PERSONAL DATA PROTECTION IN PRIVATE SECTOR ELECTRONIC SYSTEMS FOR BUSINESSES: INDONESIA VS. SOUTH KOREA

Ninne Zahara Silviani
Faculty of Law, Universitas Internasional Batam, Indonesia,
ninne@uib.ac.id

Rina Shahriyani Shahrullah
Faculty of Law, Universitas Internasional Batam, Indonesia,
rina@uib.ac.id

Vanessa Riarta Atmaja
Faculty of Law, Universitas Internasional Batam, Indonesia,
2051065.vanessa@uib.edu

Park Ji Hyun
Faculty of Law, Youngsan University, South Korea
shabd@ysu.ac.kr

Abstract

This paper explores the various practices surrounding the legal framework for protecting personal data in the context of private electronic systems used by commercial companies. The research's main focus is the ambiguity of the goals of Indonesia's Electronic System providers and how they may adopt better practices to enhance data protection within Electronic System Providers, so this extensive examination also includes a thorough comparison of the personal data protection laws in South Korea and Indonesia. This investigation aims to carefully define, evaluate, and harmonize the two countries' unique legal systems. This study uses a normative legal research framework with a Teleological and Legal Protection approach as its research technique. Additionally, it uses the comparative law method to clarify, outline, and examine the specifics of the personal data protection laws that are now in force in Indonesia and South Korea. The results of this research go beyond identifying problems; they are expected to

produce a thorough understanding of the complexities surrounding personal data security in the context of electronic commerce. These discoveries are well-positioned to be the foundation for upcoming regulatory improvements, eventually encouraging more potent and reliable data protection procedures in both nations.

Keywords: Electronic System Providers, Personal Data Protection, Business Entities

Introduction

The Fourth Industrial Revolution has pushed Indonesia's data advances toward being more thorough. The public and private sectors have started to understand and learn that big data may be treated like physical assets. Big Data refers to this revolution in data management.[1] Big Data is frequently regarded as a component of technological advancement. However, due to its ambiguous description, there isn't a clear definition as of now.

Big data plays a huge role in electronic commerce (e-commerce), the increasingly sophisticated business process that connects vendors and buyers via the Internet. E-commerce has grown significantly in recent years and reshaped the global retail industry.[2] E-commerce is a contemporary non-physical trading paradigm that does not call for original signatures or the physical presence of the trading partners.[3] E-commerce, as defined by Niniek Suparni, is any commercial activity involving customers, suppliers, manufacturers, middlemen, and service providers.[4] Due to law enforcement's incompetence in handling these instances, the law fails to protect consumers fully. The existence of electronic trading procedures has given rise to several empirical challenges society faces, such as online fraud and hacking.

---

[1] Piyush Malik, 'Governing Big Data: Principles and Practices', *IBM Journal of Research and Development*, 57.3/4 (2013), 1.

[2] Prakash Rao and others, 'The E-Commerce Supply Chain and Environmental Sustainability: An Empirical Investigation on the Online Retail Sector,' *Cogent Business & Management*, 8.1 (2021), 1938377.

[3] Margaretha Rosa Anjani and Budi Santoso, 'Urgensi Rekonstruksi Hukum E-Commerce Di Indonesia', *Law Reform*, 14.1 (2018), 89–103.

[4] Suparni Niniek, 'Cyberspace Problematika & Antisipasi Pengaturannya', *Sinar Grafika, Jakarta*, 2009.

There are critical distinctions between providers of Electronic Systems in the Public Scope and the Private Scope, according to Government Regulation Number 71 of 2019 (Next mentioned as PP No.71 of 2019). Providers of Electronic Systems in the Public Scope are organizations or institutions that administer electronic systems on behalf of state agencies. The administration of electronic systems by people, businesses, and the general public is included in the Private Scope Providers of Electronic Systems. The primary distinction thus rests in the organizations in charge of administration; one is linked to governmental agencies or their appointees, while the other involves people, businesses, and a wider swath of society. [5]

PP No.71 of 2019 mandates companies in the digital and e-commerce space, also known as Providers of Electronic Systems in the Private Scope, to register by submitting their full names and contact information. The Ministry of Trade will compile all legitimate identity numbers due to this registration and make them accessible to the public. This initiative encourages commercial enterprises to sign up for the registration program in compliance with the laws governing *Penyelenggara Sistem Elektronik* (Electronic System Providers next: PSEs). [6]

The first stage in the registration process for a business permit is to create a Business Identification Number (NIB). Users are expected to supply personal identity information as part of the registration criteria during this process. This personally identifiable information form must be filled out entirely for the registration process to move forward; therefore, getting it right is essential. Simply put, the completion of submitting personal identity information during the initial stage, which is the construction of the NIB, strongly influences the success of obtaining a business permit.[7]

---

[5] Pemerintah RI, "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik," *Pemerintah RI*, 2019, https://jdih.kemenkeu.go.id/FullText/2019/71TAHUN2019PP.pdf.

[6] Mohamad Rivaldi Moha, Sukarmi Sukarmi, and Afifah Kusumadara, 'Urgensi Pendaftaran Penyelenggara Sistem Elektronik Bagi Pelaku Usaha E-Commerce', *Jambura Law Review*, 2.2 (2020), 101–19.

[7] Deky Pariadi, 'Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen', *Jurnal Hukum & Pembangunan*, 48.3 (2018), 651–69.

The main objective of the management of Electronic Systems and Transactions (PSE) is to thoroughly regulate the use of information technology and electronic transactions to support the development of the digital economy and ensure the state's sovereignty over electronic data on the territory of the Unitary State of the Republic of Indonesia.[8] However, these goals are not specified in the regulation cited in the quote. Due to the possibility of different interpretations and confusion regarding the subjects covered by the rule, a lack of clarity in the aims and functions might generate problems.

The vagueness of the PSE goals has serious repercussions. First, this lack of clarity makes it difficult for providers of electronic systems and transactions to accurately focus their commercial efforts on complying with legislation. Businesses also find it difficult to select projects that should help long-term digital economic growth without a clear knowledge of the objectives.[9] Furthermore, this lack of transparency may have detrimental effects on other stakeholders like investors, business owners, and the general public. If the regulatory goals are poorly defined, investments in technology and electronic transaction ecosystems may become cautious. This problem may hamper the anticipated expansion of the digital economy. Businesses that fail to register their electronic systems may also be subject to fines from the government, particularly the Ministry of Communication and Information Technology (KOMINFO). Therefore, PP No. 71 of 2019's goals must be reviewed and clarified.

