Journal of Social Science Studies Vol. 3, No. 1, January 2023, pages 101 – 108

Implementation and Supervision of Personal Data Protection Law on Online Platforms

M. Usman Baraja, Rio Saputra, Pratolo Saktiawan, Febrian Dirgantara, Sarwo Waskito

Sunan Giri University of Surabaya, Indonesia

A R T I C L E I N F O

Article history:
Received 2 September 2022
Revised 30 October 2022
Accepted 29 November 2022

Key words:
Personal data protection,
Personal Data Protection Law,
Supervision,
Sanctions,
Online platforms,
Regulation,
Consumers.

A B S T R A C T

The protection of personal data of online platform users in Indonesia is becoming an increasingly relevant issue in line with the rapid development of information technology. Law Number 27 Year 2022 on Personal Data Protection (PDP) provides the necessary legal framework to regulate the collection, processing, and use of personal data by online platform operators. It regulates users' rights to protect their personal data, and requires platform operators to implement adequate security systems. A major challenge in its implementation is effective supervision and strict enforcement of sanctions for violations. This research aims to evaluate the extent to which the supervision mechanism and the application of sanctions can provide maximum protection for consumers. The research results show that although this regulation provides a strong foundation, the success of personal data protection is highly dependent on coordination between the regulatory institutions, platform operators, and educational efforts to users. To achieve optimal protection, there is a need for improvement in supervision and stricter law enforcement.

INTRODUCTION

In today's digital age, the use of online platforms is widespread and has become an integral part of everyday life. These platforms facilitate economic activities, and serve as a means of communication and entertainment for community. The increasing number of transactions and interactions that occur in cyberspace raises serious issues related to the protection of users' personal data (Usman, 2017). Violation of privacy rights and misuse of personal data are increasingly crucial issues, especially when users do not have sufficient control over their personal information that is spread in the digital world. Clear and firm regulations are needed to protect individual rights in the digital realm (Al Ghani, 2022).

To address this need, Indonesia has formulated and passed Law Number 27 Year 2022 on Personal Data Protection. This law aims to provide better protection for the personal data of Indonesian community, including in the use of online platforms. This regulation covers consumers' rights to know, manage, and control their personal data disseminated through various digital applications and services. With this law, it is expected that there will be a balance between technological advancement and the protection of users' personal rights (Aryani & Susanti, 2022).

The implementation of Law Number 27 Year 2022 still faces a number of challenges. Although this law provides a strong legal basis for personal data protection, the main challenge lies in its consistent and effective implementation at the practical level. The large number of digital platforms operating in Indonesia with varying scales and business models, as well as the different levels of public understanding of the importance of data protection, add to the complexity of monitoring and enforcement. Implementation that is not maximized can have an impact on public distrust of the use of online platforms, which has the potential to harm the digital economy itself (Maskun & Anwar, 2021).

Issues related to transparency and accountability of the use of personal data on online platforms are also a major concern. Many digital companies utilize users' personal data as valuable assets for various purposes (Elvy et al., 2018). Many users are unaware that their personal data is being used by companies for commercial purposes, and they are often uninformed about how it is processed and stored. In fact, according to this law, platform managers are required to provide clear information about the use of personal data and obtain permission from users to process the data.

* *Corresponding author, email address:* ***dr.pratolosaktiawan@gmail.com***

One of the important issues in the protection of personal rights on online platforms is the participation of the community and the private sector in complying with the existing provisions. Although the law has regulated in detail the obligations of platform managers, implementation that is not supported by high awareness from both users and platform management companies may hinder the optimal implementation of personal data protection. Regulations that have been drafted in detail will not be effective if they are not accompanied by real commitment from users and platform managers. An integrated approach is needed, which includes education, supervision, and stronger law enforcement (De Hert & Papakonstantinou, 2016).

Although Law Number 27 Year 2022 provides a clear legal basis for personal data protection, its implementation on the ground still faces various challenges. One of the main problems encountered is the inability of most platform managers to fully comply with its provisions. Most platforms are still not transparent enough in providing information about the collection and use of users' personal data. In fact, there are some companies that do not have a clear policy on personal data protection, or do not comply with data management requirements set by the government. Existing regulations also sometimes do not cover all platforms operating in Indonesia, given that some overseas apps are not fully subject to Indonesian national laws (Dhianty, 2022).

