Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 16 (1), 2024
pp. 1293 - 1303

Personal Data Protection for Upholding the Right to Privacy in Indonesia, South Korea, and India

[1] Isharyanto [2]Hartiwiningsih [3]Sunny Ummul Firdaus

[1 2 3]Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia

Email : isharyanto_fh@staff.uns.ac.id*

Abstract: Data protection is a crucial legal issue as it pertains to constitutional rights and the necessity of situating this regime within the context of the right to privacy. Its relevance becomes particularly interesting to observe alongside global developments and the proliferation of digital information. This article discusses and describes the legal framework for data protection in Indonesia, which is significant to examine given the impending enactment of Law No. 27 of 2022. This article is based on doctrinal legal research that relies on primary and secondary legal materials, employing conceptual, legislative, and comparative law approaches. The experiences of South Korea and India serve as primary references for legal comparison. The research findings indicate a common legal motivation and a desire to integrate regimes influenced by global standards, as well as positioning data protection within the context of privacy rights as a further interpretation of constitutional provisions. For Indonesia, similar to India, there are challenges in further exploring the establishment of a supervisory body or authority related to data protection.

Keywords: Privacy, Data Protection, Humans Rights

Received:20 March 2024 **Revised:** 17 May 2024 **Accepted:** 22 June 2024

1. Introduction

The cybersecurity company Surfshark reported that by 2022, the number of data breaches reached 13 million accounts, while by mid-2024, the figure decreased to 700,000 accounts (Surfshark, 2024). Among Southeast Asian and G-20 countries, Indonesia ranks third and fourth from the bottom, respectively (Adri, 2024). This data highlights the vulnerability of personal information in Indonesia to unauthorized disclosure. When personal data is leaked and falls into the hands of third parties, various forms of misuse may occur, depending on the type of data compromised. Such incidents can harm individuals and potentially place their assets or lives at risk.

The cyberattack on the Temporary National Data Center (PDNS), which disrupted public services since June 2024, is regarded as the "most severe" among a series of governmental data breaches. Furthermore, in August, the Election Supervisory Board of DKI Jakarta investigated the alleged misuse of national identity cards (KTP) to meet the requirements for an independent gubernatorial candidate pair, Dharma Pongrekun-Kun Wardana. This incident also suggests the possibility of personal data leaks affecting citizens.

As a response to these data breach issues, nearly two years ago, the Indonesian government enacted the Personal Data Protection Law (Law No. 27 of 2022). This law consists of 16 chapters and 76 articles, specifically regulating the processing and storage of personal data for both private and public entities, including government institutions. It also mandates the establishment of implementing regulations, which are expected to be finalized by 2024, marking the transition period before the full enforcement of the law. These regulations will cover two key areas: the creation of a personal data protection authority and the technical implementation of personal data protection. The continued high incidence of data breaches indicates persistent challenges within the legal and practical frameworks, revealing ambiguities in the

processing of personal data.

There has been an inclusive debate on how cultures outside the Western world approach the concept of privacy, both in daily life and law. In the context of African nations, the right to privacy is not well-defined, explained, or protected (Wambiri et al., 2023). Moreover, some African communities view privacy within the framework of collectivism, communism, and interdependence (Prinsloo and\ Kaliisa, 2022; Makulilo, 2016), rather than individualism, meaning concerns over personal privacy are less prevalent as the culture prioritizes collective interests over individual ones. Nonetheless, some scholars argue that privacy is difficult or even impossible to define, and its conceptualization appears narrow (Piasecki and Chen, 2022; Prinsloo and Kaliisa, 2022; Ukwueze, 2021).

Meanwhile, domestic laws related to personal data protection must clearly define the scope of application, protection, data retention, destruction, third-party access, and safeguards against abuse and arbitrary use. For example, India's Supreme Court recently ruled that such requirements apply to the Aadhaar program, which has been criticized for lacking comprehensive privacy protection mechanisms (Beduschi, 2019).

In contrast, South Korea's various laws and executive authorities relevant to data privacy make it an interesting case for examining the structure and enforcement of personal data protection laws. South Korea's data protection legislation has developed rapidly, despite its relatively short history (Haksoo et al., 2016).