There are other worries and challenges with the safety of personal data, in addition to the unclear goals in deploying the Electronic System and Transaction (PSE). Data entry that includes sensitive and personal information is required to register electronic systems under PSE. It includes personal information, information about corporate entities, and other vital details. Business owners are concerned about potential risks when this data must be shared with the government to comply with legislation. There are concerns regarding the

[8] Eric Jingga, 'Pelindungan Hak Ekonomi Pemilik Akun PSE Lingkup Privat Dari Pemblokiran Akibat Belum Terdaftar Di Indonesia', *COMSERVA: Jurnal Penelitian Dan Pengabdian Masyarakat*, 3.03 (2023), 849–61.

[9] Nathania Salsabila Marikar Sahib, Soesi Idayanti, and Kanti Rahayu, 'Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia', *Pancasakti Law Journal (PLJ)*, 1.1 (2023), 61–74.

government's ability to appropriately protect sensitive personal data due to prior data security problems.[10] The uncertainty around the government's steps to mitigate data breaches exacerbates these worries.[11] Although Indonesia has seen several instances of cybercrime, the processing and investigation of these cases can run into legal and technical hurdles, which ultimately undermine public confidence in the government's capacity to solve cyber security issues.[12]

Business owners know that personal data protection's unpredictability can negatively affect their reputation and brand image. Significant financial losses and a deterioration in customer relations can result from losing sensitive data.[13] They are thus faced with a conundrum due to these fears: on the one hand, PSE registration is necessary to comply with laws and benefit from a well-regulated digital environment, but on the other, the danger to personal data protection can lead to considerably bigger losses.

The government is vital in safeguarding the public interest. It is necessary to prevent numerous disruptions caused by the improper use of electronic information and electronic transactions that disturb public order.[14] The relevant regulations are contained in Article 94 of PP No. 71 of 2019 regarding implementing Electronic Systems and Electronic Transactions (PSE). [15]

---

[10] Ranita Gustisia Janis, Elko Lucky Mamesah, and Debby Telly Antow, 'Aspek Pidana Dalam Penipuan Online Dengan Modus Investasi', *LEX PRIVATUM*, 11.4 (2023).

[11] Hezkiel Bram Setiawan and Fatma Ulfatun Najicha, 'Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data', *Jurnal Kewarganegaraan*, 6.1 (2022), 976–82.

[12] Khafidah Puspita, 'Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia', *Jurisprudensi: Jurnal Ilmu Syariah, Perundangan-Undangan Dan Ekonomi Islam*, 15.1 (2023), 67–83.

[13] Dewi Rizka Yuniarti and others, 'Analisis Potensi Dan Strategi Pencegahan Cyber Crim Dalam Sistem Logistik di Era Digital', *Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN)*, 3.1 (2023), 23–32.

[14] Gian Wiatma Jonimandala, "Peran Direktorat Tindak Pidana Siber (DITTIPIDSIBER) Bareskim Polri Dalam Melakukan Penegakan Hukum Terhadap Kejahatan Pencurian Dan Penyalahgunaan Data Pribadi" 3 (2023): 680–92.

[15] Pemerintah RI, "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik."

In this sense, Indonesia is not the only nation responsible for safeguarding its inhabitants' personal information. Many countries have decided to enact laws and regulations controlling personal data protection to preserve people's privacy and data security.[16] In this regard, two nations that have demonstrated a considerable concern for the security of personal data are South Korea and Indonesia. Large populations and growing reliance on digital technology can be found in both South Korea and Indonesia. Both nations have established regulatory frameworks to govern personal data protection and address these new issues with privacy and data security. It is urgent to gain insight from this comparison to obtain a better way to data protection law in Indonesia, as South Korea is a country that has developed data protection law way before Indonesia and is facing a lot of cases regarding data privacy and data protection.

Earlier research has covered the regulation of electronic system providers (PSE) in Indonesia in several papers. One of the earliest studies looked at various PSE regulation-related topics, particularly from a legal standpoint and how it affected the digital business environment. The main emphasis in PSE regulation has been on technical rules and business operators' obligations linked to the provision of electronic systems.[17] In this study, the author will delve further into the PSE's regulatory challenges, emphasizing the privacy concerns of company operators as they relate to the protection of personal data. The purpose of this essay is to clarify the arguments made in the discussion of PSE regulation and to identify the innovations produced by this study. As a result, the author divides the issues and debates surrounding the Electronic System Provider into three categories. First, there needs to be more clarity over the main goals, which leaves business owners and providers of electronic systems without thorough rules for managing their operations. In the contemporary digital era, personal data privacy has also emerged as a critical concern, with difficulties arising from Indonesia's lack of comprehensive rules. Therefore, thorough research is required to

[16] Nadiah Tsamara, 'Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara', *Jurnal Suara Hukum*, 3.1 (2021), 53–84.

[17] Sahib, Idayanti, and Rahayu.

pinpoint the goals that PSE should support and create a robust regulatory framework.[18]

The final problem formulation compares Indonesia's and South Korea's data protection laws, which is important for analyzing the differences and similarities in regulatory approaches to protecting business entities' data privacy and institutional practices.

Method of Research

This study comprehends normative legal research with a ccomparative approach. Data and regulation were utilized in this study to compare and contrast the laws between South Korea and Indonesia and to explain and define their respective legal systems. The term "comparative law" or "comparative legal studies" refers to a method for contrasting the legal systems of two different nations.[19] This research intends to provide a deeper knowledge of the legal principles present in these regulations and suggest remedies based on teleological and legal protection approaches to protecting personal data.[20]

Results and Discussion

a. The objective of Electronic System Provider Registration

The Electronic System Provider (PSE) has become the subject of increasing attention in the digital transformation era. Information technology's development has significantly impacted various aspects of life, including in the realm of business and the economy. In Indonesia, this is reflected in the Minister of Communication and Informatics Regulation Number 5 of 2020 concerning Electronic System Providers within the Scope of Private Entities and PP Number 71 of 2019 concerning Electronic System and Transaction Implementation. Although the main objectives of these regulations are

[18] Sinta Dewi Rosadi and Garry Gumelar Pratama, 'Urgensi Perlindungandata Privasi dalam Era Ekonomi Digital Di Indonesia', *Veritas et Justitia*, 4.1 (2018), 88–110.

