International Journal of Law, Crime and Justice

E-ISSN: 3047-1362
P-ISSN: 3047-1370

*Research Article*

# Personal Data Protection Analysis : Comparison of Indonesia, the United States as Federal Countries

**Sevy Septiana Afina [1*], Rina Arum Prastyanti [2]**

[1] Universitas Duta Bangsa, Surakarta, Indonesia 1; e-mail : sevysa0209@gmail.com
[2] Universitas Duta Bangsa, Surakarta, Indonesia 2; e-mail : rina_arum@udb.ac.id
* Corresponding Author : Sevy Septiana Afina

**Abstract:** Personal data protection is a crucial issue in the digital era, which is characterized by the processing and widespread dissemination of information on the internet. In this context, the different legal approaches between Indonesia and the United States raise questions regarding the effectiveness and scope of privacy protection in each country. The focus of this research is to analyze the legal systems applicable in both countries to identify the strengths, weaknesses, and potential for cross-system policy adoption. Using a normative juridical method and a comparative law approach, analysis is conducted on key regulations such as Law No. 27 of 2022 in Indonesia as well as various sectoral regulations in the United States. The findings show that Indonesia has integrated regulations but faces challenges in implementation, while the United States has more established enforcement despite its sectoral and fragmented nature. The synthesis of these two approaches emphasizes the importance of finding a balance between regulatory comprehensiveness and enforcement effectiveness. In conclusion, efforts to strengthen personal data protection in Indonesia can be directed towards strengthening institutions and oversight, while the United States can draw lessons from its centralized regulatory model to improve consistency of protection across sectors.

**Keywords:** Data protection; Indonesia; United States

## 1. Introduction

Personal data is a critical asset that is susceptible to misuse, so it needs to be protected to maintain privacy and public trust. While technology makes it easier to collect and manage data, it also increases the risk of misuse. Indonesia already has personal data protection regulations, but there are still gaps in implementation due to unclear regulations, weak law enforcement, and low public awareness of privacy rights and digital threats.

To address this issue, Indonesia passed Law No. 27 of 2022 on Personal Data Protection (PDP Law) to regulate various aspects, such as the rights of data owners, the responsibilities of data controllers, principles in data processing, as well as the establishment of independent supervisory institutions such as general principles in line with the General Data Protection Regulation of the European Union. The United States, on the other hand, has a different approach, in that it does not yet have a comprehensive federal law on personal data protection by enacting sectoral laws. However, a number of states have begun to pass their own regulations, prompting serious discussions about the need for unified federal regulation, as reflected in California's CCPA and CPRA.

The development of digital technology has changed the way people interact, work and live their daily lives. Personal data is very easily collected, stored and processed through various digital platforms, such as public services and social media applications which raises concerns about how the data is used, who has access, and the extent to which individuals can control their personal information, meaning personal data protection is no longer just a

**Received:** May, 17 2025
**Revised:** May, 30 2025
**Accepted:** June, 15 2025
**Published:** June, 17 2025
**Curr. Ver.:** June, 17 2025

technical issue, but has become an important part of human rights protection in the digital age. Without clear regulations and strong protection mechanisms, personal data can easily be exploited for commercial, political or criminal purposes. Each country responds to this challenge in its own way, depending on its legal system and government structure. Meanwhile, Indonesia and the United States have developed personal data protection policies in different ways.

Data protection requires a legal system that is comprehensive, adaptive, and responsive to technological advances and the dynamics of a digital society, so that it can provide maximum protection to individual privacy rights without hindering technological innovation. In this context, personal data protection laws should be comprehensive and centralized to avoid regulatory gaps or overlaps. The ideal regulation should explicitly guarantee the rights of data subjects, such as the right to access, rectify, delete and transfer personal data. An independent and strong supervisory body is also needed to ensure effective implementation of the law, along with a strict system of sanctions, both administrative and criminal, for violations. The General Data Protection Regulation (GDPR) is also crucial, so that data protection can be applied across jurisdictions with the principles of equality and prudence.

Although personal data protection has become a global concern, the regulatory approaches adopted by different countries still show significant differences. Some countries, such as EU countries, have implemented a centralized and comprehensive legal framework such as the GDPR. In contrast, Indonesia has just passed the Personal Data Protection Law No. 27 of 2022, as the initial implementation stage faces various challenges, including institutional capacity, development of supporting regulations, and public awareness. The United States, as a federal country, does not have a comprehensive, national personal data protection law or it remains sectoral, with various specialized regulations, and relies heavily on state-level legislatures. While California has made efforts through regulations such as the CCPA and CPRA, legal fragmentation remains a significant issue affecting the effectiveness of national data protection. Comparisons between Indonesia and the United States in the context of personal data protection are limited, especially when considering the impact of government structure (centralized vs. federal) on the effectiveness of legal protection.