By mid-2014, 103 countries worldwide had enacted laws that met the criteria for national data protection legislation. The number of such laws has grown rapidly in each decade since the 1970s, with 22 new laws enacted in the first four years of this decade, marking the highest growth rate recorded. While more than half of these laws (53) still originate from European jurisdictions (EU member states), fifty data protection laws now exist outside Europe, and soon, non-European national laws will become the majority (Greenleaf, 2013). In Asia, which spans 26 countries from Japan to Afghanistan, including China and Timor Leste, ten countries have enacted comprehensive data protection laws covering the private sector. These laws include Taiwan's Personal Data Protection Act (2010), Hong Kong's Personal Data Privacy Ordinance (2012), South Korea's Personal Information Protection Act (2011), Macau's Personal Data Protection Act (2005), Japan's Act on the Protection of Personal Information (2003, effective 2005), Malaysia's Personal Data Protection Act (2010), Vietnam's Law on Information Technology (2006, revised 2013), India’s Information Technology/Reasonable Security Practices and Procedures and Sensitive Personal Data or Information (2011), the Philippines' Data Privacy Act (2012), and Singapore's Personal Data Protection Act (2012). Thailand (1997) and Nepal (2007) have laws that only cover their public sectors. Two other significant jurisdictions, China and Indonesia, have adopted broad data privacy laws that fall short of comprehensive legislation, with limited application to e-commerce and consumer sectors rather than the entire private sector. Whether the region has ten or fourteen data privacy laws, the critical point is that the most economically significant parts of Asia either have or are developing such laws.

The study conducted by Sudarwanto and Kharisma examined personal data protection in Indonesia, specifically in relation to the digital economy sector. The study compared personal data protection in Indonesia, Hong Kong, and Malaysia, focusing on consumer protection and the acceleration of digital economic growth, but before the enactment of Law No. 27 of 2022 on Personal Data Protection (Sudarwanto and Kharisma, 2022).

Cabezas conducted a study on personal data protection regulations by examining similarities, differences, and implications in addressing challenges posed by cybercrime in Spain and Ecuador (Cabezas *et al.*, 2024). Similarly, Prasetyoningsih compared personal data protection regulations in Malaysia and Indonesia. In Malaysia, personal data protection focuses on commercial transactions and the private sector, while in Indonesia, it encompasses both the public and private sectors (Prasetyoningsih *et al.*, 2024). Insights into personal data protection regulations, explored through the applicable laws in Peru and Ecuador, offer valuable guidance for businesses, governments, and individuals navigating the complex terrain of data protection in a rapidly evolving technological

landscape (Alvear *et al.*, 2024). Further research has examined legal sources and the most important aspects of data protection, emphasizing the rights of data subjects, with particular attention to personal and sensitive data (Hornuf *et al.*, 2023).

This article fills a gap not addressed by previous studies, by examining not only the similarities and differences in legislation but also court practices related to this critical issue through the lens of human rights. By comparing the regulatory frameworks for personal data protection in Indonesia, South Korea, and India, this study aims to provide important insights that carry practical implications for policy in Indonesia.

This article offers a general overview of the legal structure surrounding personal data in relation to human rights and the development of relevant jurisprudence in Indonesia. It outlines key characteristics of personal data protection laws and provides a comparative legal analysis between the data privacy regimes in Indonesia, India, and South Korea.

In the following sections, the legal framework and regulations governing personal data protection in Indonesia will be examined, including an overview of key features of Law No. 27 of 2022. Additionally, the enforcement structure of personal data protection laws will be discussed in light of the challenges posed by the implementation of Law No. 27 of 2022. Jurisprudence, particularly related to Constitutional Court decisions, will be analyzed to elucidate the significance of personal data protection within constitutional issues and clarify its meaning in relation to the topic at hand. Based on this discussion, the final section will extend the analysis by drawing implications for comparative law aspects related to personal data protection.

2. Theoretical Overview of the Main Concepts

Personal data Protection and Human Rights

In the digital era, states are not only required to respect and refrain from violating the right to privacy and data protection but also bear positive obligations to take proactive measures to ensure the effective enjoyment of these rights. States must establish systems that safeguard personal data protection rights, ensuring that data subjects are aware of how their personal data is processed, can exercise control over their data, and have access to remedies in cases of violations, including seeking restitution or compensation for damages (Ana Brian, 2024).

Technology alone cannot protect human rights, as it may also infringe on the rights of others who may be adversely affected. For example, blockchain technology can be used to identify persecuted groups such as the Rohingya minority in Myanmar, enabling them to access services in host countries like Bangladesh (Rohingya Project, 2018). It can also facilitate more efficient methods of discriminating against such populations by making them more visible. This risk has been seen in the marginalization of ethnic minorities like the Uyghurs in China, where digital identity systems are not immune to cybersecurity threats (Byler, 2019). Digital technologies, therefore, may aid authorities in persecuting individuals based on their ethnicity (Singer and Friedman, 2014). It is crucial that digital technologies comply with legal requirements for data protection and privacy. States that are party to international human rights treaties must respect, protect, and fulfill the right to privacy, including private life, home, and correspondence (Article 12 UDHR, Article 17 ICCPR) for all individuals within their jurisdiction. State interference with this right is only justified if it is based on domestic law, pursues a legitimate aim, and is necessary and proportionate to that aim (Big Brother Watch v United Kingdom, para 304; Escher v Brazil, para 116).