Another problem is the lack of effective supervision in the implementation of personal data protection rules. Although there are agencies responsible for supervision, there are many cases that have not been taken seriously. This is due to the insufficient resources and expertise possessed by supervision institutions, as well as the lack of coordination between institutions dealing with personal data protection issues. Under these conditions, without strict supervision, platform providers can easily ignore their obligation to protect their users' personal data (Hoofnagle et al., 2019).

Although Law Number 27 Year 2022 has provided sanctions for violations committed by platform managers, the application of these sanctions has not been effective in providing a deterrent effect. The sanctions given are often not enough to have a significant impact on violating platform managers. The community is also often unclear about the complaint and dispute resolution mechanisms related to personal data protection, which makes many cases of violations not reach the court table. This creates legal uncertainty for consumers, who should be protected firmly and clearly.

Observing the development of the use of online platforms in Indonesia is very important to ensure that the protection of community' personal data is maintained. Monitoring of digital activities and data protection policies across platforms is necessary to ensure that individual rights are not sacrificed in favor of business interests or system efficiency. Without strict supervision and strict law enforcement, the goal of Law Number 27 Year 2022 to protect the personal rights of online platform users will be difficult to achieve. Legal uncertainty arising from inconsistent implementation can harm the community, as well as hinder the rapid development of the digital economy. Attention to the implementation and enforcement of sanctions in terms of violations of personal data protection is very important.

With more cases of personal data breaches occurring, it is an obligation for the government and related institutions to strengthen supervision and law enforcement against violations that occur in cyberspace. Legal certainty in this sector plays a role in providing protection for users, and creating trust among the community towards the use of safer and more trustworthy digital platforms.

This research aims to analyze the extent to which Law Number 27 Year 2022 can be applied in protecting the personal rights of online platform users, as well as to assess the effectiveness of supervision mechanisms and sanctions against personal data violations. The results of this research are expected to contribute to improving supervision, law enforcement, and enhancing the protection of users' personal rights in the digital world.

RESEARCH METHOD

The research method used in this study is a literature study approach with a normative juridical approach. This approach prioritizes the analysis of applicable legal norms and laws and regulations related to the protection of personal data of online platform users in Indonesia, especially related to Law Number 27 Year 2022 on Personal Data Protection. In this research, the author will explore relevant legal literature, including laws, government regulations, court decisions, and scientific articles related to the topic of personal data protection. This approach allows the author to understand the application of existing laws, as well as analyze their relationship with legal practices that run in society. According to Soekanto (2017), the normative study of law focuses on the norms that exist in legislation, which will provide an understanding of the implementation of the law in everyday life.

In this research, the author will also identify various problems that arise in the implementation of the PDP Law as well as evaluate the existing supervision and law enforcement. The use of a normative juridical approach will provide space to examine the compatibility of existing regulations with the principles of personal data protection at the international level, as well as assess the effectiveness of the regulations applied in Indonesia. This approach aims to provide a comprehensive overview of the weaknesses and strengths of Law Number 27 Year 2022. As stated by Marzuki (2013), normative research aims to provide an explanation of existing legal norms and how they are applied in social reality. References from legal sources, such as legislation and court decisions, will be the main basis for this analysis.

RESULT AND DISCUSSION

The development of information and digital technology has changed many aspects of human life, including in the economic, social and communication fields. The ease of access to digital services has made people increasingly dependent on online platforms in carrying out daily activities, such as shopping, working, learning, and social interaction. In the midst of this progress, new challenges arise, one of which is the issue of personal data protection. Along with the development of online platform-based services, users often provide their personal data without realizing the potential risks that lurk, such as misuse, leakage, or identity theft (Maskun & Anwar, 2021). This poses a great risk to individual security and can be financially and psychologically damaging. In this case, the protection of personal data becomes very important to guarantee the basic rights of consumers, which are often vulnerable to violations by irresponsible parties.