[19] Iii, B., Penelitian, M., & Penelitian, A. (n.d.). Retrieved from http://e-journal.uajy.ac.id/11868/4/MIH022543.pdf

[20] Muhaimin Muhaimin, 'Metode Penelitian Hukum', *Dalam S. Dr. Muhaimin, Metode Penelitian Hukum, Mataram-NTB: Mataram*, 2020.

implicitly reflected, former Minister of Communication and Informatics Johnny G Plate has verbally conveyed these objectives. However, the lack of concrete explanations in these regulations has caused confusion among business actors regarding the true purpose and meaning of the PSE registration activities.

The government must create a framework that considers the contemporary digital era, in which technology-based services and electronic transactions have saturated society's networks. The regulations governing Electronic System Providers (PSE) have unstated but implicit goals that point to a broader regulatory direction: building an innovative, safe, and trustworthy commercial ecosystem for electronic systems.[21] Although these goals are not stated clearly in the regulatory text, former Minister Johnny G. Plate's acknowledgment suggests that setting up a legal framework that can keep up with technological advancements is essential.

Indeed, corporate stakeholders are confused by the ambiguity surrounding the PSE's aims. They have difficulty fully comprehending what the government intends for these regulations to achieve. Fundamental inquiries are raised: Is PSE registration just for legal compliance, or does it also have more in-depth implications for user privacy and data security? Without clear direction, businesses struggle to develop the best plans for incorporating PSE into their operations.

The Teleological Interpretation Theory is one of the legal theories that can be applied to assess this problem when dealing with the ambiguity of intentions in a government regulation or activity. This theory, which has intellectual roots in Aristotle, is now a widely used method in the legal profession for comprehending and interpreting rules. According to this idea, an action's goodness or badness depends on the outcome it produces. According to this viewpoint, a good action does not have good intentions but does not result in anything of value. In other words, the teleological approach emphasizes a rule

[21] Rosadi and Pratama.

or policy's ultimate goal or desired result and aims to comprehend the motivations that led to their formulation entirely.[22]

The teleological method can offer helpful direction when the goals of laws or other initiatives, like Minister of Communication and Informatics Regulation Number 5 of 2020 respecting Electronic System Providers within the Scope of Private Entities, are unclear. This strategy draws attention to the general objectives that drive the government's adoption of this regulation, even though the precise objectives are not expressly stated in the regulation's wording. In this situation, the overarching goals cover matters like consumer protection, sustainable economic growth, and the creation of a reliable digital business ecosystem.

Analyzing the social, economic, and political context in which the regulation is produced is crucial when applying the teleological approach. We can get closer to understanding the underlying goals that the government seeks to accomplish by comprehending the difficulties and opportunities that society is facing in the digital age. Johnny G. Plate, a previous minister of communication and informatics, publicly expressed these goals in his statements, which have become essential sources for illuminating the government's intentions about addressing digital transformation.

The teleological approach enables us to see PSE regulation as a means of achieving more comprehensive goals. First, the goal of secure electronic transactions takes precedence. The digital world introduces new dangers, including data theft and cyber attacks, which can erode customer confidence in online purchases. The government wants to ensure that electronic system providers utilize appropriate security procedures to safeguard user data and sensitive information, which is why it requires PSE registration.[23]

Furthermore, achieving sustainable economic growth also plays a significant role. The government may want to foster an environment

---

[22] E Fernando M Manullang, 'Penafsiran Teleologis/Sosiologis, Penafsiran Purposive Dan Aharon Barak: Suatu Refleksi Kritis', *Veritas et Justitia*, 5.2 (2019), 262–85.

[23] Rifka Pratiwi Ardikha Putri and Neni Ruhaeni, 'Kewajiban Mendaftarkan E-Commerce Dalam Sistem Elektronik Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik Dan Implementasinya Terhadap E-Commerce Informal', in *Bandung Conference Series: Law Studies*, 2022, II, 47–54.

that will attract investment in the digital sector by encouraging enterprises to participate in a regulated system. This may result in more jobs being created, higher tax revenues for the government, and general economic empowerment.

The creation of a reliable and creative digital business ecosystem also seems like it could be a goal. The government can create an atmosphere where companies feel secure in innovating and exploring new opportunities in the digital realm by regulating and supervising electronic system providers. Additionally, this raises consumer confidence in electronic services and transactions.

It's critical to realize that these goals do not compete with one another in teleological interpretation. They can converse and support one another. This method also recognizes that over time, changing situations and new issues may have an impact on how the law is interpreted. Legal interpreters must, therefore, keep up with changes in the social, economic, and technical environment when using the teleological approach.

Finally, for addressing the ambiguity of purposes in a legal environment, the Teleological Interpretation Theory, which emphasizes the ultimate goal of a rule, is a suitable option. This method aids in identifying the latent goals of PSE rules, such as transaction security, economic growth, and the development of the digital business environment. Understanding these goals will help ensure that the interpretation and application of the regulations are more accurate and in line with societal and governmental expectations.

Beyond the previously indicated ambiguity, other interpretations might be drawn from a broader context. First, PSE's establishment might be viewed as an effort to reduce the risks associated with electronic transactions. The safety of financial and personal data becomes essential in a digital ecosystem that is susceptible to cyberattacks and data theft. The government may guarantee that the relevant electronic system providers have complied with the necessary security standards by requiring PSE registration.[24]

The PSE's covert goals can also be connected to initiatives to promote inclusive digital economic growth. The government may want to foster an environment that will attract investment in the digital

[24] Putri and Ruhaeni, II.

sector by encouraging enterprises to participate in a regulated system. In the long term, this may affect job creation, raise tax revenue for the government, and strengthen the economy as a whole.

Another possible interpretation of PSE's goals is that they involve enhancing the reliability and trust of electronic transactions. If government-supervised processes are in place, consumers can feel confident that their transactions will be performed according to reasonable and fair standards. Regulations pertaining to consumer protection, conflict resolution, and operational openness may fall under this category.

