Pak. j. life soc. Sci. (2024), 22(2): 18490-18500 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.001354

RESEARCH ARTICLE

The Evolution of Data Privacy Laws: Balancing Technological Innovation and Human Rights in the Age of Big Data

Dwi Nur Fauziah Ahmad[1]*, Putri Amalia Zubaedah[2], Royyan Hafizi[3], Farhan Chaerul Umam[4], Loso Judijanto[5]

[1]Universitas Muhammadiyah Tangerang, Indonesia
[2]IAIN Syekh Nurjati Cirebon, Indonesia
[3]Universitas Swadaya Gunung Jati, Indonesia
[4]Institut Agama Islam Cirebon, Indonesia
[5]IPOSS Jakarta, Indonesia

ARTICLE INFO

Received: Oct 24, 2024
Accepted: Dec 7, 2024

Keywords

Personal Data Protection,
GDPR,
CCPA,
Technology and Privacy,
Regulatory Ethics

***Corresponding Author:**

dwihijaj18@gmail.com

ABSTRACT

The rapid development of technology, especially in the context of big data and artificial intelligence (AI), has challenged the legal system to create effective personal data protection regulations without hindering innovation. This article analyzes the evolution of personal data protection laws and how the law can strike a balance between individual privacy protection and technological advancements. Through a comparative study of various regulations at the global level, such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDP) in Indonesia, this study identifies the strengths and weaknesses of each legal framework. The GDPR is a reference in terms of creating a balance, but its implementation poses challenges for small and medium-sized businesses, while a sectoral approach in the US results in an imbalance in data protection. On the other hand, Indonesia as a country with newer regulations faces challenges in implementation and supervision, although the PDP shows significant progress. The study also highlights the importance of incorporating ethical principles in personal data regulation, such as fairness, accountability, and transparency, to meet the challenges posed by evolving technologies. In conclusion, international cooperation is needed to harmonize personal data protection policies to ensure individual privacy rights while supporting sustainable innovation in this digital era.

INTRODUCTION

Rapid technological developments, especially in the context of big data, have profoundly changed the way personal data is collected, stored, and utilized. Big data, which refers to enormous and complex data sets that are difficult to manage with traditional methods, has created new opportunities in various sectors, from healthcare, finance, social media, to marketing. In the health sector, for example, the use of big data allows for more personalized health analysis, such as in the development of treatments tailored to individual genetic profiles (Adams, 2017). In the financial sector, big data is used to improve risk analysis and identify fraud patterns that are invisible with traditional data (Renuka et al., 2025). Likewise in the social media and marketing industry, large companies are using big data to make more accurate predictions about consumer behavior and design more effective marketing strategies (Richard & Schlick, 2024).

However, despite the great benefits resulting from the use of these technologies, there are growing concerns regarding the protection of individual privacy rights. The personal data collected by various digital platforms often includes sensitive information that is at risk of being misused. The phenomenon of data breaches, which occurred in large companies such as Facebook and Equifax, became the focus in this discussion (Rouvroy, 2008). In addition, with the increasing sophistication of technologies such as artificial intelligence and predictive analytics, the potential for manipulating personal data or conducting massive surveillance is increasing. This leads to an urgent need to protect individual privacy in an increasingly complex digital landscape.

The main challenge in dealing with these changes is the creation of a legal framework that is able to balance technological innovation and the protection of human rights, especially the right to privacy. Technology is evolving much faster than existing laws, creating a gap that allows for the misuse of personal data (Song & Ma, 2022). For example, although regulations such as the General Data Protection Regulation (GDPR) enacted in the European Union have been a major step in protecting personal data, there are still many countries that do not have adequate similar laws in place or that fail to enforce existing laws effectively. Even in countries that already have regulations, weak implementation and oversight often allow large companies to ignore user data protection.

In addition, new technologies such as artificial intelligence (AI) and machine learning add complexity in enforcing personal data laws. AI systems that can collect and analyze large amounts of data to make automated decisions are often not transparent, leading to problems related to accountability and oversight (Aiello, 2024; Sembiring et al., 2024). At the same time, the use of personal data for legitimate purposes in improving services or operational efficiency often clashes with concerns regarding excessive oversight and violations of individual privacy.

As the debate over data privacy grows, many are calling for a more integrated approach between technological innovation and the protection of individual rights. However, responding to these issues requires a more holistic and systematic approach, which involves not only legislation but also changes in the ethical level, transparency, and community involvement in the technological decision-making process (Debbarma, 2023; Tene & Polonetsky, 2012). In this case, it is important to think about how to create a balance between technological advancement and human rights in the digital space.