Seeing this situation, Law Number 27 Year 2022 on Personal Data Protection (PDP Law) comes as a regulation that is expected to provide stronger and more comprehensive protection for consumers in Indonesia. This law provides a clear legal basis related to the collection, use, and management of personal data by online platform providers. This regulation also emphasizes the obligation of platform operators to maintain the confidentiality and security of the data they manage, and establishes the rights of users to control how their personal data is processed. Users also have specific rights, such as the right to access, correct, delete personal data, as well as withdraw consent that has been given. With this regulation, it is hoped that the community can feel safer and more protected when using various digital services (Dhianty, 2022).

Article 1 paragraph (2) states that PDP includes all efforts to protect personal data in the context of processing such data, in order to guarantee the constitutional rights of personal data subjects. This provision emphasizes that personal data is protected by law as a guarantee of basic rights for community. In Article 5, it is stipulated that the subject of personal data has the obligation to obtain information regarding the clarity of identity, the basis of legal interests, the purpose of the request, and the use of personal data, as well as the accountability of the party requesting the personal data.

Article 13 paragraph (1) stipulates that personal data subjects have the right to obtain and/or use personal data about themselves from the personal data controller in a form that is in accordance with the structure and/or format commonly used or readable by electronic systems. Article 13 paragraph (2) confirms that a personal data subject has the right to use and transmit personal data about him/her to another personal data controller, provided that the systems used can communicate with each other securely in accordance with the principles of PDP under this law. The implementation of this article is an important part of strengthening the position of individuals in the digital ecosystem.

The rules regarding the processing of personal data are stipulated in Article 16 paragraph (1), which includes: a) Acquisition and collection; b) Processing and analysis; c) Storage; d) Correction and updating; e) Display, announcement, transfer, dissemination, or disclosure; and/or f) Erasure or destruction. Article 16 paragraph (2) explains that the processing of personal data as referred to in paragraph (1) must be carried out in accordance with the principles of PDP, which include: a) Personal data must be processed in a limited and specific, lawful, and transparent manner; b) Personal data processing must be carried out in accordance with its purpose; c) Personal data processing must guarantee the rights of the personal data subject; d) Personal data processing must be accurate, complete, not misleading, up-to-date, and accountable; e) Personal data processing must protect the security of Personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, and loss of personal data; f) The processing of personal data shall disclose the purposes and activities of the processing, as well as PDP failures; g) Personal data shall be destroyed and/or erased after the end of the retention period or based on the request of the personal data subject, unless otherwise provided by laws and regulations; and h) The processing of personal data shall be carried out responsibly and clearly demonstrable.

Article 21 paragraph (1) stipulates that in the case of processing personal data, the personal data controller shall provide information regarding: a) The legality of the processing of personal data; b) The purpose of processing personal data; c) The type and relevance of personal data to be processed; d) The retention period of documents containing personal data; e) Details regarding the information processed; f) The period of processing personal data; and g) The rights of the personal data subject. In the articles that regulate the processing of personal data, it is emphasized that the processing must be carried out lawfully and transparently, and must have legality in order to be legally accountable. This provision also emphasizes the protection of community privacy rights with legal certainty if the data is disseminated.

Article 34 paragraph (1) stipulates that the personal data controller is obliged to conduct a PDP impact assessment in the case of personal data processing that has a high potential risk to the personal data subject. Article 35 affirms that the controller of personal data shall protect and ensure the security of the personal data processed by conducting: a) The preparation and implementation of operational technical measures to protect personal data from processing interference contrary to the provisions of laws and regulations; and b) The determination of the security level of personal data by taking into account the nature and risks of the personal data to be protected in the processing of personal data. Article 36 states that in conducting personal data processing, personal data controllers are obliged to maintain the confidentiality of personal data. This provision emphasizes the obligation of the personal data controller to maintain the confidentiality of individual personal information.