Article 12 of the 1948 United Nations Declaration of Human Rights (UDHR) recognizes privacy as a fundamental human right (Combe, 2009; Schöpfel, 2016; Zhu et al., 2020). Similarly, Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with privacy, family, home, or correspondence, and grants individuals legal protection against such interference or attacks. The ASEAN Declaration of Human Rights (Article 21) also explicitly recognizes privacy as a human right (Greenleaf, 2012). Personal data is a key aspect of privacy (Al-Abdullah et al.,

2020). Every individual has the right to decide whether or not to disclose their personal information to others (Tsavli et al., 2015; Watson and Lupton, 2020). Therefore, the protection of personal information is synonymous with the protection of privacy (Murray, 2010). The recognition of privacy, including the right to control how one's personal data is used, as a fundamental human right in the UN Declaration and various regional instruments highlights the necessity and importance for all nations to enact comprehensive personal data protection laws.

Values Underpinning Data Protection as a Fundamental Right

2.1 Privacy

Privacy is a fundamental right, and protecting it is one of the key values underlying the right to data protection (Hildebrandt, 2006). Data protection is an extension of the right to privacy, safeguarding an individual's identity and data, particularly when there is a reasonable expectation of privacy, such as with medical information. It also applies to other forms of identifiable data, like addresses or phone numbers. In essence, data protection encompasses the right to be left undisturbed in one's personal life (Lyon, 2014).

2.2 Autonomy

Another critical value protected by the right to data protection is individual autonomy, as seen in the European data protection framework, which emphasizes the centrality of ongoing consent (as outlined in the General Data Protection Regulation or GDPR). The principle of autonomy relates closely to the concept of dignity. For example, German courts have developed the notion of "informational self-determination," linking it to the constitutional right to dignity (McDermott, 2017). The emphasis on consent within data protection aligns with the "will theory" of rights, which views rights as a way of giving individuals control over whether others are obligated to respect those rights (Harris, 1972). The right to remedies, as outlined in Chapter 8 of the GDPR, further supports this view by enhancing the individual's control over their data (Lynskey, 2014).

2.3 Transparency

Transparency is another crucial value in data protection, particularly given the inherent power imbalances related to consent and knowledge (Lynskey, 2014). This notion addresses the forced disclosure of information and the imbalance of power involved in the transfer and use of personal data (Schwartz, 2004). For this reason, De Hert and Gutwirth argue that while privacy can be seen as a tool for obscurity, setting normative boundaries against power, data protection serves as a transparency tool to regulate the use of such power (De Hert and Gutwirth, 2009).

3. Methodology

This article was the result of doctrinal legal research. Data were primarily obtained from literature, as well as relevant primary and secondary legal materials. The research employed a comparative approach and a statutory approach. The comparative approach involved comparing the laws of one country with those of another or comparing the laws of one era with those of a different era. For data related to legal comparisons, international legal documents and publications from scholars in South Korea and India, accessible to the author, were utilized. In this article, South Korea was chosen for comparison due to its rapid digital development and its possession of some of the strictest data protection laws in the world. India was selected because it is one of the most populous countries in the world and holds significant capital in the region. Similar to Indonesia, the legislative experience in both countries is relatively recent, offering an intriguing comparison for further examination.

4. Discussion

3.1 South Korea

South Korea began adopting data protection laws related to the public sector in the 1990s, followed by private sector regulations in 2001, and eventually a comprehensive Personal Information Protection Act (PIPA) in 2011. This act replaced the existing public sector laws and, in the private sector, superseded

previous legislation, except for certain additional privacy obligations on information and communication service providers.

3.1.1 Positioning Data Privacy

PIPA, enacted in 2011, replaced the Public Data Protection Act (1995), which governed public sector data privacy issues. The 2001 Act on the Promotion of Information and Communications Network Utilization and Information Protection regulated privacy in the private sector, particularly in relation to internet activities, and remains in force alongside PIPA.

Under PIPA, data subjects must generally be informed, and their consent obtained, before any personal data can be collected or used. Personal information refers to identifiable details, such as name, resident registration number, and photographs of living individuals. Exceptions to consent requirements exist but are narrowly applied.

PIPA defines personal information and requires consent before collecting such data, aligning with approaches in the European Union and the United States. With consent, cross-border data transfers can occur without regulatory interference. This contrasts with the EU's approach, where regulators are expected to play a more active role, regardless of individual consent.

In enforcing data privacy laws, there are three main remedies in South Korea. First, government authorities can mandate corrective actions and impose administrative fines. Second, criminal penalties may be applicable, as many laws include provisions for violations. Third, victims of data breaches or other affected individuals can file civil lawsuits to seek monetary compensation.