Although businesses may initially struggle to understand PSE's goals, they can turn to the guiding principles that guide these rules. The main goals the government hopes to accomplish through PSE are probably security, economic growth, transaction integrity, and technology empowerment. It is imperative that the government address this uncertainty by offering businesses more precise explanations and thorough guidelines. By doing so, PSE implementation will run more easily and accomplish the strong yet unstated goals outlined in governmental regulations and directives.

b. National Policies for Personal Data Protection of Private Electronic System Providers in Indonesia and South Korea

The government is the accountable authority for protecting human rights, including the right to data privacy. The preservation, promotion, enforcement, and fulfillment of human rights are specifically stated as being the state's obligation in Article 28I, paragraph 4 of the 1945 Indonesian Constitution. Furthermore, the government itself is the main target of this responsibility. Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law) is one of the key legal bases for this. However, by passing Law No. 27 of 2022 on Personal Data Protection, Indonesia has gone a step further in acknowledging the need for more thorough data protection that keeps up with technological changes. However, the complexity of the digital environment has made it urgently necessary to recognize the need for more precise legislation for comprehensive personal data protection, focusing on privacy considerations.

Indonesia created and passed Law No. 27 of 2022 on Personal Data Protection to address this.[25]

In addition, the protection of personal data is cited as one of the human rights that includes preserving personal identity, as governed by Article 28G paragraph (1) of the 1945 Indonesian Constitution, in the considerations of the Draft Personal Data Protection Bill (RUU PDP) version of January 2020. In short, the state has a duty to defend its residents, particularly by defending citizens' rights to their personal information.[26] In fact, there is a glaring vacuum in Indonesia's rules regarding the government's responsibility towards electronic system providers (PSEs) when it comes to personal data protection. Several laws have been passed to protect personal information in the electronic sphere. Still, they often emphasize the duties and obligations of businesses more than defining precisely how the government will hold PSEs formally accountable for their deeds.[27]

The public's and businesses' skepticism and worries are based on earlier instances of personal data breaches in Indonesia. The Covid-19 digital vaccination certificate data breach is one of these instances, which highlights major problems with the protection of personal data and the government's obligation to protect the data of its residents. This case has raised several issues on how the government should handle data breaches and how data protection should be enforced.[28]

[25] Adhigar *Di Ruang Siber: Studi Tenta* 1).

[26] Rahman a Pribadi Masyarakat," 2021, https://www.kc itah-dalam-melindun

[27] Ditam -Undang Perlindungan Data Pribadi, *Ditama Binbangkum - BPK RI*, no. 016999 (2022): 1–50, https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022.

[28] Hendro Wijayanto, Daryono Daryono, and Siti Nasiroh, 'Analisis Forensik Pada Aplikasi Peduli Lindungi Terhadap Kebocoran Data Pribadi', *Jurnal Teknologi Informasi Dan Komunikasi (TIKomSiN)*, 9.2 (2021), 11–18.

Jurnal Hukum dan Peradilan Vol. 12 No. 3 (2023), 517-546
ISSN: 2303-3274 (p), 2528-1100 (e)
DOI: https://doi.org/10.25216/jhp.12.3.2023.517-546


KEAMANAN SIBER

Kebocoran Data Pribadi Jadi Atensi Presiden Jokowi

Presiden menggelar rapat tertutup membahas keamanan data dari serangan siber. Masyarakat sipil mendorong audit berkala dan penerapan standar pengamanan data.

Audio Berita 7 menit

Oleh Tim Kompas
13 September 2022 05:55 WIB · 5 menit baca

A TEKS

Figure 1: Leakage of President's Personal Data News'

A severe occurrence that has affected public confidence in the government's handling of personal data is the release of digital Covid-19 vaccination certificate data, followed by irresponsible parties' exploitation of it. The government, however, needs to be more active in taking accountability for lax regulations, insufficient security measures, or simply a lack of monitoring of prospective data security concerns. [29]

Indonesia has also witnessed a severe event linked to the disclosure of BPJS Ketenagakerjaan (Social Security Agency for Manpower) data, which was brought on by a hacker named Bjorka. This is in addition to the Covid-19 vaccine data breach. As a result of this incident, the public and businesses now have even more reservations about Indonesia's data privacy laws.[30]

[29] Wijayanto, Daryono, and Nasiroh.

[30] Fadhi Khoiru Nasrudin and Rosalinda Elsina Latumahina, 'Perlindungan Hukum Terhadap Konsumen Kartu Sim Yang Mengalami Kebocoran Data Akibat

Figure 2: Data Leak Case News by Bjorka from Kompas

These incidents ultimately expose flaws in the security measures the government puts in place to safeguard the personal information of its constituents. The Bjorka case also highlights important issues regarding how the government should handle these kinds of data breaches. The government handles events that have already happened, protects potential victims of data exploitation, and prevents data leaks in this situation.[31]

Businesses and investors will feel confident registering their electronic systems with the Ministry of Communication and Information Technology (KOMINFO) if there are clear-cut processes to ensure government accountability for Electronic System Providers (PSEs). It will significantly improve the environment for digital businesses in Indonesia. A more stable and favorable investment environment for PSEs can be produced by increased legal certainty and belief in the government's sincere commitment to protecting personal data. When companies are confident and secure in their position, several positive effects may start to manifest.

When comparing the legal frameworks in Indonesia and South Korea concerning the responsibility of Electronic System Providers (PSE), a significant variation in the regulatory environment becomes

Peretasan', *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 2.1 (2022), 331–43.

[31] Wijayanto, Daryono, and Nasiroh.

apparent. Although Article 31 of the Personal Information Protection Act (PIPA) in South Korea clearly stipulates the requirement for a designated privacy officer, Indonesia still needs a comprehensive legislative framework that is unique to Electronic System Providers.

As a comparison in this study, South Korea's legal system has given substantial consideration to personal data protection. The fundamental framework for governing personal data protection in the nation is the Personal Information Protection Act, which became effective in 2011. This law provides vital guidelines to be followed while gathering and using personal data, including necessity, openness, and lawfulness. The Personal Information Protection Commission (PIPC), which regulates and enforces personal data protection, is also present in South Korea. The PIPC is crucial in overseeing how the law is being applied, offering direction, and enforcing penalties for infractions. It reflects the South Korean government's dedication to protecting the confidentiality and security of its inhabitants' personal information.