This research uses a comparative approach to analyze the legal systems of personal data protection in Indonesia and the United States, focusing on how governance structures influence the establishment of effective regulatory frameworks. Previous research on personal data protection has only focused on the normative aspects or substantive comparison of regulations, without delving deeper into the governance context underlying the formulation of these policies. This research also critically examines harmonization efforts with international standards such as the General Data Protection Regulation (GDPR) and analyzes the potential adoption of data protection principles in various jurisdictions. This research can contribute to the development of Indonesia's legal system, such as strengthening oversight

institutions, improving the effectiveness of law enforcement, and providing more comprehensive protection of the rights of data subjects.

The use of big data from social media in social research highlights several methodological issues, such as the representativeness, validity and context of the data. While platforms like Twitter or Facebook provide broad access to digital social behavior, the use of such data often ignores the fact that social media users are not representative of the entire population. There are biases in who uses the platform, how the platform is used, and how algorithms distribute information. Many studies also fail to consider the social context and interpretation of meaning behind online activities, potentially leading to misleading conclusions. Methodological caution is therefore essential in utilizing big data, including the need to integrate quantitative and qualitative approaches and an understanding of the social and technological dynamics behind the data collected. The main focus should be on maintaining scientific accuracy and analytical relevance when handling large volumes of digital data.

The concept of personal data protection is not only legal-formal, but also has a normative dimension that is closely related to the principles of ethics, human dignity and justice. Privacy protection reflects basic values that illustrate respect for individual autonomy and the right to control personal information. In the context of technological advancement, ethical principles are becoming increasingly important in guiding policy and regulatory formulation, especially as data collection and processing capacities become more extensive and complex. Principles such as transparency, fairness, accountability and proportionality should be the normative basis for designing data protection systems that are responsive to digital challenges. Personal data protection should therefore be viewed as an effort to maintain a balance between the interests of technological innovation and the protection of individual human rights in the modern information society.

## 2. Literature Review

This section must contain a state-of-the-art explanation. It can be explained in several ways. First, you can discuss several related papers, both about objects, methods, and their results. From there, you can explain and emphasize gaps or differences between your research and previous research. The second way is to combine theory with related literature and explain each theory in one sub-chapter.

In Indonesia, the study of personal data protection has grown rapidly following the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). Some scholars, such as Wahyudi Djafar (2022) and Rony Syahrudin (2023), emphasize the importance of institutional set-up and strengthening of supervisory mechanisms to ensure effective implementation of the PDP Law. However, these studies are generally still limited to normative aspects and do not compare practices with other countries. Research on personal data protection has become a major topic in legal and public policy literature due to the increasing threats to individual privacy in the digital age. Several studies highlight the need for

strong and comprehensive regulations to address data collection, storage and processing by public and private entities. The right to personal data protection and the right to privacy are inseparable, as both are progressively understood in the context of technological developments that emphasize the importance of a rights-based approach in designing data policies (Yvonne McDermott, 2017). In the context of personal data protection, threats are not only technical but also related to social control and power imbalances between individuals and data collection institutions (Solove, 2006).

According to Schwartz and Solove (2011), the United States has sectoral laws that shape privacy policy, discussing the fragmentation of regulation in the US and the challenges of harmonizing national policies. The California Consumer Privacy Act (CCPA) is often held up as an example of progressive state-level regulation that gives consumers control over their data, although it has not been widely adopted across the US. However, there are very few studies that specifically compare the Indonesian and US legal systems in the context of personal data protection, especially when considering the different legal systems (civil law vs. federal common law) as well as centralized versus sectoral regulatory approaches. Therefore, this literature review highlights a significant space for comparative research that not only examines the rule of law but also evaluates the implementation effectiveness and relevance of best practices between legal systems.

### 2.1. Personal Data Protection Theory

Privacy protection is an important asset of the right to privacy. Westin (1967) states that privacy is the ability of individuals to control their personal information and determine when and to whom it is disclosed. As technology advances, the approach to data protection becomes more complex. Solove (2006) developed a theory of data protection that deals with confidentiality, surveillance, extensive data collection, and potential abuse by public and private institutions. Meanwhile, McDermott (2017) argues that personal data protection should be seen as a recognition of human rights in the digital environment. Indonesia's PDP Law represents a shift from an administrative to a rights-based approach, similar to the principles set out in the European Union's General Data Protection Regulation (GDPR).