Recent amendments to privacy laws have significantly increased the maximum administrative fines, and it remains to be seen whether these changes will enhance compliance. The Prosecutor's Office and the Police have become more active in enforcement, raising concerns about the growing role of criminal law in data privacy regulation.

3.1.2 Views of the Constitutional Court

The right to privacy is not explicitly stated in the 1987 Constitution of South Korea. However, the Constitutional Court affirmed data privacy as a constitutional right. This was first established in the 2005 case commonly referred to as the "fingerprint case" (Constitutional Court of Korea, 2007). The Court ruled that fingerprints constitute personal information and that collecting and using fingerprint data limits the right to informational self-determination.

In a subsequent 2015 decision, the Constitutional Court reinforced its position that data privacy is a constitutional right. The Court ruled that the national resident registration number system must provide a procedure for citizens to change their registration numbers, thus ensuring the right of individuals to control their own information.

Based on practices in South Korea, data privacy should be regarded as a constitutional right, granting informational self-determination constitutional significance.

However, despite this recognition, South Korea's data privacy laws do not yet provide clear legal standards or predictability for businesses that rely on data collection, processing, and sharing. While such laws may restrict the growth of data-driven industries, they do not necessarily offer stronger protections for individuals' information.

3.2 India

3.2.1 Positioning Data Privacy

During the drafting of the Constitution in the 1940s, the Constituent Assembly discarded the idea of institutionalizing privacy as a fundamental right. Almost seven decades later, in 2017, the significance of the constitutional right to privacy was recognized. The debates within the Constituent Assembly reflected two divergent poles: discussions on the confidentiality of correspondence and protection against

unreasonable searches and seizures (Arun, 2014). These debates indicated that the primary concern in discussing the fundamental right to privacy and/or confidentiality of communication was the potential hindrance to bureaucratic operations concerning India's large population.

India's Parliament enacted its first comprehensive data protection law on August 11, 2023, known as the Digital Personal Data Protection Act (DPDPA). This legislation replaces various existing data protection rules in India and is expected to trigger significant changes regarding personal data processing. However, the law has yet to become operational due to the lack of an effective date and no official timeline for full implementation. The DPDPA serves as a "Umbrella" law, establishing a framework for a new data protection regime, which necessitates the development of implementing rules at a later date. The DPDPA follows principles that are generally similar to those of the General Data Protection Regulation (GDPR) and sets forth regulations for data controllers, data processing, and data subjects. Once established, the Data Protection Board will have the authority to impose corrective or mitigatory actions in the event of personal data breaches.

The DPDPA regulates the processing of digital personal data or data collected in non-digital form that will undergo digitization. Although the definition of personal data aligns with GDPR provisions, this law excludes personal data published by the data principal or by others who have a legal obligation to publish such data. Processing of personal data may occur if there is consent from the data principal or for legitimate uses specified by law. The consent standards outlined in the DPDPA are akin to those of the GDPR, requiring that consent be “freely given, specific, informed, unambiguous, and not conditional.” Unlike the GDPR, the DPDPA does not allow processing based on the legal grounds of contractual necessity or legitimate interests. The DPDPA permits cross-border data transfers outside India's jurisdiction unless otherwise specified by the government, and it does not mandate the implementation of transfer mechanisms.

3.2.2. Views of the Supreme Court

The foundation for the enactment of a single law for personal data protection was established in 2017, following the Supreme Court's decision in the case of KS Puttaswamy v. Union of India (Puttaswamy Judgment). The Supreme Court recognized privacy as an intrinsic right to life and liberty, as stipulated in Article 21 of the Constitution (1950), thus affirming privacy as a fundamental right. The Court addressed the protection that should be afforded to individuals in the private sphere and connected the value of privacy to individual dignity. According to the former President, this established a positive obligation for the state to uphold and preserve individual dignity. The Puttaswamy ruling not only laid the groundwork for prohibiting state actions that infringe on privacy but also mandated the government to regulate private contracts and various private data for the sake of individual privacy.

Previously, in the case of M.P. Sharma and Ors. v. Satish Chandra, District Magistrate, Delhi and Ors. (1954), the Supreme Court first considered the constitutional significance of human rights. At that time, the case involved warrants issued for searches and seizures alleged to have violated the right to privacy. However, the ruling did not categorize privacy as a fundamental right, citing that the authority to conduct searches and seizures was necessary for public interest and was legally inherent to the state.

Furthermore, in the case of Kharak Singh v. State of Uttar Pradesh and Ors. (1962), the Supreme Court determined that nighttime visits to the homes of the accused for surveillance indeed violated Article 21 of the Indian Constitution. Nonetheless, the majority of the judges opined that the Article did not encompass any provisions regarding privacy, thus could not be regarded as a fundamental right.