A number of countries, such as the European Union, have taken steps to introduce stricter regulations on the protection of personal data through the GDPR. This regulation not only focuses on individual privacy but also establishes obligations for companies to maintain transparency in data collection as well as give individuals access and control rights over their data (European Commission, 2016). Although the GDPR is a reference for many countries, there are still challenges in adapting and implementing similar regulations in other countries with different cultures and legal structures.

On the other hand, in the United States, although there are some regulations regarding personal data, there is no comprehensive law like GDPR. Instead, the country relies on more specific laws, such as the California Consumer Privacy Act (CCPA) that gives consumers the right to know and control the personal data collected by companies. However, this state-based approach creates inconsistencies in data protection, which can be confusing for users as well as companies operating in many regions (Ehimuan et al., 2024).

Indonesia, as the country with the largest population in Southeast Asia, faces major challenges related to data privacy in the era of big data. Along with the rapid development of technology, especially in the field of digitalization and artificial intelligence, many sectors in Indonesia, such as e-commerce, social media, banking, and the health sector, are beginning to utilize big data to improve efficiency and provide services that are more tailored to individual needs (Hidayat et al., 2024; Sollisa, 2024). However, it also has a significant impact related to data privacy protection and human rights. This phenomenon creates a tension between the need to encourage technological innovation and the obligation to protect the personal data of Indonesians who are increasingly connected to the digital world.

One of the major phenomena that stands out is the increase in the use of digital platforms by the Indonesian people. Based on data from **Statista** in 2022, Indonesia has more than 190 million internet

users and nearly 170 million social media users, a number that continues to increase every year. This presents a huge opportunity for the business and technology sectors to leverage user data to improve services and design more effective marketing strategies (D. R. Saputra et al., 2024). However, on the other hand, the high penetration rate of the internet and social media opens up a huge gap for privacy violations. For example, a number of large data leaks have occurred, such as the Tokopedia user data leak in 2020 and Shopee in 2021. This data leak sparked concerns about the extent to which users' personal data is protected by technology companies in Indonesia.

In this context, the big issue that arises is how to create an adaptive legal framework, which can accommodate technological changes while maintaining the basic principles of privacy and human rights. Current regulations are often too static and unable to keep pace with the pace and scale of technological developments, especially when it comes to the use of big data and increasingly advanced artificial intelligence.

Therefore, it is important to further explore the evolution of data privacy law and how existing regulations can better respond to the need for human rights protection without hindering the potential for technological innovation. This research aims to examine changes and developments in personal data protection law, as well as assess how the balance between the protection of technological innovation and human rights can be achieved in the era of big data. In addition, this research will also analyze the challenges faced in creating a legal framework that is responsive to evolving technology (Lawalata et al., 2024).

With a focus on the global context and comparisons between legal approaches in different countries, this study aims to provide policy recommendations that can help create a more effective legal framework, which not only supports technological innovation but also protects the rights of individuals in this increasingly complex digital world.

LITERATURE REVIEW

A. Privacy as a Human Right

Privacy, as a fundamental human right, has evolved over centuries to meet the demands of new societal and technological challenges. The right to privacy is embedded in various international human rights instruments. One of the most prominent is the Universal Declaration of Human Rights (UDHR), which, in Article 12, asserts that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence" (United Nations, 1948). This idea of privacy, often referred to as informational privacy, has expanded with technological advancements, particularly in the digital era, where personal data has become a commodity. The emergence of the Internet and the digitization of personal data have fundamentally reshaped our understanding of privacy. In the context of the digital age, informational privacy refers to the control individuals have over their personal information, how it is collected, stored, and used (Yanamala et al., 2024)

The concept of privacy in international law has also evolved. The International Covenant on Civil and Political Rights (ICCPR), adopted by the United Nations in 1966, guarantees the right to privacy in Article 17. However, the rapid technological changes and the pervasive use of personal data in modern society challenge the application of these rights. Scholars like (Ambedkar, n.d.) argue that the traditional legal frameworks for privacy are inadequate in addressing the complexities of digital privacy. This has led to calls for a more comprehensive and dynamic approach to data privacy, integrating both legal protections and individual autonomy over personal information.

Moreover, recent developments in global data protection laws, like the European General Data Protection Regulation (GDPR), have become key reference points in balancing privacy with technological innovation. The GDPR's emphasis on individual control over personal data represents a significant shift toward recognizing privacy as an individual’s right, further framing privacy within the context of human rights in the digital age (Nadir & Farah, 2023).