Article 38 provides that personal data controllers shall protect personal data from unauthorized processing. Unauthorized processing refers to any form of use of personal data without a clear legal basis, without the data subject's legitimate consent, or which is contrary to the principles of data protection as set out in law. This provision clearly states the legal protection of personal data from illegal processes or transactions or those that are not in accordance with applicable regulations. As such, this law provides a strong legal framework to protect the rights of personal data subjects and ensure that data processing is conducted in a lawful and responsible manner. In an era where personal data is a highly valuable digital asset, this regulation ensures that its utilization remains within the legal and ethical corridors. This ultimately supports the creation of a safer digital ecosystem.

Article 47 stipulates that personal data controllers shall be responsible for the processing of personal data and demonstrate accountability in the implementation of PDP principles. This responsibility is not only limited to maintaining the technical security of data, but also includes compliance with data protection principles, such as legality, transparency, accountability, and purpose limitation. Article 55 paragraph (2) states that the personal data controller who transfers personal data and receives the transfer is obliged to implement PDP in accordance with the provisions of this law. The two articles emphasize that personal data sent or transferred to the data controller is protected by law and the Act. The same also applies to the management of data received by the data controller. This principle of accountability is at the core of ethical and professional data governance

Article 65 paragraph (1) prohibits any person from unlawfully obtaining or collecting personal data that does not belong to him/her with the intent to benefit himself/herself or others, which may result in harm to the personal data subject. Paragraph (2) emphasizes that every person is prohibited from unlawfully disclosing personal data that does not belong to him/her. Paragraph (3) states that every person is prohibited from unlawfully using personal data that does not belong to him/her. This provision clearly regulates the prohibition of using Personal Data belonging to others for the purpose of profit, which is considered an illegal law. The three paragraphs in this article comprehensively form a strong legal framework to protect data subjects from manipulative and exploitative practices of personal data, while strengthening law enforcement against privacy violations in the digital realm.

The PDP Law also stipulates the legal sanctions that can be imposed on anyone who violates the protection of personal data, as stipulated in Article 67 paragraph (1). Any person who intentionally and unlawfully obtains or collects personal data that does not belong to him/her with the intent to benefit himself/herself or another person, which may result in harm to the personal data subject, shall be punished with a maximum imprisonment of five years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah). This provision underlines that the right to personal data is part of human rights that cannot be violated without consequences. The enforcement of these sanctions is also expected to increase public awareness of the importance of maintaining the confidentiality of personal information and encourage the formation of a more ethical, safe and responsible digital culture in Indonesia.

Similarly, Article 67 paragraph (2) stipulates that any person who intentionally and unlawfully discloses personal data that does not belong to him/her may be punished with a maximum imprisonment of four years and/or a maximum fine of IDR 4,000,000,000.00 (four billion rupiah). Article 67 paragraph (3) states that any person who intentionally and unlawfully uses personal data that does not belong to him/her may be punished with a maximum imprisonment of five years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah). The provisions in Article 67 paragraphs (2) and (3) as a whole emphasize the importance of authorization in any action relating to personal data. The heavy sanctions reflect that personal data is a valuable asset protected by law, and violations of it can have far-reaching impacts, both individually and socially. This arrangement not only serves as a legal threat to violators, but also as a preventive measure to shape a digital culture that respects the right to privacy and prioritizes the protection of personal information in the era of digital transformation.

The existence of legal sanctions in this regulation is expected to enforce legal protection of community personal data and ensnare anyone who commits violations. This reflects the state's commitment to providing justice for its community. Criminal sanctions of imprisonment and fines with large amounts aim to provide a deterrent effect to all parties who commit violations of misuse of personal data. More than that, this regulation aims to support and accommodate the activities of Indonesian community who are vulnerable to the dissemination of personal data, and ensure adequate legal protection. This law provides space for citizens to claim their rights in the event of a violation, and guarantees that the state is present in providing adequate legal protection amid the swift flow of digital transformation.

Overall, the provisions of this law aim to create a safe and transparent environment for the processing of personal data, as well as provide adequate protection for individual privacy rights. Its provisions detail the rights and obligations of both data subjects and data controllers, including basic data protection principles such as transparency, validity of purpose, security, and access restrictions (Negara et al., 2022). With clear regulations, it is expected that trust will be created between personal data subjects and personal data controllers, so as to support the development of a sustainable and responsible digital economy. Through strong data protection, the state signals that technological advancement should not come at the expense of citizens' basic rights.