South Korea's privacy protection legislation has been established since the early 1990s. Korea, as an Organization for Economic Cooperation and Development (OECD) member since 1996, initially only legislated in relation to the public sector, like some other OECD members such as Australia, Canada, and Japan.[32] South Korea has passed additional legislation pertaining to the protection of personal data in particular situations, such as the telecommunications and banking sectors, in addition to the Personal Information Protection Act (PIPA), which was first established in 2020 and last amended in 2023. [33] It exemplifies South Korea's all-encompassing strategy for tackling data protection problems in various industries.

The Personal Information Protection Commission (PIPC), which oversees and enforces personal data protection legislation in South Korea, is particularly important for the e-commerce industry. As an independent body, the PIPC oversees procedures connected to gathering, handling, and using personal data in various industries,

[32] Graham Greenleaf and Whon-il Park, 'South Korea's Innovations in Data Privacy Principles: Asian Comparisons', *Computer Law & Security Review*, 30.5 (2014), 492–505.

[33] Personal Information Protection Commission General Website, (https://www.pipc.go.kr/eng, 2023)

including e-commerce. The PIPC has the right to audit businesses and organizations that process personal data to determine if they abide by the law. [34]

Article 31 of PIPA provides a strong foundation for protecting personal data, mandating that personal information controllers appoint a privacy officer.[35] This clause acknowledges the vital role that a designated person plays in supervising and managing the handling of personal data. The focus on a privacy officer indicates a proactive strategy to guarantee the proper management of personal information.

The clause permits exceptions by the standards specified in the Presidential Decree. For example, an organization might not be required to select a privacy officer if its size, turnover, or other characteristics match certain requirements. This method ensures that larger businesses with more extensive data processing obligations follow greater responsibility standards while acknowledging that smaller entities may have different operational demands.

Moreover, PIPA Article 31 requires privacy officers to carry out a variety of duties, such as creating and executing plans for protecting personal information and regularly surveying processing procedures. This diverse position also includes managing complaints about the processing of personal data, developing internal control frameworks, and supervising privacy education initiatives. The clause forbids any unfair disadvantages during their work, recognizing the value of privacy officers' independence.

The permission under the provision for the formation of a council of privacy officers emphasizes the collaborative nature of the work. This council provides a forum for collaboration on projects, information sharing, and group efforts to improve personal data protection. The government's dedication to promoting a unified and prosperous approach to data protection is further evidenced by the Protection Commission's support.

On the other hand, the legislative framework in Indonesia concerning Electronic System Providers needs to include a

[34] Fahreza Daniswara and Faiz Rahman, "Perlindungan Data Pribadi: Studi Komparasi Terhadap Praktik Di Singapura, Amerika Serikat, Dan Malaysia," *Center For Digital Society* 31 (2018): 24

[35] Robert Walters and Marko Novak, *Cyber Security, Artificial Intelligence, Data Protection & the Law* (Springer, 2021).

comprehensive and explicit provision similar to Article 31 of PIPA in South Korea. While legislation like Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) has helped Indonesia make progress toward data protection, a noteworthy lack of a specific regulation mandating the nomination of a responsible figure for personal data protection still needs to be made. The lack of any particular regulation makes it difficult to ensure responsibility regarding Electronic System Providers' processing of personal data in Indonesia. In the absence of a designated privacy officer or a similar legal obligation, who is in charge of supervising and carrying out data protection procedures may need to be clarified.

As the first point emphasizes, this regulatory gap becomes even more apparent when one takes into account the importance of accountability in fostering innovation and digital transformation. The lack of a designated responsible individual could hinder the development and execution of comprehensive plans for safeguarding personal information, conducting routine evaluations of processing procedures, and addressing complaints pertaining to personal information.

A comparison between the PIPA Article 31 of South Korea and the current legislative framework in Indonesia shows the significance of having a specific clause for accountability in processing personal data. With its focus on a designated privacy officer and cooperative measures, South Korea's approach offers a comprehensive framework that encourages trust and creativity in the digital space. Clear rules and regulations, like those in South Korea, must be established as Indonesia advances its digital transformation to guarantee accountability and encourage responsible innovation in personal data protection.

Analyzed from several consequences of the electronic systems for businesses in Indonesia and South Korea have several differences. The teleological analysis between Indonesia and South Korea aims in Private Sector Electronic Systems regulation reveals a stark contrast in the legislative frameworks regarding personal data protection between South Korea and Indonesia. South Korea's robust legal system, exemplified by Article 31 of the Personal Information Protection Act (PIPA), mandates the appointment of a privacy officer, fostering accountability and ensuring proper management of personal data. This

proactive approach aims to promote trust and innovation in the digital space, ultimately enhancing data protection measures and fostering a conducive environment for digital businesses.

Conversely, Indonesia's legislative framework needs a comprehensive provision similar to Article 31 of PIPA, resulting in a notable gap in ensuring accountability for Electronic System Providers (PSEs) regarding personal data processing. This regulatory deficiency could impede the development and execution of comprehensive plans for safeguarding personal information and hinder innovation in the digital sector. Therefore, establishing clear rules and regulations, starting from the aim of the PSE System akin to those in South Korea, is imperative for Indonesia's digital transformation to ensure accountability and foster responsible innovation in personal data protection.

c. Indonesia and South Korea on Data Privacy Protection: Best Practices

It is vital to recognize that there are other countries where there are concerns about government accountability toward PSE.[36] In many countries, regulations often place a greater emphasis on the role of businesses in managing personal data rather than direct government obligations. This is partly due to the rapidly changing nature of technology and complex privacy issues. South Korea is a state that has significant technological advancements and a recognition of the importance of personal data protection. Therefore, comparing the data protection laws between Indonesia and South Korea becomes essential to understanding the approaches, principles, and challenges both countries face in addressing these issues.

It is crucial to evaluate the legal methods both countries have taken to protect personal data in an era when data may readily traverse international borders and global entities gather data from numerous sources. Do the fundamental tenets of protecting personal data converge or diverge? How do the two nations deal with cross-border cooperation in protecting the personal information of their citizens?