B. Balancing Innovation and Regulation

The challenge of balancing technological innovation with privacy protection has long been discussed in regulatory theory. Risk regulation theory provides a framework for managing the uncertainties and potential harms that new technologies, such as big data and artificial intelligence, introduce to privacy. This theory suggests that regulations should be based on the assessment of risks posed by new technologies, which can often be uncertain and difficult to predict. According to (Vargiolu, 2022), risk regulation should balance the need for technological innovation with the imperative to protect fundamental rights. This includes ensuring that technologies are developed and deployed in ways that respect individual privacy and human dignity.

One of the key principles in the theory of regulatory balance is technology neutrality, which argues that regulations should not favor one technology over others but instead focus on the societal impacts of those technologies. This principle has been central to debates surrounding data protection laws, where regulators must find ways to protect individuals' rights without stifling innovation. For instance, the GDPR takes a technology-neutral approach, regulating the processing of personal data without limiting specific technologies. It ensures that the laws remain applicable across a wide range of technological developments, fostering both innovation and privacy protection (Ali, 2024).

The role of law in balancing innovation and privacy is especially critical in an era where data has become a driving force behind economic growth. Innovations like artificial intelligence and machine learning rely heavily on vast amounts of data, which often include personal information. As a result, the law must navigate the complexities of these innovations, ensuring that they do not infringe upon fundamental rights. The tension between innovation and regulation is particularly evident in sectors such as healthcare, finance, and social media, where personal data is often at the core of services and products. By developing legal frameworks that are flexible and adaptable to new technological realities, regulators can strike a balance that promotes innovation while safeguarding individual privacy (Singla, 2024)

C. The Role of Ethics in Data Privacy

As technological advancements continue to shape the ways in which personal data is collected, processed, and shared, ethical considerations play a critical role in assessing their impact on human rights. Ethics provide a foundation for the development of legal and regulatory frameworks, guiding decision-makers in considering not only what is legal but also what is morally acceptable. One of the primary ethical concerns in data privacy is the concept of informed consent. Individuals should be fully aware of how their data will be used and should have the autonomy to grant or withhold consent based on their understanding of these uses. The ethical principle of autonomy emphasizes the right of individuals to control their personal data, ensuring that their participation in data collection or processing is voluntary and based on clear, unambiguous consent (Singh, 2024).

Ethical frameworks such as utilitarianism and deontology have been applied to the data privacy debate. From a utilitarian perspective, the benefits of data-driven innovation, such as improved healthcare, better public services, and enhanced economic opportunities, may justify the collection and use of personal data. However, from a deontological standpoint, the moral right to privacy could outweigh the potential benefits of data use. This tension between the benefits of technological innovation and the ethical obligation to protect individual rights presents a significant challenge for lawmakers and regulators (Sharma et al., n.d.).

The intersection of ethics and law in data privacy can be seen in the regulatory practices of various jurisdictions. In the European Union, the GDPR incorporates ethical principles, such as transparency, fairness, and accountability, into its legal framework, emphasizing that data collection and processing must be done in a way that respects individual privacy rights. Similarly, the recent developments in ethical AI frameworks have stressed the importance of ensuring that technologies such as machine learning algorithms operate within ethical boundaries that respect human dignity and privacy (Saxena, 2020).

Overall, ethics plays an essential role in shaping the legal and regulatory frameworks that govern data

privacy, ensuring that the protection of individual rights is prioritized even as technological advancements continue to evolve. The continuous dialogue between law and ethics is necessary to safeguard the rights of individuals in the digital age, ensuring that technology serves humanity rather than exploiting it.

METHODOLOGY

This study adopts a comparative legal analysis methodology to examine the evolution of data privacy laws across different jurisdictions (Moleong, 2000). By comparing the data privacy frameworks in key regions—such as the European Union, the United States, and Southeast Asia—this research seeks to identify best practices, regulatory gaps, and the strengths and weaknesses of various legal systems in protecting individuals' privacy rights in the face of technological advancements. In particular, the analysis will focus on major legislation like the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in countries like Indonesia, exploring their legal scope, enforcement mechanisms, and the impact they have had on data protection.