Although the PDP Law provides much progress in terms of protecting users' personal rights, implementation challenges remain. Ineffective supervision, lack of socialization of users' rights, and low public awareness of the importance of PDP may hinder the effective implementation of this law. In this regard, in addition to the active role of controlling institutions, collaboration between platform providers, the community, and the government is crucial to create a safe digital ecosystem, where users' privacy rights can be properly safeguarded and protect them from all forms of personal data abuse (Aryani & Susanti, 2022).

One of the important aspects regulated in this law is the obligation for online platform providers to seek explicit consent from users before collecting, processing, or using their personal data. This consent must be given clearly and without coercion, allowing users to better understand what is happening with their personal data. The PDP Law also gives consumers the right to access, correct, delete, or transfer their personal data, which is a significant step in strengthening the position of consumers in the legal relationship with platform providers. This marks a major shift in the relationship between users and platform organizers, from a previously unbalanced relationship to a fair and transparent one. The existence of these provisions is an important first step in creating a safe and transparent digital ecosystem. Transparency, accountability, and compliance with data protection principles are key factors for the success of Law Number 27 Year 2022 (Kusumawardani et al., 2020). The articles governing user consent and rights in this Law are a very strategic first step in the development of modern and consumer protection-oriented data governance.

The supervision mechanism for the implementation of this law relies heavily on the Personal Data Protection Agency (BPDP), which is tasked with supervising and enforcing the stipulated provisions. The BPDP has the authority to receive complaints, examine alleged violations, and impose sanctions on platform operators that violate personal data protection provisions. This supervision aims to ensure that online platform operators comply with applicable regulations and protect consumers' personal protection rights in a lawful and transparent manner. An effective supervision process is key to creating a safe digital environment for users, as well as fostering public trust in the use of digital services (Sjahputra, 2010). BPDP is the main actor in bridging the interests of the community as the data owner and the platform organizer as the party that manages the data. The role of BPDP is strategic to support the growth of an equitable digital economy.

Sanctions applied by the BPDP against violations by platform operators are also an important component in ensuring effective personal data protection. The PDP Law provides for administrative sanctions that can be imposed on platform operators who do not fulfill the obligations that have been regulated. The sanctions are in the form of significant fines, which aim to have a deterrent effect on the offending party. In some more severe cases, platform operators may be subject to criminal sanctions, which may include imprisonment for individuals found to have committed serious violations related to personal data. With strict sanctions, it is hoped that platform operators will be more careful in managing users' personal data and preventing potential misuse that can harm consumers (Dhianty, 2022).

The application of sanctions in the PDP Law still faces challenges related to the effectiveness of supervision and the firmness of law enforcement. One of the main problems is that there are still loopholes in the application of sanctions that can be used by platform operators to avoid legal responsibility. The absence of consistent supervision makes legal provisions lose their power to pressure violators, especially from digital platform operators. Some platforms may rely on consumers' incomprehension or inability to fully understand their rights in terms of personal data protection, allowing them to violate the provisions without too many consequences (Van Dijk et al., 2018). Strengthening the supervision system by the BPDP as well as better coordination between related institutions is necessary so that the sanctions applied actually provide maximum protection for consumers (Kurniawati & Yunanto, 2022). With strong supervision and a strict legal system, the sanctions in the PDP Law can truly provide a deterrent effect and optimally protect consumer rights amid the rapid development of the digital ecosystem.

The implementation of effective supervisory mechanisms and the application of strict sanctions must be complemented by increasing public awareness of the importance of personal data protection (Maskun & Anwar, 2021). Many consumers do not fully understand their rights in terms of personal data, be it the right to request information regarding the management of their data or the right to file claims in the event of a violation. Massive education and socialization campaigns on personal data protection are very important so that community better understand the risks associated with using online platforms and how to protect their personal data. Strengthening the capacity of regulatory institutions in counseling the community will also have a positive impact on law enforcement (Raditio, 2014).