### 2.2. Comparative Legal Theory

Comparative law in these two countries uses a scientific approach to understand the characteristics of different legal systems to find the best solution or perfect the national legal system, such as five methods in comparative law: historical background, legal structure, legal institutions, terminology, and basic ideas of the legal system (Zweigert and Kötz, 1998). This comparison is used to analyze the Indonesian legal system which is based on civil law and the United States which uses common law within a federal state framework, so that what can be analyzed is not only the legal substance, but also the social, political and cultural context that influences the implementation of personal data protection in both countries.

### 2.3 Federal State Theory

Federalism is a system of power sharing between the central government and local (state) governments, each with its own constitutional authority. Wheare (1963) argues that a system of federalism is characterized by a written constitution that formally divides power between the two levels of government. In relation to personal data protection, the federal system in the United States means that there are no nationally uniform privacy laws. Instead, laws are sectoral and largely enforced by the states, such as California through the California Consumer Privacy Act (CCPA). This is in contrast to Indonesia's unitary state system, which allows for the creation of national laws that apply uniformly across the country.

## 3. Proposed Method

This research on personal data protection uses a normative juridical approach with a comparative law method to analyze and compare regulations, legal principles, and institutional frameworks related to personal data protection in Indonesia and the United States, taking into account the different legal structures and government systems in the two countries. The method used in this research is a qualitative descriptive method, which focuses on analyzing legal texts, legal doctrines, and relevant public policies..

The research is grounded in three main theoretical frameworks. First, the theory of personal data protection, which explains individuals' rights to privacy and the fundamental principles of personal data management within the context of technological advancement. Second, comparative law theory serves as a methodological approach to understand and evaluate the differences and similarities between legal systems, including their governmental structures and legal traditions. Third, federalism theory explains the federal structure of the United States and its implications for the formulation and implementation of legal policies, particularly in the area of personal data protection.

The primary data in this research are laws and regulations such as Law No. 27 of 2022 on Personal Data Protection (PDP Law) in Indonesia and various regulations at the federal and state level in the United States, such as the California Consumer Privacy Act (CCPA). Secondary data was obtained from various academic literatures, legal journals, reports of international organizations, and court decisions relevant to the research topic. Data collection was conducted by using content analysis to identify the substantive meaning of applicable legal norms and conducting a comparative study of the legal systems of Indonesia and the United States in terms of legal substance, institutional structure, and legal culture, while taking into account the social, political, and governmental context of each country.

## 4. Results and Discussion

Personal data protection can be understood as an effort to protect and secure information relating to a person's identity from being misused. The term consists of three main elements: “protection”, which means the act of keeping something safe from threat or

harm; 'data', which refers to information or details that can be processed, whether in the form of writing, numbers, images, or sounds; and 'personal', which relates to an individual or something that belongs to a private person. As such, personal data protection refers to measures or mechanisms to secure all information related to a person, such as name, address, identification number, financial information, or digital footprint, to prevent unauthorized access, use, or dissemination without the owner's consent. This protection is very important to uphold the right to privacy and prevent misuse of data by irresponsible parties. Data protection and privacy are closely related. Individuals need the right tools and skills to implement personal data protection and protect their information from misuse by unauthorized entities. It is also essential for data processors to understand their responsibilities and take appropriate measures to protect users' personal data.

According to some experts, personal data protection is an integral part of the right to privacy, which is a fundamental right of every individual. Alan F. Westin, a leading privacy expert, defines privacy as the right of individuals to control how their personal information is collected and used. In his book Privacy and Freedom (1967), Westin emphasized that control over personal information is key to maintaining individual autonomy in the technological age. Meanwhile, Daniel J. Solove argues that personal data protection is not only about maintaining confidentiality but also how data is used, disseminated and stored. In the concept of "privacy taxonomy", Solove highlighted various forms of privacy violations, including surveillance, unauthorized dissemination, and labeling. On the other hand, Charles Raab asserts that data protection should be seen as an ethical and public policy issue, as it involves balancing the interests of the individual with those of the state or company. These experts emphasized that personal data protection is not just a technical issue, but also a legal, ethical, and individual freedom issue in the digital age.

In the framework of personal data protection policies, anonymization technologies are often considered as the main solution to reduce privacy risks. While anonymization has the potential to reduce the exposure of personal data, these techniques often fail to provide the expected protection. Data deletion or obfuscation cannot fully guarantee security, as anonymized data remains vulnerable to de-anonymization attacks, especially in the context of big data and analytics that integrate other data sources. Therefore, data protection policies that rely too much on anonymization technologies may create the illusion of ineffective protection. A more effective policy should not only rely on anonymization technology as the only solution, but should also introduce a more comprehensive approach. This approach includes greater control for individuals over their personal data, clearer transparency in data usage, and stricter oversight of data collection and distribution. This more comprehensive policy framework is essential to ensure the protection of individuals' right to privacy, even as anonymization-related technologies continue to evolve.