Additionally, case studies of technological innovations will be utilized to demonstrate the real-world impact of evolving data privacy laws (Taylor et al., 2015). These case studies will examine how innovations in social media platforms, healthcare data usage, and AI-driven data collection have influenced legal approaches to privacy protection. Social media platforms, for example, have been at the center of privacy debates, where the data generated by users often conflicts with traditional privacy rights. Similarly, AI and machine learning technologies raise new questions about data ownership, consent, and transparency, which will be explored to understand the challenges faced by existing laws in adapting to rapid technological progress (Bryman, 2016).

To build a comprehensive understanding of the state of data privacy, this study will employ a combination of secondary data and primary data collection methods. The primary data will consist of a thorough review of academic articles, legal texts, and policy papers that provide a historical and contemporary view of data privacy laws (Patton, 2002). These sources will include landmark case law, legal commentaries, and scholarly publications that offer insights into the regulatory environment of data privacy.

In addition, case law will be examined to understand how courts have interpreted and applied data privacy laws in different jurisdictions, focusing on cases that highlight emerging issues such as data breaches, unauthorized data sharing, and user consent (Creswell & Creswell, 2017). The legal texts to be reviewed will include international treaties, national laws, and guidelines issued by regulatory bodies like the European Data Protection Supervisor (EDPS) or the Federal Trade Commission (FTC).

Interviews with legal experts, policymakers, and technology professionals will be conducted to gather insights into the practical challenges of implementing data privacy laws and their evolving interpretations (Sugiyono, 2013). These interviews will aim to capture the perspectives of those who are directly involved in shaping or enforcing data protection policies. Legal experts will provide insight into the effectiveness of current legal frameworks, while policymakers will offer a broader perspective on the challenges of balancing innovation with privacy protection. Technology professionals, especially those involved in AI and big data, will discuss the ethical and technical challenges of complying with data protection regulations.

The data collected will undergo a qualitative analysis to track the evolution of data privacy laws over time. This analysis will involve examining the legal texts, case law, and academic literature to identify key milestones in the development of data privacy regulations (Boell & Cecez-Kecmanovic, 2015). The study will focus on how these laws have responded to emerging technological trends and how they have adapted to protect individual privacy in the digital age (Lundström & Lundström, 2021).

A comparative analysis will be conducted to assess the effectiveness of different legal frameworks in achieving data privacy goals. This analysis will evaluate how various jurisdictions balance the need for innovation with the protection of privacy rights. Key factors such as the scope of the law, enforcement

mechanisms, penalties for non-compliance, and public awareness will be examined. The comparative study will identify areas where certain jurisdictions have been more successful than others in protecting privacy while encouraging technological advancement.

Furthermore, the research will highlight the challenges and gaps in current regulatory approaches. Issues such as cross-border data flow, technological neutral frameworks, and the lack of enforcement in certain regions will be analyzed. The identification of regulatory gaps will provide insights into areas where future legal reforms are necessary to bridge the divide between technological progress and the protection of human rights. Finally, the study will propose policy recommendations for improving data privacy regulations considering these findings.

RESULTS

Data Privacy in Indonesia in the Context of Big Data and Technological Innovation

Indonesia, as the country with the largest population in Southeast Asia, faces major challenges related to data privacy in the era of big data. Along with the rapid development of technology, especially in the field of digitalization and artificial intelligence, many sectors in Indonesia, such as e-commerce, social media, banking, and the health sector, are beginning to utilize big data to improve efficiency and provide services that are more tailored to individual needs. However, it also has a significant impact related to data privacy protection and human rights. This phenomenon creates a tension between the need to encourage technological innovation and the obligation to protect the personal data of Indonesians who are increasingly connected to the digital world.

One of the major phenomena that stands out is the increase in the use of digital platforms by the Indonesian people. Based on data from Statista in 2022, Indonesia has more than 190 million internet users and nearly 170 million social media users, a number that continues to increase every year. This presents a huge opportunity for the business and technology sectors to leverage user data to improve services and design more effective marketing strategies. However, on the other hand, the high penetration rate of the internet and social media opens up a huge gap for privacy violations. For example, a number of large data leaks have occurred, such as the Tokopedia user data leak in 2020 and Shopee in 2021. This data leak sparked concerns about the extent to which users' personal data is protected by technology companies in Indonesia.

a. Data Protection Regulations in Indonesia

One of the important efforts made by the Indonesian government to address data privacy issues is to propose the Personal Data Protection Law (PDP Law) which was passed in October 2022. The law aims to provide greater protection for the personal data of Indonesian citizens and place stricter obligations on companies that collect and manage personal data. The PDP Law regulates the rights of individuals to access, correct, and delete their personal data and establishes legal sanctions for companies that violate existing provisions. In addition, this law also regulates the principles of transparency, accountability, and fairness in the collection of personal data, which is expected to increase public trust in the management of personal data.