[36] Tsamara.

These are important inquiries that can be resolved through careful comparison.

Comparing the laws and regulations of Indonesia and South Korea reveals that both nations place equal emphasis on the rights of the individual, data gathering with consent, the responsibilities of data collecting institutions, and regulatory monitoring. However, there are still variations in the specifics and accents. South Korea compiled all the Personal Information Protection regulations in one website managed by PIPC.

This comparison also shows how these two nations approach the problems of securing personal data in different ways. While South Korea has included elements of personal data protection in numerous sectoral regulations, Indonesia has more recent and narrowly focused laws on the subject.

South Koreans are heavy users of social network services (SNSs) and various other Internet-based services. Along the way, the country has become immensely information-intensive.[37] As a significant player in the technology and e-commerce sectors, South Korea has taken proactive measures to guarantee the security and legality of customer data. The South Korean government now places a high priority on monitoring and enforcing laws pertaining to personal data protection, particularly in the context of e-commerce.[38] The task of ensuring that e-commerce platforms abide by the rules of personal data protection regulations falls under the purview of PIPC in the context of e-commerce. It involves ensuring that consumers formally consent before their personal information is gathered and used. PIPC also monitors whether the personal information gathered is used for what it was meant to be used for and whether there are procedures in place to enable customers to view, update, or delete their personal information.

PIPC has the power to impose penalties for breaches of personal data protection in addition to providing oversight. It includes financial

37 Haksoo Ko, John Leitner, Eunsoo Kim, Jonggu Jeong, Structure and enforcement of data privacy law in South Korea, International Data Privacy Law, Volume 7, Issue 2, May 2017, Pages 100–114, https://doi.org/10.1093/idpl/ipx004

38 Sekaring Ayumeida Kusnadi, 'Perlindungan Hukum Data Pribadi Sebagai Hak Privasi', *AL WASATH Jurnal Ilmu Hukum*, 2.1 (2021), 9–16.

penalties and other administrative sanctions against organizations or people who disobey the rules governing personal data protection. Different sanctions may be imposed depending on the severity of the infraction and how it affects customers. As a result, South Korean e-commerce businesses have a solid incentive to abide by the legal requirements for personal data protection.

The South Korean government has also developed rules controlling consumer protection in e-commerce and PIPC.[39] The law requires e-commerce platforms to provide clear information on how personal data will be used and to protect consumers' rights to privacy and data security. E-commerce companies are also required to have easily accessible and understandable privacy. South Korea began to enforce these regulations for its public sector during the 1990s[40] and extended them to the private sector in 2001, ultimately leading to the Comprehensive Personal Information Privacy Act of 2011.[41]

The importance of supervision and law enforcement in the protection of personal data in the e-commerce sector in South Korea cannot be underestimated. As mentioned in Article 5 of PIPA, The State and local governments shall formulate policies to prevent harmful consequences of beyond-purpose collection, abuse and misuse of personal information, indiscrete surveillance and tracking, etc., and to enhance the dignity of human beings and to ensure the protection of individual privacy. South Korea's special provision regarding Pseudonymized Information in Articles 28-2 to 28-7 supports the privacy data of Business entities. At the beginning of 2020, South Korea's legislative body revised significant laws related to data protection. The changes were implemented to, among other things, encourage the use of pseudonymized personal data. It involved permitting the processing of such data for purposes such as archiving, scientific research, or statistical analysis, even without obtaining consent from the individuals to whom the data pertains.[42]

---

[39] Daniswara and Rahman.

[40] Jihyun Park, Dodik Setiawan Nur Heriyanto, 'Immigration Exemptions Provision of UK Data Protection Act and Personal Information Protection,' *Hongik Law Review,* 23.3 (2022), 391-400.

[41] Greenleaf and Park.

[42] Haksoo Ko and Sangchul Park, 'How to De-Identify Personal Data in South Korea: An Evolutionary Tale,' *International Data Privacy Law*, 10.4 (2020), 385–94.

The processing of pseudonymized data is covered under Article 28-2 to Article 28-7 of the Korean Personal Information Protection Act (PIPA), which provides a sophisticated method of striking a balance between privacy concerns and public objectives. This clause gives controllers of personal information the right to process pseudonymized data for archiving, scientific, statistical, and public interest purposes without obtaining the express agreement of data subjects. Pseudonymized information is information that has been altered to make it difficult or almost impossible to identify specific individuals. However, when providing pseudonymized material to other parties, the law expressly forbids including any information that could be used to identify a person individually.

Notwithstanding Article 28.2, the combination of pseudonymized information between different personal information processors for statistical compilation, scientific research, public record-keeping, etc., shall be performed by a specialized organization designated by the Protection Committee or the head of the relevant central administrative agency. A personal information manager who wishes to export combined information outside of the organization that performed the combination must process it as pseudonymized information and then obtain approval from the head of the specialized organization[43].

In terms of restrictive process processing pseudonymized information, the personal information processor shall take technical, administrative, and physical measures necessary to ensure the safety of such information so that it is not lost, stolen, leaked, forged, altered, or damaged, including separately storing and managing additional information to restore it to its original state, as prescribed by Presidential Decree[44].

Most of all, a person processing pseudonymized information shal l not process pseudonymized details to identify a specific individual. If information that can identify a particular individual is generated in the course of processing pseudonymized information, the personal inform ation processor shall immediately stop processing the data and retrieve

[43] Personal Information Protection Act of Korea, Article 28-3.
[44] Personal Information Protection Act of Korea, Article 28-4.

and destroy it without delay[45].

This clause protects people's privacy by using pseudonyms to acknowledge the value of supporting scientific study, statistical analysis, and public archiving. The emphasis placed on eliminating components that make it easier for an individual to be identified during data sharing reflects a dedication to protecting the security and confidentiality of pseudonymized data. Processing without express consent is permitted as long as the data is used responsibly and ethically, minimizing the possibility of abuse or damage.