Personal data protection in Indonesia has been regulated through various regulations, both specialized and sectoral in nature. The main regulation that provides detailed guidance is Law No. 27 of 2022 on Personal Data Protection (PDP Law), which is an important milestone in Indonesia's legal system on data privacy and security. It regulates the rights of data subjects, the obligations of data controllers and processors, the legal basis for data processing, and the establishment of an independent supervisory authority tasked with overseeing compliance with the provisions of the law. Prior to the enactment of the PDP Law, limited personal data protection was regulated in Law No. 11/2008 on Electronic Information and Transactions (ITE Law), specifically in Article 26 paragraph (1), which states that the use of personal information in electronic systems must obtain the consent of the data owner. This regulation is further strengthened through Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions (PP PSTE), which outlines the responsibilities of electronic system providers in maintaining the confidentiality and security of user data.

The proposed regulation to replace Directive 95/46/EC is an important step forward in strengthening personal data protection in the European Union. The new regulation, known as the General Data Protection Regulation (GDPR), is designed to give individuals greater control over their personal data and increase transparency in data processing by data controllers. It emphasizes the rights of individuals by introducing new provisions such as the right to access data, the right to be forgotten, and the obligation to inform data subjects about the processing of their personal data. An important element of the regulation is the enforcement of stricter sanctions against privacy violations, with the aim of creating higher accountability among data controllers and improving regulatory compliance. However, while this policy offers stronger protections, there are some technical and implementation challenges to be faced, such as how to adapt this regulation to the rapid technological advancements and complexities of data globalization. In this policy analysis, it is important to assess the extent to which the regulation is able to respond to these challenges and how it can be adjusted to ensure better privacy protection without hindering innovation and the growth of the digital economy. Overall, the GDPR may be a better policy model for protecting personal data, but its implementation should be accompanied by close monitoring and adjustments over time. It was emphasized that while the GDPR aims to provide strong protection of individuals' personal data, many of the core principles in the regulation are at odds with data processing practices used in big data, artificial intelligence (AI) and predictive analytics. One of the main issues raised is that the GDPR requires explicit consent from individuals for data collection, which becomes difficult to implement in the context of big data, where data is often collected in large quantities and does not always come from clear or identifiable sources. In addition, the concept of the right to be forgotten in the GDPR is also

difficult to apply in big data, as data that is widely dispersed and used across multiple contexts is difficult to completely erase.

The use of Internet of Things (IoT) devices that continuously collect and transmit personal data is an important issue that requires the implementation of appropriate regulations. The PDP Law passed in 2022 provides a legal framework for protecting personal data, but its implementation in the IoT ecosystem faces significant challenges, especially in the technological and regulatory aspects. One of the key challenges is the application of regulations to IoT devices, which are diverse and often difficult to track. IoT collects large amounts of data in real-time, increasing the risk of data breaches and misuse of personal data. Therefore, the implementation of more advanced data security technologies, such as encryption and strict auditing, is important to protect user data. In addition, the importance of supervision and law enforcement is essential to ensure effective data protection. The government and private sector must work together to ensure that IoT devices on the market meet high security standards. Public awareness regarding their privacy rights is also crucial for this regulation to be effectively implemented. Overall, this article suggests that Indonesia should continue to adjust and update its regulations on personal data protection to anticipate rapid technological changes. A comprehensive, flexible and sustainable regulatory approach will be needed to ensure that individuals' privacy remains protected amidst the rapid development of IoT. While technology can help strengthen data security, concerns remain regarding the potential misuse of data by third parties, especially with the proliferation of technologies such as big data, cloud computing, and IoT. Therefore, the protection of personal data cannot rely solely on legal policies, but must also be accompanied by enhanced cybersecurity and private sector involvement in ensuring that consumer data is protected.

In Bygrave's book, it is argued that personal data protection regulation should be based on the right to individual privacy, which includes the principles of transparency, consent, accountability and individual control over their personal data. These principles need to be adopted globally, despite the differences in legal systems and cultures between countries. The proposed normative framework emphasizes the need for harmonization of data protection policies at the international level to effectively protect privacy rights in the face of the challenges of globalization and new technological developments such as big data and artificial intelligence (AI). The book also highlights that data protection is not only a legal issue, but also an ethical issue relating to human dignity and individual freedom. Therefore, the regulations implemented must ensure that data protection policies not only protect personal information, but also support individual freedoms and maintain public trust in data management systems. In this context, a more holistic approach is needed so that data protection policies can quickly adapt to technological changes and global trends. The United States has not enacted one comprehensive federal law governing personal data protection, such as the General Data Protection Regulation (GDPR) in the European Union or the