However, although the PDP Law provides a stronger legal basis for protecting personal data, major challenges still exist in its implementation. Many are concerned about the effectiveness of surveillance of large companies, especially those based abroad, that collect and process data on Indonesian citizens. In addition, supervision of local companies is often limited by limited oversight infrastructure and lack of adequate resources to enforce the law effectively. For example, although the PDP Law regulates sanctions for violators, there is still no clear mechanism regarding the application of these sanctions, especially for large technology companies operating across borders.

b. Limitations of Infrastructure and Community Education

In addition to regulatory challenges, Indonesia also faces infrastructure problems in terms of personal data protection. Weak law enforcement and lack of technical infrastructure to protect personal data are major obstacles. Although many technology companies in Indonesia have implemented data protection

policies that are in line with international standards, such as the General Data Protection Regulation (GDPR), many small and medium-sized companies have not fully understood the importance of data protection or do not have the capacity to meet adequate personal data protection requirements.

In addition, the awareness of the Indonesian people about the importance of personal data protection is also still low. A survey conducted by CIGI-Ipsos in 2020 showed that most internet users in Indonesia do not know how to protect their personal data effectively. This is exacerbated by a lack of understanding of the risks arising from personal data leaks, such as identity theft, fraud, or even manipulation of personal information.

c. Use of Data by the Government

Another phenomenon that deserves attention is how the Indonesian government uses the personal data of its citizens in the management and implementation of public services. One of the major initiatives is the use of population data through the Electronic Identity Card (e-KTP) which functions as official identification. The data collected in this e-KTP can be used for various purposes, including social assistance programs, COVID-19 vaccination registration, and even general elections. While the use of this data can make it easier for citizens to access various public services, there are also concerns about the potential for data misuse by irresponsible parties.

For example, in the implementation of COVID-19 vaccinations, highly sensitive personal data such as health status and user location are collected by applications used for vaccination registration. This raises questions about the extent to which the data can be kept confidential and who has access to it, especially amid concerns over the potential use of the data for purposes other than its intended purpose.

The phenomenon that occurred in Indonesia shows that there is a tension between the rapid development of technology, especially in the use of big data, and efforts to protect citizens' privacy rights. Although Indonesia has passed the PDP Law to improve personal data protection, challenges in terms of regulatory implementation, weak supervision, and low public awareness remain major obstacles in creating an effective personal data protection system. Therefore, it is very important for Indonesia to continue to strengthen its data protection infrastructure, increase public education on the importance of maintaining privacy, and improve law enforcement mechanisms to face the challenges that arise in this digital era.

Evolution of Data Privacy Laws

The development of data privacy laws has been a response to the increasing complexity of data usage in society. One of the earliest milestones was the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), which established foundational principles for data protection, including purpose limitation and accountability. The European Union's Data Protection Directive (1995) marked another significant step, introducing binding data protection laws for member states. This was later superseded by the General Data Protection Regulation (GDPR) in 2018, which set a global benchmark for comprehensive data protection laws. GDPR introduced critical concepts such as data portability, the right to be forgotten, and stringent penalties for non-compliance, with fines reaching up to 4% of a company's global turnover (European Commission, 2016).

In contrast, the California Consumer Privacy Act (CCPA), enacted in 2020, provides a more limited framework. While it grants rights to know, delete, and opt-out of the sale of personal data, it lacks the breadth of GDPR in areas such as cross-border data flow and automatic data processing (Solove & Schwartz, 2021). Despite these advances, many countries, particularly in the Global South, still struggle with limited or outdated privacy laws, leaving significant gaps in global data governance.

Technological Innovation and Its Impact

Technological advancements, particularly in big data and AI, have exponentially increased the volume and complexity of data privacy challenges. Big data analytics allow organizations to infer sensitive information from seemingly benign datasets, raising concerns about profiling and discrimination. For example, the Cambridge Analytica scandal highlighted how Facebook data was exploited to influence

elections through targeted advertising (Rayhan & Rayhan, 2023). Similarly, AI-driven surveillance systems in China have sparked global debates about the ethical implications of facial recognition technology (Sumartono, 2024).

The pace of technological innovation often outstrips legal responses. For instance, the rise of generative AI and predictive analytics has blurred the boundaries of consent and data ownership, exposing significant gaps in current legal frameworks. These technologies pose a challenge to laws like GDPR, which struggle to regulate automated decision-making systems and the ethical use of AI models trained on personal data.