In the case of Govind v. State of Madhya Pradesh (1974), the Supreme Court ruled that police regulations were incompatible with personal liberty, asserting that the right to privacy is part of human rights; however, its application was deemed case-specific. Later, in the case of Maneka Gandhi v. Union of India (1978), the Supreme Court interpreted Article 21 of the Constitution with a broader understanding, fundamentally including the right to privacy within the right to life.

3.3 Indonesia

3.3.1 Positioning Data Privacy

In its evolution, particularly after the constitutional amendments—UUD 1945, the right to privacy, including personal data protection, has been recognized as a constitutional right of citizens. This aligns with the inclusion of a specific chapter on human rights (bill of rights) in the amended constitution (Chapter XA—Articles 28 A-J). The provisions regarding the guarantee of personal data protection can be found in Article 28G, paragraph (1) of UUD 1945, which states, "Everyone has the right to protection of their personal self, family, honor, dignity, and property under their control, and has the right to feel safe and to be protected from threats and fears to do or not do something that is a human right." . In addition to constitutional protection, Indonesia's involvement as a state party to the International Covenant on Civil and Political Rights (ICCPR), ratified through Law No. 12/2005, emphasizes the government's obligation to protect the privacy and personal data of its citizens. This is also in line with Law No. 39/1999 on Human Rights, which guarantees protection of citizens' privacy rights in several articles, such as Article 14 (2), Article 29 (1), and Article 31.

In general, Article 29, paragraph (1), acknowledges every person's right to the protection of their personal self, family, honor, dignity, and property. This protection encompasses not only direct relationships but also personal information or data. Furthermore, Article 14, paragraph (2) states that one of the rights to self-development includes the right to seek, obtain, store, process, and convey information using any available means. This relates to Article 31 of the Human Rights Law, which guarantees the confidentiality of communication through electronic means, except under the order of a judge or other legitimate authority in accordance with legal provisions. At a more specific level, there are several regulations related to personal data—its protection, collection, processing, and usage. These regulations can be grouped into sectors:

- Telecommunications and Informatics: Law No. 36/1999 on Telecommunications and Law No. 11/2008 on Information and Electronic Transactions.
- Population and Archiving: Law No. 23/2006 on Population and Law No. 43/2009 on Archiving.
- Finance, Banking, and Taxation: Law No. 10/1998 on Banking, Law No. 21/2008 on Islamic Banking, and Law No. 21/2011 on Financial Services Authority.
- Trade and Industry: Law No. 8/1999 on Consumer Protection and Law No. 7/2014 on Trade.
- Health Services: Law No. 29/2004 on Medical Professions, Law No. 44/2009 on Hospitals, Law No. 18/2014 on Mental Health, Law No. 35/2009 on Narcotics, Law No. 38/2014 on Nursing, and Law No. 17/2023 on Health.
- Security and Law Enforcement: This sector includes exceptions for law enforcement/intelligence agencies to record personal communications, access personal data, and access personal accounts (e.g., Law No. 8/1981 on the Code of Criminal Procedure, Law No. 31/1999 on the Eradication of Corruption, Law No. 30/2002 on the Corruption Eradication Commission, Law No. 21/2007 on the Eradication of Human Trafficking, Law No. 8/2010 on the Eradication of Money Laundering, Law No. 17/2011 on State Intelligence, Law No. 18/2011 on the Judicial Commission, Law No. 5/2018 on the Eradication of Terrorism, and Law No. 9/2013 on the Prevention and Eradication of the Crime of Terrorism Financing).

After waiting since 2019, Law No. 27/2022 on Personal Data Protection has been approved. As outlined in its considerations, this law aims to guarantee citizens' rights to personal data protection, raise public awareness, and recognize the importance of personal data. This law is expected to serve as a robust legal umbrella for the governance and protection of citizens' personal data and the administration.

According to Law No. 27/2022, a personal data protection agency will be established; however, the Ministry of Communication and Informatics will temporarily serve as the relevant authority. The application scope applies if the processing has legal consequences in Indonesia or involves data subjects who are Indonesian citizens, even if these individuals are outside Indonesia. Regarding cross-border

transfers, the receiving country must have an equal or higher level of personal data protection than Indonesia or there must be binding personal data protection for the transferred data, or consent has been obtained from the data subjects.

Law No. 27/2022 will take effect in October 2024. However, before its implementation, at least two derivative policies must be prepared. First, regarding the establishment of a personal data protection agency through presidential regulation (Article 58). Second, the formulation of government regulations to follow up on Articles 12-61, which include regulations on (i) mechanisms for filing objections to automated data processing; (ii) violations of personal data processing and procedures for imposing compensation; (iii) the rights of data subjects to utilize their personal data; (iv) the implementation of personal data processing; (v) impact assessments of personal data protection; (vi) notification procedures; (vii) officials or officers performing personal data protection functions; (viii) personal data transfer; (ix) procedures for the imposition of administrative sanctions; and (x) the execution of the powers of the Personal Data Protection Agency.