Personal Data Protection Law (PDP Law) in Indonesia. Instead, the United States takes a sectoral and fragmented approach, with each sector or type of data governed by its own regulations. Some of the key federal laws in place include the Health Insurance Portability and Accountability Act (HIPAA) of 1996 for the protection of health data, the Gramm-Leach-Bliley Act (GLBA) of 1999 to regulate consumer financial data, and the Children's Online Privacy Protection Act (COPPA) of 1998 which regulates the data of children under the age of 13. In addition, the Federal Trade Commission Act (FTC Act) authorizes the Federal Trade Commission (FTC) to crack down on unfair and fraudulent business practices, including those related to data privacy violations. Beyond federal regulations, states have broad authority to pass their own data protection laws, leading to a wide variety of rules across the country. One of the most prominent is the California Consumer Privacy Act (CCPA) of 2018, which was strengthened by the California Privacy Rights Act (CPRA) of 2020. These regulations give consumers greater rights over their personal data and require companies to be more transparent in data collection and processing. Other states such as Virginia, Colorado and Connecticut have also followed suit. As such, personal data protection in the United States depends heavily on the type of data and the geographic jurisdiction in which it is processed, creating a diverse and non-uniform legal system nationwide. Meanwhile, the General Data Protection Regulation (GDPR) is an EU regulation that came into effect on May 25, 2018 and aims to strengthen and unify personal data protection across member states. GDPR gives individuals strong rights over their data, such as the right to access, correct, delete (right to be forgotten), and transfer their data (data portability). The GDPR also requires companies to obtain explicit consent before processing personal data and implement the principles of transparency, accountability and data security. The regulation applies not only to organizations within the European Union, but also to entities outside the EU that offer goods or services, or monitor the behavior of individuals within the EU. Fines imposed for GDPR violations can be up to €20 million or 4% of a company's total annual revenue, whichever is greater. Therefore, GDPR is seen as the global gold standard in personal data protection and has become a reference for many countries, including Indonesia, in shaping national regulations that are aligned with international privacy protection principles.

The California Consumer Privacy Act (CCPA) is a personal data protection law passed by the California state legislature in 2018 and took effect on January 1, 2020. This law gives consumers in California more control over their personal information. The CCPA provides consumers with the right to know what personal data is stored, access and delete that data, and object to the sale of their personal information to third parties. The CCPA also requires companies to maintain transparency and protect consumer data, and sets penalties for non-compliance. The CCPA is considered a milestone in privacy protection in the United States and is often used as a model for digital privacy policies in other states.

The Children's Online Privacy Protection Act (COPPA) is a United States federal law passed in 1998 to safeguard the privacy of minors of 13 when using online services. It requires websites, apps, and online platforms that are aimed at children or that knowingly collect data from children to receive accountable parental consent before collecting, using or disclosing a child's personal information. Such information includes names, addresses, emails, phone numbers, locations, and other online identifiers. COPPA also requires relevant entities to provide clear privacy policies, ensure data security, and limit data retention to only the necessary period. Enforcement is carried out by the Federal Trade Commission (FTC), and violations of these provisions may be subject to legal sanctions. However, COPPA only provides limited protection for voice data, which is increasingly collected by artificial intelligence (AI)-based devices such as smart speakers and virtual assistants. Children are often unaware of how their voice data is being used, stored, or even misused, and current regulations do not adequately anticipate the risks associated with voice data as biometric and behavioral data. A number of bills have been proposed to extend privacy protections to voice data and set clearer voice protection standards. Nonetheless, establishing a comprehensive legal framework remains a major challenge, especially in balancing the rapid development of technology and the protection of privacy rights.

The Federal Trade Commission Act (FTCA) is a United States federal law passed in 1914 to prevent unfair trade practices and protect consumers and promote fair competition in the marketplace. The act established the Federal Trade Commission (FTC), an independent agency authorized to investigate and act against violations of antitrust and consumer protection laws. The FTCA prohibits "unfair or misleading acts or practices in commerce," which includes false advertising, misleading marketing, and anti-competitive behavior such as monopolies or cartels. The FTC has the authority to issue cease-and-desist orders, formulate administrative rules, and initiate legal action against businesses that violate the Act. Over time, the FTCA has become an important foundation of consumer and trade regulation in the United States, whose relevance extends to the digital age and personal data protection. Through its broad mandate, the FTC plays an important role in protecting consumers from misleading practices, including those involving the misuse of personal information in the online and digital environment.