Balancing Innovation with Human Rights

Balancing innovation with human rights remains a persistent challenge. The GDPR represents one of the most robust attempts to reconcile these priorities. By adopting a technology-neutral approach, it ensures that legal protections remain applicable across various innovations. For example, GDPR's principles of data minimization and transparency aim to mitigate privacy risks while still allowing innovation to flourish (Fitrianingsih et al., 2024).

However, weaknesses remain. GDPR's stringent requirements have been criticized for imposing significant compliance costs on small and medium enterprises (SMEs), potentially stifling innovation. Moreover, its enforcement has been uneven, with tech giants often able to absorb fines without changing their practices significantly. By contrast, jurisdictions like the United States have opted for a sectoral approach, where privacy protections vary by industry. While this approach may offer flexibility, it often leads to gaps in protection and inconsistencies in enforcement (Habibah, 2024).

DISCUSSION AND ANALYSIS

The findings highlight the critical importance of aligning legal frameworks with technological realities. A hybrid approach combining the comprehensive protections of GDPR with the flexibility of sectoral regulations like those in the U.S. may offer a balanced solution. Additionally, international cooperation is vital to address cross-border data flows and harmonize standards. Policymakers must also ensure that data privacy laws are inclusive, affordable to implement, and adaptable to emerging technologies (Hakim, 2024). Furthermore, as technological advancements like AI and big data continue to evolve, there is a pressing need for proactive legal frameworks that incorporate ethical principles, such as fairness and accountability, into the design and use of these technologies. Strengthening public awareness and investing in enforcement mechanisms will also be essential for ensuring the efficacy of data privacy laws in protecting human rights.

The increasing tension between technological innovation and the protection of data privacy has been a focal point of legal discussions, particularly in the context of big data and artificial intelligence (AI). The risk regulation theory highlights the need for legal frameworks that proactively address the potential risks of emerging technologies. This is crucial when considering the exponential growth of data collection and processing capabilities, which, as demonstrated by scandals like Cambridge Analytica, can easily infringe on individuals' privacy (Rosyalita, 2024). Here, the precautionary principle emphasizes the importance of safeguarding human rights in the face of technological uncertainty, a perspective echoed by the General Data Protection Regulation (GDPR), which balances innovation with privacy protection by enforcing strict data processing rules (European Commission, 2016). However, the GDPR, while a pioneering effort, faces criticisms for its potential to stifle innovation, particularly for small and medium-sized enterprises (SMEs), which may struggle with the compliance costs (Harianto, 2024). The principle of technology neutrality adopted by GDPR allows it to remain adaptable to new technologies, but challenges arise when applied to complex systems like AI, which can process personal data in ways that are opaque to users and regulators alike (Zaini, 2023).

In contrast, the United States' sectoral approach, exemplified by the California Consumer Privacy Act (CCPA) and the Health Insurance Portability and Accountability Act (HIPAA), offers flexibility but also results in fragmentation and gaps in privacy protection, especially in emerging fields like AI (Kartina, 2024). The Equifax data breach of 2017, where personal data of over 145 million individuals were

exposed, underscores the weaknesses in the U.S. privacy framework, which lacks a uniform, comprehensive approach to data protection (Takaeb et al., 2024). Meanwhile, in the Global South, countries like Indonesia face their own set of challenges in implementing effective privacy laws, despite the enactment of the Personal Data Protection Act (PDP) in 2022 (Republic of Indonesia, 2022). While this law marks progress, its implementation remains uncertain, as seen in the collection of biometric data for national ID systems without adequate safeguards (D. Saputra, 2023).

Furthermore, as technological innovations continue to outpace the ability of legal frameworks to keep up, the integration of ethical principles into data privacy laws becomes essential. Legal frameworks like GDPR, though grounded in legal norms, must incorporate ethical considerations surrounding fairness, accountability, and transparency, particularly in the AI context. This shift towards ethics-driven regulation will be critical for ensuring that technology benefits society while respecting fundamental rights. Finally, global cooperation will be necessary to harmonize data privacy laws, addressing the transnational nature of data flows and preventing exploitation by multinational corporations, thus safeguarding individuals' privacy rights globally. The challenge lies in ensuring that privacy laws are flexible, enforceable, and capable of adapting to the ever-evolving technological landscape, as demonstrated by both successful frameworks like GDPR and the shortcomings of fragmented approaches such as in the U.S.