The PDP Law also opens up opportunities for international collaboration in terms of personal data management. Since cyberspace knows no borders, the protection of personal data of online platform users that are cross-border requires cooperation between countries to reduce the potential for personal data leaks that can harm consumers. Indonesia, through the PDP Law, also harmonizes personal data protection policies with international standards, such as those regulated in the GDPR (General Data Protection Regulation) in the European Union. By strengthening supervision and law enforcement mechanisms in accordance with international standards, Indonesia can ensure that the personal rights of online platform users are well protected (Al Ghani, 2022). Aligning regulations with international standards will increase the trust of trading partners and investors in Indonesia's data protection system. This will positively impact the growth of the digital economy and facilitate Indonesia's participation in the global technology ecosystem.

Platform providers should also have the obligation to build better security systems to protect users' personal data from the threat of leakage or misuse. This includes the implementation of strong encryption technology, continuous monitoring of activities on the platform, and training for internal staff on the importance of safeguarding users' personal data. The successful implementation of the PDP Law depends not only on the existing regulations, but also on the efforts made by platform providers in implementing high security standards. When providers actively implement high security standards and carry out their obligations consistently, the risk of data breaches can be significantly minimized. These measures will increase public trust in digital services, strengthen the reputation of these platforms, and support the creation of a safe, transparent, and sustainable digital ecosystem.

An effective protection mechanism also includes a complaint system that is easily accessible to consumers in the event of a breach of their personal data. In the PDP Law, there are provisions regarding the right of consumers to file complaints with the This is a very important tool in guaranteeing consumer rights in the digital realm. BPDP if they feel that their rights as data users have been violated. The BPDP has the authority to process these complaints and conduct investigations to ascertain whether any violations have been committed by platform operators. With a clear and easily accessible complaint mechanism, consumers will feel more protected and more trust in using online platforms.

In practice, supervision of online platform operators is often hampered by challenges related to rapidly evolving technology. Online platforms often have enormous global influence, making it more difficult for national supervision institutions to monitor. Platform operators often make periodic system updates without transparent reporting, leaving oversight mechanisms lagging behind actual developments on the ground. This creates a legal loophole that can be exploited by irresponsible parties. There is a need for increased cooperation between national and international supervision institutions to create a more effective system for monitoring and enforcing laws against offenses that occur in cyberspace (Anrova & Sembiring, 2022). This cooperation can prevent violations of personal data rights because the perpetrators are outside Indonesian jurisdiction and comprehensive protection for digital consumers can be realized in real terms.

The implementation of Law Number 27 Year 2022 on PDP in Indonesia is an important step in safeguarding the privacy rights of online platform users. This regulation provides a clear legal framework for how personal data should be collected, used, stored, and deleted, and sets out the rights of individuals over their data. With this regulation, it is expected that consumer rights in terms of personal data management and protection can be better guaranteed. To ensure successful implementation, close cooperation is needed between various related parties, including the government, regulatory institutions, and platform operators. This cross-sector collaboration is crucial in creating a safe digital environment, where users' privacy rights are respected and optimally protected, and public trust in digital services can continue to grow. Without well-coordinated efforts, the protection of personal data will remain at risk, and community trust in digital services may be eroded (Dhianty, 2022).

Effective supervision is key in ensuring that the provisions of the PDP Law are complied with by all parties. Without a strict and responsive monitoring system, the existence of regulations will only be a normative document without real impact. The government and regulatory institutions have a great responsibility in ensuring that online platform operators carry out their obligations in accordance with applicable regulations. Strict enforcement of sanctions against violations, whether in the form of fines or other actions, must be an integral part of the supervision system to create a deterrent effect for violators and prevent the leakage or misuse of personal data. Strong supervision and fair law enforcement are expected to create a safe digital ecosystem.

The success of personal data protection lies in regulation and supervision, and also in community awareness itself (Khaq & Hidayat, 2022). In today's digital era, individuals often easily share personal data through various platforms, whether for transaction purposes, social media, or the use of other digital services. Without awareness of the risks involved, people tend to overlook the importance of safeguarding personal information, opening the door for data misuse by irresponsible parties. Massive socialization and education to users about their rights and how to keep personal data safe should be a priority. With high awareness, community will be more careful in sharing personal information in the digital world, creating a safer and more trusted digital environment.