The Gramm-Leach-Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act, is a United States federal law that establishes how financial institutions collect, use, and protect consumers' personal information. The law has three main provisions: Financial Privacy Protection Guidelines, which require financial institutions to inform consumers of their privacy protection policies and provide the option not to share their data with third parties; Safeguards Guidelines, which require institutions to develop and implement security measures to protect consumer information; and a prohibition against pretexting, which refers to the fraudulent acquisition of personal data. GLBA is designed to strike a

balance between the modernization of financial services and the protection of consumers' privacy rights, especially in the banking, insurance, and securities sectors. Enforcement of the GLBA is carried out by agencies such as the Federal Trade Commission (FTC), which ensures that institutions comply with the privacy and data protection standards set by this law.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a United States federal law that aims to improve the efficiency of the healthcare system and protect the confidentiality and safety of individuals' medical data. HIPAA has two main components: first, it ensures portability of health insurance coverage for workers and their family members when they change jobs or lose their jobs, and second, it sets national standards for the protection of individually identifiable health information, known as Controlled Health Information (PHI). Through the enactment of rules such as the Privacy Rule and Security Rule, HIPAA requires healthcare providers, insurers, and their business partners to protect patient medical data in both physical and digital formats. Violations of HIPAA are subject to civil and criminal penalties. This law serves as the basic legal framework for health data protection in the United States.

Fundamental differences between the regulations on personal data protection in Indonesia and the United States lies in the regulatory approach. Indonesia adopts a comprehensive approach with a PDP Law that applies nationally and covers all sectors. Meanwhile, the US applies a sectoral and decentralized approach, where data protection is regulated based on specific sectors without any overarching federal legislation. In addition, Indonesia has a unitary state system with uniform regulations across the country, whereas the US, with its federal system, allows states to create their own regulations. Differences are also seen in legal traditions: Indonesia uses a civil law system, while the US relies on a common law system that favors judicial precedent.

While the regulations regarding personal data protection system in Indonesia and he United States aim to provide effective protection for individual privacy, both have weaknesses that need to be addressed. In Indonesia, the main weakness of Law No. 27 of 2022 on Personal Data Protection (PDP Law) lies in its limited implementation and supervisory capacity. While this law covers many aspects of data protection, the biggest challenge is the effectiveness of supervision by the newly established personal data protection authority. The infrastructure and resources required to comprehensively enforce this regulation across Indonesia are still very limited, which may lead to legal uncertainty and difficulties in enforcement. In addition, the heavy reliance on explicit consent from data subjects may result in a lack of understanding among the public regarding the legal implications of their consent. Meanwhile, in the United States, the main weakness lies in regulatory fragmentation resulting from a sectoral and decentralized approach. The absence of a comprehensive federal personal data protection law leads to legal uncertainty, with companies having to comply with various rules in different sectors and states. This not only creates confusion for businesses, but also

leads to disparities in the level of data protection for individuals across states. In addition, surveillance systems that rely on agencies such as the Federal Trade Commission (FTC) are often less assertive in addressing personal data breaches, as the primary focus is on deceptive business practices rather than comprehensive data protection oversight. Other weaknesses include inadequate protection of children's personal data outside of the COPPA framework, as well as reliance on consent that is not always easily understood by consumers in the digital ecosystem.

Data leak cases in Indonesia and the United States highlight the urgency of stronger privacy protections for individuals in the digital age. In Indonesia, the BPJS Kesehatan data leak in 2021 became a major issue, where data on more than 279 million people, including their National Identification Numbers (NIK), addresses, phone numbers, and other sensitive information, was leaked and sold on online forums. In that situation, Indonesia did not yet have a Personal Data Protection Law (UU PDP), so the response was limited to investigations by the Ministry of Communication and Information Technology (Kominfo) and the National Cyber and Crypto Agency (BSSN) without adequate legal sanctions. Meanwhile, in the United States, the Facebook-Cambridge Analytica scandal in 2018 revealed the misuse of data of around 87 million Facebook users without proper consent, which was then used for political campaign purposes, including the presidential election. As a result of this negligence, Facebook was fined $5 billion by the Federal Trade Commission (FTC). This case emphasized the weakness of the sectoral regulatory system in the US and triggered the emergence of state-level data protection regulations, such as the California Consumer Privacy Act (CCPA).

Indonesia and the United States have made various efforts to strengthen personal data protection as threats to privacy increase in the digital era. In Indonesia, the main effort was realized through the passage of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which provides the national legal basis for comprehensively protecting personal data. The government is also preparing an independent supervisory authority to oversee the implementation of this law, impose sanctions, and improve public digital literacy. In addition, socialization and training are conducted for businesses and public agencies to improve compliance with data protection principles. On the other hand, while the United States has yet to pass a comprehensive federal personal data protection law, it has taken steps through strengthening state-level regulations, most notably through the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), which give consumers significant rights over their personal data. In addition, agencies such as the Federal Trade Commission (FTC) have become increasingly active in addressing privacy violations through investigations and imposing substantial sanctions on digital companies that ignore or misuse user data. Amid technological developments, both countries are also promoting international and regional collaboration to improve cybersecurity standards and cross-border data protection. Through

these initiatives, Indonesia and the United States seek to address global privacy challenges with approaches tailored to their respective legal and social systems.