CONCLUSION

The conclusion of this study shows that despite significant progress in the development of personal data protection laws, especially with the implementation of regulations such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, there are still major challenges in creating a truly effective legal framework at the global level. While the GDPR provides an example of success in balancing technological innovation with the protection of individual privacy rights, its strict implementation and high compliance costs can be a barrier for small and medium-sized businesses. In addition, a fragmented sectoral approach in the United States results in uneven protection, especially in the rapidly evolving field of technology such as artificial intelligence (AI). Nevertheless, this regulation still shows the importance of regulations that can maintain privacy without hindering innovation, and become the basis for the formation of broader policies.

On the other hand, countries with newer or less than perfect legal infrastructures, such as Indonesia, present their own challenges in terms of the implementation of personal data protection regulations. Although Indonesia has passed the Personal Data Protection Law (PDP) in 2022, the implementation of this law still faces obstacles, especially in terms of supervision and compliance with inadequate data collection practices. In this context, the application of ethical principles in personal data protection law is very relevant. The integration of the principles of fairness, accountability, and transparency in personal data protection regulations will strengthen the protection of individual privacy rights while supporting the development of innovative technologies. Therefore, international cooperation to harmonize personal data protection policies will be crucial to face the ever-evolving global challenges in this digital era.

REFERENCES

Adams, M. (2017). Big data and individual privacy in the age of the internet of things. *Technology Innovation Management Review*, *7*(4).

Aiello, S. (2024). Privacy Principles and Harms: Balancing Protection and Innovation. *Journal of Cybersecurity Education, Research and Practice*, *2024*(1), 15.

Ali, A. (2024). Artificial Intelligence and Data Privacy: Balancing Innovation with Security. *Frontiers in Artificial Intelligence Research*, *1*(02), 289–328.

Ambedkar, N. S. (n.d.). *PRIVACY RIGHTS AND DATA PROTECTION IN CONSUMER LAW: BALANCING INNOVATION AND REGULATION*.

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic'in literature reviews. *Formulating Research Methods for Information Systems: Volume 2*, 48–78.

Bryman, A. (2016). *Social research methods*. Oxford university press.
Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.
Debbarma, R. (2023). The changing landscape of privacy laws in the age of big data and surveillance. *Rivista Italiana Di Filosofia Analitica Junior*, *14*(2), 1740–1752.
Ehimuan, B., Chimezie, O., Akagha, O. V., Reis, O., & Oguejiofor, B. B. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070.
Fitrianingsih, F., Rahayu, H. W. S., & Najahah, K. (2024). Technique Self Management In Overcoming Procastination Of Junior High School Students. *Side: Scientific Development Journal*, *1*(3), 97–101.
Habibah, N. (2024). Pengembangan Kompetensi Karyawan di Era Digital: Tantangan dan Strategi bagi Departemen MSDM. *Journal of Knowledge and Collaboration*, *1*(1), 23–27.
Hakim, L. (2024). Manajemen peserta didik berprestasi melalui pendekatan spiritual. *Indonesian Journal of Research and Service Studies*, *1*(1), 49–65.
Harianto, J. E. (2024). Implementasi Manajemen Pendidikan Berbasis Teknologi dalam Meningkatkan Kualitas Pembelajaran. *Indonesian Journal of Research and Service Studies*, *1*(4), 169–177.
Hidayat, R., Manurung, F., Sinaga, C. H., & Suci, R. M. (2024). PENEGAKAN HUKUM PIDANA TERHADAP PEMBERIAN HUKUMAN KEBIRI BAGI PEDOFILIA DARI PERSPEKTIF HAM. *Mandalika Law Journal*, *2*(1), 1–8.
Kartina, H. B. (2024). PENGARUH GAYA KEPEMIMPINAN DAN BUDAYA ORGANISASI TERHADAP DISIPLIN KERJA SERTA DAMPAKNYA PADA KINERJA PEGAWAI PUSKESMAS PUGUNG RAHARJO KABUPATEN LAMPUNG TIMUR. *Journal of Mandalika Social Science*, *2*(1), 97–114.
Lawalata, J. N., Djogo, A. T. L., & Panjaitan, J. D. (2024). MEDIASI PENAL SEBAGAI UPAYA PENYELESAIAN KASUS MALPRAKTIK DI BIDANG MEDIS. *Jurnal Cahaya Mandalika ISSN 2721-4796 (Online)*, *5*(1), 109–123.
Lundström, M., & Lundström, T. P. (2021). Podcast ethnography. *International Journal of Social Research Methodology*, *24*(3), 289–299.
Moleong, L. J. (2000). Qualitative Research Methodology, Bandung: PT. *Youth Rosdakarya*.
Nadir, J., & Farah, J. (2023). *Balancing AI Innovation and Data Protection: Regulatory Challenges and Opportunities*.
Patton, M. Q. (2002). *Qualitative research & evaluation methods*. sage.
Rayhan, R., & Rayhan, S. (2023). AI and human rights: balancing innovation and privacy in the digital age. *DOI: 10.13140/RG. 2.2*, *35394*.
Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data Privacy and Protection: Legal and Ethical Challenges. *Emerging Threats and Countermeasures in Cybersecurity*, 433–465.
Richard, M., & Schlick, K. (2024). *Data Governance in the AI Era: Balancing Privacy, Human Rights, and Algorithmic Accountability*.
Rosyalita, D. (2024). Strategi Inovatif dalam Manajemen Sumber Daya Manusia untuk Meningkatkan Kinerja Organisasi. *Journal of Knowledge and Collaboration*, *1*(7), 324–330.
Rouvroy, A. (2008). Privacy, data protection, and the unprecedented challenges of ambient intelligence. *Studies in Ethics, Law, and Technology*, *2*(1).
Saputra, D. (2023). Analisis Dampak Kepemimpinan Transformasional terhadap Kinerja Organisasi: Studi Komparatif pada Berbagai Sektor Industri. *Mandalika Journal of Business and Management Studies*, *1*(1), 11–15.
Saputra, D. R., Dony, M., Siregar, H., & Imelda, R. (2024). The Crime of Genocide and Its Implications In Law Number 39 Of 1999 Concerning Human Rights. *Journal of Law and Humanity Studies*, *1*(2), 21–27.
Saxena, A. K. (2020). Balancing privacy, personalization, and human rights in the digital age. *Eigenpub Review of Science and Technology*, *4*(1), 24–37.
Sembiring, T. B., Marshinta, F. U., Mangkunegara, R. M. A., Utami, I. S., & Haipon, H. (2024). Digital