Indonesia has no specific clause similar to Article 28-2 of Korea. Indonesia's existing data protection system needs to include preventive measures of this kind, which could make it challenging to strike a compromise between promoting research and safeguarding individuals' privacy. Without explicit restrictions regulating pseudonymized information, there might be a heightened danger of unlawful or inadvertent identification of persons through shared data. Provisions akin to those found in Korea's PIPA would be beneficial to Indonesia's data protection landscape, as they would provide clear guidelines for the responsible processing of pseudonymized information and define the parameters for its use in public interest and scientific research projects. These regulatory improvements would bring Indonesia's data protection system up to date with international standards and best practices, making it more thorough and privacy-conscious. [46] And so on the comparison results are mentioned in the table below.

Table 1. Comparison of Personal Data Protection of Electronic System Operators between Indonesia and South Korea.

Regulatory Aspects as Comparison points	South Korea	Indonesia

[45] Personal Information Protection Act of Korea, Article 28-5.

[46] Trias Palupi Kurnianingrum, 'URGENSI PELINDUNGAN DATA PRIBADI KONSUMEN DI ERA EKONOMI DIGITAL', *Kajian*, 25.3 (2023), 197–216.

Regulatory Aspects as Comparison points	South Korea	Indonesia
Main Laws	Personal Information Protection Act / South Korea data protection law (PIPA) 2020 and amended 2023	Law Number 27 of 2022 concerning Personal Data Protection, and PP No. 71 of 2019 concerning Personal Data Protection.
Key Principles	- Necessity - Openness - Courage - Public Interest - Obligation - Provision of information - Deletion of data	- Written permission - Transparency - Individual rights (access, correction, deletion) - Principle of fairness - Provision of information - Supervision by PPDP
Oversight and Enforcement	PIPC has the authority to: - Check and assess compliance - Give sanctions (fines, administrative sanctions)	The Ministry of Communication and Information and PPDP have a role in monitoring and enforcement, including providing sanctions.
Individual Rights	Individuals' rights to access, correct, and delete their personal data are strictly regulated.	Individual rights are recognized and regulated, including the right to access and assign delegation personal data.
Electronic System Registration for business entities	South Korea emphasizes the importance of written consent in collecting and processing personal data.	Indonesia also emphasizes written consent as a critical principle, requiring permission from the personal data owner.
Pseudonymized Information	The processing of pseudonymized information is expressly addressed by Article 28-2 of the Personal Information Protection Act (PIPA), which is the legislative foundation for protecting personal data in South Korea. According to this clause, controllers of personal information are allowed to treat data for statistical, scientific, and public interest purposes	There needs to be a specific regulation in Indonesia that explicitly regulates the processing of pseudonymized data, similar to Article 28-2 in South Korea.

Regulatory Aspects as Comparison points	South Korea	Indonesia
	without getting the express agreement of the subjects. The Act, which carefully balances privacy concerns with the advancement of research and public interest programs, clearly forbids including any information that could be used to uniquely identify an individual when exchanging pseudonymized data with other parties.	
Privacy Officers	Article 31 of the Personal Information Protection Act (PIPA) in South Korea requires personal information controllers to designate Privacy Officers, highlighting the officer's vital role in supervising the processing of personal data. The clause lists particular duties, such as creating protection strategies, conducting routine evaluations of processing procedures, and managing complaints. Furthermore, it promotes teamwork by establishing a council of Privacy Officers.	Indonesia still needs to develop a specific law governing the appointment of Privacy Officers to Electronic System Providers. This regulatory vacuum prevents the development of a thorough framework for moral data management and innovation by creating uncertainty about the duties and accountability of those in charge of personal data protection.

The laws of South Korea provide guidance that emphasizes the importance of written consent and openness in the gathering and processing personal data. Building trust and ensuring that customers have control over their personal data requires giving customers clear information about how their data will be handled. Additionally, requiring explicit authorization ensures that users voluntarily consent to the use of their data, limiting the gathering of illegitimate or undesirable data.

Indonesia may adopt South Korea's effective strategy of creating a solid independent regulatory organization to monitor personal data protection procedures in the e-commerce industry, such as the Personal Information Protection Commission (PIPC). It involves appointing a Chief Privacy Officer and putting policies in place pertaining to data that has been pseudonymized. In contrast to South Korea's proactive steps, Indonesia currently needs clearer policies regarding pseudonymized information and the function of a privacy officer. To improve the regulation and protection of personal information in e-commerce, Indonesia should consider either strengthening current supervisory organizations or creating comparable new ones. A major step toward enhancing Indonesia's personal data protection would be to adopt South Korea's model, which includes appointing privacy officers and implementing laws about pseudonymized information.

Conclusion

The objectives of PSE and personal data protection have both been impacted by uncertainty in the legislation governing personal data protection in the private sector in Indonesia, the world of Electronic System Providers (PSE).[47] Unfortunately, the confusion impacting company operators has come from the need for more clarity around the Electronic System Providers' (PSE) principal function as tools for promoting economic growth and digital innovation or as regulatory instruments. As a result, there needs to be more personal data protection, primarily due to flaws in the laws and a lack of government accountability for PSE. On the other hand, Indonesia's government still needs to present complex regulations that keep pace with technological advancements and ensure adequate personal data protection due to its unclear aims and fewer protection practices.

Insights gained from South Korea's method of implementing personal data protection regulations also expose notable variations between the two nations' methods. By implementing comprehensive laws and establishing a powerful supervisory organization, the Personal Information Privacy Commission (PIPC), South Korea has

[47] Moha, Sukarmi, and Kusumadara.

adopted more comprehensive, all-encompassing measures to address the issue of personal data privacy. It has been found that South Korea, in nearly 30 years, has developed a protection not only within the law that demands obedience from the society and business entities but also the institutional and protection practice with Pseudonymized information and requires a privacy officer to control the data from the business entities.