Although the Personal Data Protection Law (PDP Law) is designed to provide better protection for personal data, key challenges include a lack of capacity and coordination among state agencies responsible for personal data protection. Although a personal data protection authority has been established as a supervisory body, it still faces limitations in terms of human resources, competencies and budget to effectively carry out its duties. This has resulted in weak oversight of sectors that process large amounts of personal data, especially the private sector. In addition, the lack of understanding and awareness among businesses, government agencies, and the public about the importance of personal data protection is a significant obstacle to the implementation of the PDP Law. A supervisory system that has not been effectively integrated also worsens the implementation of this regulation. Therefore, it should be emphasized that there is a need for more intensive education and training for all parties involved in personal data management, so that Indonesia can increase institutional capacity and strengthen inter-agency cooperation to improve the effectiveness of the implementation of the PDP Law. In addition, a more holistic approach is needed to address these institutional challenges, including strengthening law enforcement, raising public awareness, and improving the infrastructure that supports personal data protection.

## 5. Comparison

Indonesia and the United States share a common goal of protecting individual privacy in the digital era but adopt different approaches based on their respective legal and governmental structures. Indonesia, as a unitary state with a civil law legal system, implements a comprehensive, nationwide regulation through Law No. 27 of 2022 on Personal Data Protection (PDP Law). This law broadly governs data subjects' rights and data controllers' obligations, and it establishes an independent supervisory authority. However, major challenges remain in implementation and oversight, particularly due to institutional capacity limitations and low public awareness. In contrast, the United States, with its federal system and common law tradition, adopts a sectoral approach. There is no single federal data protection law; instead, data privacy is regulated based on data type—for example, HIPAA for health data, COPPA for children's data, and CCPA/CPRA at the state level in California. Enforcement is carried out by various agencies, primarily the Federal Trade Commission (FTC), but the fragmented legal landscape across states leads to unequal levels of protection. Overall, Indonesia needs to strengthen its implementation mechanisms and supervisory authority, while the U.S. should work toward greater national harmonization. Both countries can learn from each other and align with international standards such as the GDPR to address global privacy and data protection challenges.

## 6. Conclusions

Although Indonesia and the United States share a common objective of protecting personal data as part of individual privacy rights in the digital era, their approaches differ significantly due to divergent legal systems and governmental structures. Indonesia, as a unitary state with a civil law system, adopts a centralized and comprehensive approach through Law No. 27 of 2022 on Personal Data Protection (PDP Law). This regulation outlines the rights of data subjects, the obligations of data controllers, and the establishment of an independent supervisory authority. However, implementation challenges remain, particularly due to limited institutional capacity and low public awareness. Conversely, the United States, as a federal state with a common law system, employs a sectoral and fragmented regulatory model, with different laws applying to specific types of data, such as HIPAA, COPPA, and the CCPA/CPRA at the state level. This fragmented approach leads to inconsistencies in protection across jurisdictions and complicates efforts to achieve national harmonization. This study emphasizes that effective personal data protection must be adaptive, rights-based, and supported by strong institutional frameworks, regardless of the legal system in place. Indonesia must focus on strengthening enforcement mechanisms and institutional capacity, while the U.S. is encouraged to move toward a more harmonized federal framework. Both countries would benefit from aligning their data protection laws with international standards such as the GDPR to address the growing global challenges in digital privacy and cross-border data flows.