Privacy Rights in the Age of Big Data: Balancing Security and Civil Liberties. *Global International Journal of Innovative Research*, *2*(3), 712–720.

Sharma, G., hD Scholar, P., & Bassi, A. (n.d.). *" BALANCING PRIVACY AND INNOVATION: ASSESSING DATA PROTECTION LAWS IN THE MODERN ERA*.

Singh, B. (2024). Cherish Data Privacy and Human Rights in the Digital Age: Harmonizing Innovation and Individual Autonomy. In *Balancing Human Rights, Social Responsibility, and Digital Ethics* (pp. 199–226). IGI Global.

Singla, A. (2024). The Evolving Landscape of Privacy Law: Balancing Digital Innovation and Individual Rights. *Indian Journal of Law*, *2*(1), 1–6.

Sollisa, R. A. (2024). The Effect of the Application of Big Data Technology in Increasing Agricultural Productivity in Rural Areas of the Philippines. *Journal of Law and Humanity Studies*, *1*(1), 9–12.

Song, L., & Ma, C. (2022). Identifying the fourth generation of human rights in digital era. *International Journal of Legal Discourse*, *7*(1), 83–111.

Sugiyono, D. (2013). *Educational research methods approach quantitative, qualitative and R&D*. Bandung: Alfabeta.

Sumartono, E. (2024). The Life of Seafarers in the Digital Age: An Analysis of the Philosophy of Ethics and Morality in the Use of Technology. *Side: Scientific Development Journal*, *1*(3), 78–87.

Takaeb, A. F., Gunawan, R., & Nugroho, A. R. (2024). Menurunkan Kecanduan Game Online Melalui Konseling Kelompok Dengan Teknik Self Management. *Journal of Mandalika Social Science*, *2*(1), 62–70.

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). *Introduction to qualitative research methods: A guidebook and resource*. John Wiley & Sons.

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, *11*, 239.

Vargiolu, A. (2022). *Personal Privacy and Internet Regulation: Balancing Security and Freedom in the Digital Age*.

Yanamala, A. K. Y., Suryadevara, S., & Kalli, V. D. R. (2024). Balancing Innovation and Privacy: The Intersection of Data Protection and Artificial Intelligence. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *15*(1), 1–43.

Zaini, R. (2023). Manajemen Keragaman dalam Lingkungan Kerja Multikultural: Studi tentang Strategi Efektif dalam Mengelola Tim Multinasional. *Mandalika Journal of Business and Management Studies*, *1*(1), 21–25.