The personal data protection agency will not only function as a supervisor, auditor, consultant, educator, policy advisor, and negotiator, but it will also have the authority to enforce the law when private or public actors violate the regulations. In general, the agency's authority can be categorized into three groups. First, the authority for regulation and investigation of reports (Article 60 of Law Number 27 of 2022). Second, the authority for oversight and imposition of sanctions (Article 60 letters b, c, h, g, and f of Law Number 27 of 2022). Third, coordination and cooperation. This authority includes assisting law enforcement agencies in handling allegations of personal data offenses, seeking legal assistance from the prosecutor's office in resolving personal data protection disputes, and collaborating with similar agencies in other countries to address alleged cross-border personal data protection violations (Article 60 letters d, o, and e).

3.3.2 Views of the Constitutional Court

In 2003, the Constitutional Court emphasized the growing importance of privacy. In Decision Number 006/PUU-I/2003, in the case of KPKPN vs. KPK, the Court stated that the right to privacy is a right that can be restricted, allowing the State to impose limitations. However, to prevent abuse of power through wiretapping and recording, legislation outlining the procedures for such activities is necessary. Although this case pertains to the application and use of authority by law enforcement agencies using technology and its impact on privacy, it highlights that privacy is becoming increasingly significant as a broader social issue within Indonesian society. Furthermore, in Decision Number 012,016/PUU-IV/2006, the Constitutional Court reaffirmed privacy as a fundamental right within the state. In this decision, it was stated that the right to privacy, based on Article 28F of the Constitution, is not an absolute right and can be restricted according to Article 28J of the Constitution and Article 73 of Law Number 39 of 1999 concerning Human Rights.

Decision Number 5/PUU-VII/2010 confirmed the recognition of the right to privacy in Indonesia in accordance with Article 28G of the 1945 Constitution. This Court ruling is significant regarding the boundaries of privacy in light of internet developments, emphasizing that for Indonesia, this progressive innovation is notable in the region, as countries like Australia and Singapore do not have similar rulings. However, at that time, the Court had not explicitly discussed privacy.

In Decision Number 5/PUU-VIII/2011, it was stated that the right to privacy is part of human rights, encompassing the right to information. Subsequently, in Decision Number 108/PUU-XX/2022, the Constitutional Court provided opinions regarding exceptions to the rights of data subjects in the interests of national defense and security. This was contested partly because the personal data protection law did not provide a clear definition of what constitutes national defense and security interests.

3.4 Relevant Discussion

When analyzing the comparative structure of regulations related to privacy rights among South Korea, India, and Indonesia, a consistent uniformity emerges, particularly encompassing: (i) obligations in the collection/handling/transportation of data; (ii) the rights of data subjects to inquire about and modify their data; (iii) cross-border obligations; (iv) requirements for breach notification; and (v) penalties.

Additionally, the regulations in all three countries cover data from both the public and private sectors. In South Korea, the supervisory authority is the Personal Information Protection Commission, while in India, it is the Data Protection Board. In Indonesia, the Data Protection Authority is yet to be established, with temporary authority residing with the Ministry of Communication and Information. In South Korea and India, there are no restrictions regarding sensitive personal data. Conversely, Indonesia imposes restrictions that include health data, biometric data, genetic data, sexual orientation/life data, political views, criminal records, data pertaining to minors, and personal financial data. In South Korea, violations of personal data are subject to fines, whereas in India, specific violations may incur penalties depending on the nature of the case. In Indonesia, the established fines can reach up to two percent of annual revenue.

Judicial practices in all three countries demonstrate a significant focus on the contextualization of human rights. Jurisprudence evolves in response to the dynamics of cases through court interpretations, given that privacy is not explicitly enshrined in the constitutions. The judicial practices across these countries reflect the relationship between privacy rights and data protection.

The research indicates that data protection regulations in South Korea were institutionalized in 2011, while Indonesia and India established theirs in 2022 and 2023, respectively. In both of the latter countries, it appears that the regulations related to data protection are still awaiting effectiveness due to the need for follow-up actions regarding the establishment of delegated regulations and the formation of data protection supervisory authorities. Thus, both Indonesia and India seem to still be evolving regulations related to personal data, which are dispersed across various legislative frameworks. South Korea, India, and Indonesia share similar legal motivations for personal data protection, particularly in facing the advancements of digital information and the unification of related regimes. The comparative regulations among these three countries also indicate the functionalization of criminal fines. All three countries are striving to integrate global norms pertaining to personal data protection.