## References

[1] F. Arianti, "Data Protection in the Digital Age: Facing Legal Challenges in Indonesia," Cyberlaw Nusantara Review, vol. 1, no. 1, pp. 21–24, 2024.
[2] G. Anand, A. Y. Hernoko, and A. G. Dharmadji, "The Urgency of Enacting Personal Data Protection Law as a Patronage from the Development of Communication and Information Technology in Indonesia," Perspektif, vol. 25, no. 1, 2020.
[3] T. R. Ananthan and M. F. Zolkipli, "Challenges and Issues in Implementing Personal Data Protection," International Journal of Recent Contributions from Engineering, Science & IT (iJES), vol. 10, no. 2, pp. 53–61, 2022, doi: 10.3991/ijes.v10i02.29373.
[4] L. A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford: Oxford University Press, 2014.
[5] F. H. Cate, "The Failure of Fair Information Practice Principles," in *Consumer Protection in the Age of the 'Information Economy'*, pp. 343–366, 2010.
[6] California Legislature, *California Consumer Privacy Act of 2018*, Cal. Civ. Code §§ 1798.100–1798.199, West, 2018.
[7] P. De Hert and V. Papakonstantinou, "The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals," *Computer Law & Security Review*, vol. 28, no. 2, pp. 130–142, 2012.
[8] N. van Dijk et al., "A Short History of Privacy in the Context of Information Technology," *Law, Innovation and Technology*, vol. 7, no. 1, pp. 1–17, 2016.
[9] S. Dutta and J. H. L. Hansen, "Navigating the U.S. Legislative Landscape on Voice Privacy: Existing Laws, Proposed Bills, Protection for Children, and Synthetic Data for AI," *arXiv preprint arXiv:2407.19677*, 2024.
[10] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L119, pp. 1–88, 2016.
[11] M. A. Fauzie, "Securing the Future: Indonesia Personal Data Protection Law and Its Implication for Internet of Things (IoT) Data Privacy," *Sriwijaya Crimen and Legal Studies*, vol. 2, no. 1, 2024.
[12] G. Hakim, H. Jabalnur, S. Ruliah, and M. Mohammad, "A Comparative Legal Analysis of Personal Data Protection Regulations in the EU and Indonesia," *Halu Oleo Legal Research*, vol. 5, no. 2, pp. 443–453, 2023.
[13] H. Hasnati and P. M. Seruni, "Consumer's Personal Data Protection in the Digital Era," *Jurnal Ius Constituendum*, vol. 8, no. 2, 2023.
[14] U.S. Congress, *Health Insurance Portability and Accountability Act of 1996*, Pub. L. No. 104-191, 110 Stat. 1936.
[15] L. Judijanto, N. Solapari, and I. Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *The Easta Journal Law and Human Rights*, vol. 3, no. 1, pp. 20–29, 2024.

[16] B. J. Koops et al., "A Typology of Privacy," *University of Pennsylvania Journal of International Law*, vol. 38, no. 2, pp. 483–575, 2017.
[17] C. Kuner, "The Internet and the Global Reach of EU Law," *Columbia Journal of Transnational Law*, vol. 52, pp. 117, 2015.
[18] Y. McDermott, "Conceptualising the right to data protection in an era of Big Data," *Big Data & Society*, vol. 4, no. 1, pp. 1–7, Jan. 2017, doi: 10.1177/2053951716686994.
[19] C. Nyst and T. Falchetta, "The Right to Privacy in the Digital Age: Challenges and Opportunities," *Journal of Human Rights Practice*, vol. 9, no. 1, pp. 104–118, 2017.
[20] P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, vol. 57, pp. 1701, 2010.
[21] P. M. Regan, "Privacy, Surveillance, and Public Trust," *Palgrave Communications*, vol. 1, no. 1, pp. 1–7, 2015.
[22] P. M. Schwartz, "Privacy, Ethics, and Data Protection," *International Data Privacy Law*, vol. 1, no. 1, pp. 1–3, 2011.
[23] N. Z. Silviani, R. S. Shahrullah, V. R. Atmaja, and J. H. Park, "Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea," *Jurnal Hukum dan Peradilan*, vol. 12, no. 3, pp. 517–546, 2023.
[24] M. Y. Sipahutar and L. M. Jannah, "Personal Data Protection Law in Indonesia: Institutional Challenges," *International Journal of Law Management & Humanities*, vol. 6, no. 4, pp. 1–17, 2023.
[25] D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477–560, 2006, doi: 10.2307/40041279.
[26] A. S. Sudarwanto and D. B. B. Kharisma, "A Comparative Study of Personal Data Protection Regulations in Indonesia, Hong Kong, and Malaysia," *Journal of Financial Crime*, vol. 29, no. 4, pp. 1443–1457, 2022.
[27] Z. Tufekci, "Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls," *Proceedings of the 8th International AAAI Conference on Weblogs and Social Media*, pp. 505–514, 2014.
[28] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
[29] U.S. Congress, *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. §§ 6501–6506.
[30] U.S. Congress, *Federal Trade Commission Act of 1914*, 15 U.S.C. §§ 41–58.
[31] U.S. Congress, *Gramm-Leach-Bliley Act of 1999*, 15 U.S.C. §§ 6801–6827.
[32] K. C. Wheare, *Federal Government*, Oxford: Oxford University Press, 1963.
[33] D. Wright and C. Raab, "Constructing a Surveillance Impact Assessment," *Computer Law & Security Review*, vol. 30, no. 3, pp. 224–239, 2014.
[34] A. F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967.
[35] K. Zweigert and H. Kötz, *An Introduction to Comparative Law*, 3rd ed., Oxford: Oxford University Press, 1998.
[36] T. Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," *Seton Hall Law Review*, vol. 47, no. 4, pp. 995–1020, 2016.