, 2020-May:1–7, 2020. https://doi.org/10.4043/30794-ms.

Nolin, Jan Michael. "Data as Oil, Infrastructure or Asset? Three Metaphors of Data as Economic Value." *Journal of Information, Communication and Ethics in Society* 18, no. 1 (2020): 54–69. https://doi.org/10.1108/JICES-04-2019-0044.

Ozeran, Larry, Anthony Solomonides, and Richard Schreiber. "Privacy versus Convenience: A Historical Perspective, Analysis of Risks, and an Informatics Call to Action." *Applied Clinical Informatics* 12, no. 2 (2021): 274–84. https://doi.org/10.1055/s-0041-1727197.

Prastyanti, Rina Arum, and Ridhima Sharma. "Establishing Consumer

Trust Through Data Protection Law as a Competitive Advantage in Indonesia and India." *Journal of Human Rights, Culture and Legal System* 4, no. 2 (May 2024): 354–90. https://doi.org/10.53955/jhcls.v4i2.200.

Quelle, Claudia. "Not Just User Control in the General Data Protection Regulation." In *Privacy and Identity Management. Facing up to Next Steps*, edited by Anja Lehmann, Diane Whitehouse, Simone Fischer-Hübner, Lothar Fritsch, and Charles Raab, 140–63. Cham: Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-55783-0_11.

Reshetnikova, Marina, Irina Pugacheva, and Alina Evseevicheva. "China or South Korea: A Comparative Analysis of Innovative Development." In *E3S Web of Conferences*, 295:1–9, 2021. https://doi.org/10.1051/e3sconf/202129501060.

Rizki, Muhamad, and Surgana Surgana. "Data Breach of General Elections Commission: Causes and Prevention Efforts." *Jurnal Sistem Informasi Dan Teknologi Informasi* 2, no. 1 (January 1, 2025): 157–60. https://doi.org/10.33197/justinfo.v2i1.1793.

Rosiyana, Reza Nur, Melyana Agustin, Ivan Kalka Iskandar, and Senny Luckyardi. "A New Digital Marketing Area for E-Commerce Business." *International Journal of Research and Applied Technology (INJURATECH)* 1, no. 2 (December 2021): 370–81. https://doi.org/10.34010/injuratech.v1i2.6765.

Satwiko, Brahmantyo Suryo. "Privacy and Data Protection: Indonesian Legal Framework." *Corporate and Trade Law Review* 1, no. 2 (2021): 98–118. https://doi.org/10.21632/ctlr.1.2.98-118.

Sexton, Anna, Elizabeth Shepherd, Oliver Duke-Williams, and Alexandra Eveleigh. "The Role and Nature of Consent in Government Administrative Data." *Big Data and Society* 5, no. 2 (2018): 1–17. https://doi.org/10.1177/2053951718819560.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (January 3, 2024): 1–20. https://doi.org/10.20956/halrev.v10i1.5016.

Sinclair, John. "Magazines and Advertising in the Digital Age." In *The Handbook of Magazine Studies*, 105–19, 2020. https://doi.org/10.1002/9781119168102.ch8.

Solove, Daniel J. "The Myth of the Privacy Paradox." *George Washington Law Review* 89, no. 1 (2021): 1–51.

https://scholarship.law.gwu.edu/faculty_publications/1482/.

Swamy, L Narayana. "The Digital Economy: New Business Models and Key Features." *International Journal of Research in Engineering, Science and Management* 3, no. 7 (July 2020): 118–22.

Tan, David. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463–78. https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601.

Terkan, Remziye. "Importance of Creative Advertising and Marketing According to University Students' Perspective." *International Review of Management and Marketing* 4, no. 3 (2014): 239–46.

Trisna Dewi, Luh Anastasia, Ni Putu Suci Meinarni, and I Dewa Gede Dana Sugama. "Analisis Ekonomi Terhadap Hukum Dalam Kegagalan Perlindungan Data Pribadi Pengguna E-Commerce." *Jurnal IUS Kajian Hukum Dan Keadilan* 9, no. 3 (December 2021): 698–708. https://doi.org/10.29303/ius.v9i3.976.

Wartoyo, Franciscus Xaverius, and Yuni Priskila Ginting. "Convergence of Law and Technology Through Optimization of Pancasila." *Journal of Digital Law and Policy* 1, no. 2 (2022): 61–72. https://doi.org/10.58982/jdlp.v1i2.139.

Wieringa, Jaap, P.K. Kannan, Xiao Ma, Thomas Reutterer, Hans Risselada, and Bernd Skiera. "Data Analytics in a Privacy-Concerned World." *Journal of Business Research* 122 (January 2021): 915–25. https://doi.org/10.1016/j.jbusres.2019.05.005.

*lembar ini sengaja dikosongkan