5. Conclusion

Data protection is an integral part of human rights, further interpreted from the provisions of constitutional rights enshrined in the Constitution and manifested in relevant court decisions. The comparative analysis of data obtained from South Korea, India, and Indonesia reveals a common legal motivation and a desire to integrate regimes influenced by global standards. The legal structure in Indonesia regarding data protection differs from those in South Korea and India, particularly concerning the definition of sensitive data. However, there are similarities in relation to: (i) obligations regarding the collection/handling/transportation of data; (ii) the rights of data subjects to inquire about and modify their data; (iii) cross-border obligations; (iv) requirements for breach notification; and (v) penalties.

For Indonesia, similar to India, there are challenges regarding the establishment of a supervisory authority related to data protection. As seen in South Korea, such authorities should not only be independent but also ensure proportional representation in their composition and membership. These authorities must perform administrative functions while also having dispute resolution capabilities akin to those in the judicial system.

References

[1] Adri, A. (2024), “Keamanan Siber Lemah Indonesia Jadi Pasar Besar Judi Daring”, 13 June.

[2] Al-Abdullah, M., Alsmadi, I., AlAbdullah, R. and Farkas, B. (2020), “Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR”, Digital Policy, Regulation and Governance, Vol. 22 No. 5/6, pp. 389–411, doi: 10.1108/DPRG-04-2020-0050.

[3] Alvear, G., Hernández, E. and Arcos-Argudo, M. (2024), “Insights into Personal Data Protection Legislation: Peru and Ecuador Compared”, in Alareeni, B. and Hamdan, A. (Eds.), Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation, Vol. 1082, Springer Nature Switzerland, Cham, pp. 473–482, doi: 10.1007/978-3-031-67434-1_45.

[4] Ana Brian, N. (2024), “Individuals must be able to realise right to remedy for privacy violations in

data protection: UN Expert", United Nations Human Rights, 3 December, available at: https://www.ohchr.org/en/press-releases/2024/03/individuals-must-be-able-realise-right-remedy-privacy-violations-data.

[5] Anam, M.K. (n.d.). "Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember Fakultas Syariah April 2024".

[6] Arun, C. (2014), "Paper-Thin Safeguards and Mass Surveillance in India", National Law School of India Review, Student Advocate Committee, Vol. 26 No. 2, pp. 105–114.

[7] Beduschi, A. (2019), "Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights", Big Data & Society, Vol. 6 No. 2, p. 205395171985509, doi: 10.1177/2053951719855091.

[8] Byler, D. (2019), "China's hi-tech war on its Muslim minority", The Guardian.

[9] Cabezas, D., Lucas, G., Arcos-Argudo, M., Bojorque, R., Plaza-Cordero, A. and Morquecho-Yunga, P. (2024), "Comparative Analysis of Data Protection Laws in Ecuador and Spain: Similarities, Differences, and Implications", in Yang, X.-S., Sherratt, S., Dey, N. and Joshi, A. (Eds.), Proceedings of Ninth International Congress on Information and Communication Technology, Vol. 1004, Springer Nature Singapore, Singapore, pp. 385–393, doi: 10.1007/978-981-97-3305-7_32.

[10] Combe, C. (2009), "Observations on the UK transformational government strategy relative to citizen data sharing and privacy", Transforming Government: People, Process and Policy, Vol. 3 No. 4, pp. 394–405, doi: 10.1108/17506160910997892.

[11] Constitutional Court of Korea. (2007), Decisions of The Korean Constitutional Court (2005), Constitutional Courts Korea, Korea.

[12] De Hert, P. and Gutwirth, S. (2009), "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", in Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. and Nouwt, S. (Eds.), Reinventing Data Protection?, Springer Netherlands, Dordrecht, pp. 3–44, doi: 10.1007/978-1-4020-9498-9_1.

[13] Greenleaf, G. (2012), "Global Data Privacy Laws: 89 Countries, and Accelerating", SSRN Scholarly Paper, Rochester, NY, 6 February.

[14] Greenleaf, G. (2013), "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories", SSRN Electronic Journal, doi: 10.2139/ssrn.2280877.

[15] Haksoo, K., John, L., Eunsoo, K. and Jong Gu, J. (2016), "structure and enforcement of data privacy law in south korea", Brussels Privacy Hub Working Paper, Brussels Privacy Hub Working Paper, Brussels.

[16] Harris, N.G.E. (1972), "Hart on Natural Rights", British Journal of Political Science, Vol. 2 No. 1, pp. 125–127, doi: 10.1017/S0007123400008486.

[17] Hildebrandt, M. (2006), "Privacy and Identity", in Claes, E., Duff, A. and Gutwirth, S. (Eds.), Privacy and the Criminal Law, Intersentia, Antwerp.