Bibliography

Anjani, Margaretha Rosa, and Budi Santoso, 'Urgensi Rekonstruksi Hukum E-Commerce Di Indonesia', *Law Reform*, 14.1 (2018), 89–103

Budiman, Adhigama, Genoveva Alicia K.S. Maya, Maidina Rahmawati, and Zainal Abidin, *Mengatur Ulang Kebijakan Pidana Di Ruang Siber: Studi Tentang Penerapan UU ITE Di Indonesia* (Jakarta Selatan: ICJR, 2021)

Greenleaf, Graham, and Whon-il Park, 'South Korea's Innovations in Data Privacy Principles: Asian Comparisons', *Computer Law & Security Review*, 30.5 (2014), 492–505

Haksoo Ko, John Leitner, Eunsoo Kim, Jonggu Jeong, Structure and enforcement of data privacy law in South Korea, *International Data Privacy Law*, Volume 7, Issue 2, May 2017, Pages 100–114, https://doi.org/10.1093/idpl/ipx004

Janis, Ranita Gustisia, Elko Lucky Mamesah, and Debby Telly Antow, 'ASPEK PIDANA DALAM PENIPUAN ONLINE DENGAN MODUS INVESTASI', *LEX PRIVATUM*, 11.4 (2023)

Jingga, Eric, 'Pelindungan Hak Ekonomi Pemilik Akun PSE Lingkup Privat Dari Pemblokiran Akibat Belum Terdaftar Di Indonesia', *COMSERVA: Jurnal Penelitian Dan Pengabdian Masyarakat*, 3.03 (2023), 849–61

Jihyun Park, Dodik Setiawan Nur Heriyanto, 'Immigration Exemptions Provision of UK Data Protection Act and Personal Information Protection', *Hongik Law Review,* 23.3 (2022), 391-400.

Ko, Haksoo, and Sangchul Park, 'How to De-Identify Personal Data in South Korea: An Evolutionary Tale', *International Data Privacy Law*, 10.4 (2020), 385–94

Kurnianingrum, Trias Palupi, 'URGENSI PELINDUNGAN DATA PRIBADI KONSUMEN DI ERA EKONOMI DIGITAL', *Kajian*, 25.3 (2023), 197–216

Kusnadi, Sekaring Ayumeida, 'Perlindungan Hukum Data Pribadi Sebagai Hak Privasi', *AL WASATH Jurnal Ilmu Hukum*, 2.1 (2021), 9–16

Malik, Piyush, 'Governing Big Data: Principles and Practices', *IBM Journal of Research and Development*, 57.3/4 (2013), 1

Manullang, E Fernando M, 'Penafsiran Teleologis/Sosiologis, Penafsiran Purposive Dan Aharon Barak: Suatu Refleksi Kritis', *Veritas et Justitia*, 5.2 (2019), 262–85

Moha, Mohamad Rivaldi, Sukarmi Sukarmi, and Afifah Kusumadara, 'Urgensi Pendaftaran Penyelenggara Sistem Elektronik Bagi Pelaku Usaha E-Commerce', *Jambura Law Review*, 2.2 (2020), 101–19

Muhaimin, Muhaimin, 'Metode Penelitian Hukum', *Dalam S. Dr. Muhaimin, Metode Penelitian Hukum, Mataram-NTB: Mataram*, 2020

Nasrudin, Fadhi Khoiru, and Rosalinda Elsina Latumahina, 'Perlindungan Hukum Terhadap Konsumen Kartu Sim Yang Mengalami Kebocoran Data Akibat Peretasan', *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, 2.1 (2022), 331–43

Niniek, Suparni, 'Cyberspace Problematika & Antisipasi Pengaturannya', *Sinar Grafika, Jakarta*, 2009

Pariadi, Deky, 'Pengawasan E Commerce Dalam Undang-Undang Perdagangan Dan Undang-Undang Perlindungan Konsumen', *Jurnal Hukum & Pembangunan*, 48.3 (2018), 651–69

Pemerintah RI. "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik."

Pemerintah RI, 2019. https://jdih.kemenkeu.go.id/FullText/2019/71TAHUN2019PP.pdf.

Puspita, Khafidah, 'Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia', *Jurisprudensi: Jurnal Ilmu Syariah, Perundangan-Undangan Dan Ekonomi Islam*, 15.1 (2023), 67–83

Putri, Rifka Pratiwi Ardikha, and Neni Ruhaeni, 'Kewajiban Mendaftarkan E-Commerce Dalam Sistem Elektronik Berdasarkan Peraturan Pemerintah Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik Dan Implementasinya Terhadap E-Commerce Informal', in *Bandung Conference Series: Law Studies*, 2022, II, 47–54

Rao, Prakash, Sreejith Balasubramanian, Nitin Vihari, Shazi Jabeen, Vinaya Shukla, and Janya Chanchaichujit, 'The E-Commerce Supply Chain and Environmental Sustainability: An Empirical Investigation on the Online Retail Sector', *Cogent Business & Management*, 8.1 (2021), 1938377

RI, Ditama Binbangkum - BPK, and Bpk.go.id. "Undang-Undang Perlindungan Data Pribadi." *Ditama Binbangkum - BPK RI*, no. 016999 (2022): 1–50. https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022.

Rosadi, Sinta Dewi, and Garry Gumelar Pratama, 'Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia', *Veritas et Justitia*, 4.1 (2018), 88–110

Sahib, Nathania Salsabila Marikar, Soesi Idayanti, and Kanti Rahayu, 'Problematika Aturan Penyelenggara Sistem Elektronik (PSE) Di Indonesia', *Pancasakti Law Journal (PLJ)*, 1.1 (2023), 61–74

Setiawan, Hezkiel Bram, and Fatma Ulfatun Najicha, 'Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data', *Jurnal Kewarganegaraan*, 6.1 (2022), 976–82

Tsamara, Nadiah, 'Perbandingan Aturan Perlindungan Privasi Atas

Data Pribadi Antara Indonesia Dengan Beberapa Negara', *Jurnal Suara Hukum*, 3.1 (2021), 53–84

Walters, Robert, and Marko Novak, *Cyber Security, Artificial Intelligence, Data Protection & the Law* (Springer, 2021)

Wijayanto, Hendro, Daryono Daryono, and Siti Nasiroh, 'Analisis Forensik Pada Aplikasi Peduli Lindungi Terhadap Kebocoran Data Pribadi', *Jurnal Teknologi Informasi Dan Komunikasi (TIKomSiN)*, 9.2 (2021), 11–18

Yuniarti, Dewi Rizka, Hafidz Fauzan Alfarizy, Zifron Siallagan, and Mochamad Whilky Rizkyanfi, 'ANALISIS POTENSI DAN STRATEGI PENCEGAHAN CYBER CRIM DALAM SISTEM LOGISTIK DI ERA DIGITAL', *Jurnal Bisnis, Logistik Dan Supply Chain (BLOGCHAIN)*, 3.1 (2023), 23–32