[18] Hornuf, L., Mangold, S. and Yang, Y. (2023), "Data Protection Law in Germany, the United States, and China", Data Privacy and Crowdsourcing, Springer Nature Switzerland, Cham, pp. 19–79, doi: 10.1007/978-3-031-32064-4_3.

[19] Lynskey, O. (2014), "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in The EU Legal Order", International and Comparative Law Quarterly, Vol. 63 No. 3, pp. 569–597, doi: 10.1017/S0020589314000244.

[20] Lyon, D. (2014), "Surveillance, Snowden, and Big Data: Capacities, consequences, critique", Big Data & Society, Vol. 1 No. 2, p. 205395171454186, doi: 10.1177/2053951714541861.

[21] Makulilo, A.B. (Ed.). (2016), African Data Privacy Laws, Springer Verlag, Cham.

[22] McDermott, Y. (2017), "Conceptualising the right to data protection in an era of Big Data", Big Data

& Society, Vol. 4 No. 1, p. 205395171668699, doi: 10.1177/2053951716686994.

[23] Murray, A. (2010), Information Technology Law: The Law and Society, Oxford Univ. Press, Oxford.

[24] Piasecki, S. and Chen, J. (2022), "Complying with the GDPR when vulnerable people use smart devices", International Data Privacy Law, Vol. 12 No. 2, pp. 113–131, doi: 10.1093/idpl/ipac001.

[25] Prasetyoningsih, N., Ismail Nawang, N., Putri, W.V. and Amirullah, M.N.R. (2024), "Legal Protection for the Personal Data in Indonesia and Malaysia", in Moallem, A. (Ed.), HCI for Cybersecurity, Privacy and Trust, Vol. 14728, Springer Nature Switzerland, Cham, pp. 161–169, doi: 10.1007/978-3-031-61379-1_11.

[26] Prinsloo, P. and Kaliisa, R. (2022), "Data privacy on the African continent: Opportunities, challenges and implications for learning analytics", British Journal of Educational Technology, Vol. 53 No. 4, pp. 894–913, doi: 10.1111/bjet.13226.

[27] Rohingya Project. (2018), "A Rohingya Initiative", available at: https://rohingyaproject.com/.

[28] Schöpfel, J. (2016), "Open Access, Privacy, and Human Rights: A Case Study on Ethics in Library and Information Sciences Education", in Gorham, U., Taylor, N.G. and Jaeger, P.T. (Eds.), Advances in Librarianship, Vol. 41, Emerald Group Publishing Limited., pp. 349–371, doi: 10.1108/S0065-283020160000041015.

[29] Schwartz, P.M. (2004), "Property, Privacy, and Personal Data", Harvard Law Review, Vol. 117 No. 7, p. 2056, doi: 10.2307/4093335.

[30] Singer, P.W. and Friedman, A. (2014), Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford Univ. Press, Oxford.

[31] Srivastava, R. (2021), "Reconciling Extraterritorial Surveillance", Vol. 54.

[32] Sudarwanto, A.S. and Kharisma, D.B.B. (2022), "Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia", Journal of Financial Crime, Vol. 29 No. 4, pp. 1443–1457, doi: 10.1108/JFC-09-2021-0193.

[33] Surfshark. (2024), "Data breach statistics globally", Surfshark, 15 July, available at: https://surfshark.com/research/data-breach-monitoring (accessed 9 September 2024).

[34] Tsavli, M., Efraimidis, P.S., Katos, V. and Mitrou, L. (2015), "Reengineering the user: privacy concerns about personal data on smartphones", Information & Computer Security, Vol. 23 No. 4, pp. 394–405, doi: 10.1108/ICS-10-2014-0071.

[35] Ukwueze, F. (2021), "Strengthening the Legal Framework for Personal Data Protection in Nigeria", The Nigerian Juridical Review, Vol. 16, pp. 124–142, doi: 10.56284/tnjr.v16i1.16.

[36] Waldman, A.E. (2020), "Data Protection by Design? A Critique of Article 25 of the GDPR", Vol. 53.

[37] Wambiri, D., Masinde, J. and Mugambi, F. (2023), "Big Data and Personal Information Privacy in Developing Countries: A Case of Kenya", 21 February, doi: 10.21203/rs.3.rs-2604181/v1.

[38] Watson, A. and Lupton, D. (2020), "Tactics, affects and agencies in digital privacy narratives: a story completion study", Online Information Review, Vol. 45 No. 1, pp. 138–156, doi: 10.1108/OIR-05-2020-0174.

[39] Zhu, R., Srivastava, A. and Sutanto, J. (2020), "Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective", Information Technology & People, Vol. 33 No. 6, pp. 1601–1626, doi: 10.1108/ITP-03-2019-0117.