CONCLUSION

Law Number 27 Year 2022 on PDP provides a strong legal basis to protect the personal rights of online platform users. The success of personal data protection relies heavily on effective implementation, including in terms of supervision and enforcement of sanctions against violations that occur. A proactive monitoring mechanism by the BPDP and the application of strict sanctions for platform operators who violate applicable provisions are expected to create a safe and transparent digital environment. Meanwhile, strengthening the security system by platform organizers is also an important factor to protect users' personal data.

The implications of the results of this study indicate that although the PDP Law provides a clear legal framework, its implementation still faces a number of challenges, especially in terms of effective supervision and sanctions. More intensive collaboration between supervision institutions, platform operators, and the community is needed for this regulation to run well. Platform operators must also be more active in educating users about the importance of personal data protection and ensuring that data management policies are in accordance with applicable regulations.

As a suggestion, steps are needed to strengthen the supervisory system by BPDP by increasing its capacity to process complaints and handle violations that occur. The application of firmer and more systematic sanctions for platform operators who violate the provisions of the PDP Law is also very important. In order for the protection of personal data to be maximally achieved, education to the community regarding their rights as users of online platforms also needs to be strengthened, both through campaigns and broader socialization.

REFERENCES

Al Ghani, M. F. (2022). Urgensi Pengaturan Perlindungan Data Pribadi pada Penyelenggaraan Layanan Pinjaman *Online*. *The Digest: Journal of Jurisprudence and Legisprudence*, 3(1), 38-58.

Anrova, Y., & Sembiring, A. (2022). Peran Lembaga Penjamin Simpanan terhadap Saldo Uang Elektronik pada Dompet Elektronik Dana. *Jurnal Res Justitia: Jurnal Ilmu Hukum*, 2(1), 149-161.

Aryani, A. P., & Susanti, L. E. (2022). Pentingnya Perlindungan Data Pribadi Konsumen dalam Transaksi Online pada Marketplace terhadap Kepuasan Konsumen. *Ahmad Dahlan Legal Perspective*, 2(1), 20-29.

De Hert, P., & Papakonstantinou, V. (2016). The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?. *Computer Law & Security Review*, 32(2), 179-194.

Dhianty, R. (2022). Kebijakan Privasi *(Privacy Policy*) dan Peraturan Perundang-Undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi. *Scripta: Jurnal Kebijakan Publik dan Hukum*, 2(1), 186-199.

Elvy, S. A. (2018). Commodifying Consumer Data in the Era of the Internet of Things. *Boston College Law Review*, 59(2), 423-522.

European Union. (2018). *General Data Protection Regulation (GDPR)*. EUR-Lex.

Gani, A. & D. Darmawan. (2022). Ethics and Accountability in Artificial Intelligence-Based Managerial Decision Making, *Journal of Social Science Studies*, 2(1), 147 – 152.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What It Is and What It Means. *Information & Communications Technology Law*, 28(1), 65-98.

Khairi, M. & D. Darmawan. (2022). Developing HR Capabilities in Data Analysis for More Effective Decision Making in Organizations, *Journal of Social Science Studies*, 2(1), 223 – 228.

Khaq, I. E., & Hidayat, A. (2022). The Law Enforcement Against an Illegal Online Loans Platform. *IUS POSITUM: Journal of Law Theory and Law Enforcement*, 65-76.

Kurniawati, H., & Yunanto, Y. (2022). Perlindungan Hukum terhadap Penyalahgunaan Data Pribadi Debitur dalam Aktivitas Pinjaman *Online*. *Jurnal Ius Constituendum*, 7(1), 102-114.

Kusumawardani, S., Rosadi, S. D., & Gultom, E. (2020). Good Corporate Governance Principles on Internet Intermediary Companies in Protecting the Privacy of Personal Data in Indonesia. *Yustisia*, 9(1), 67-78.

Marzuki, P. M. (2013). *Penelitian Hukum*. Kencana.

Maskun, M., & Anwar, R. N. (2021). Regulation and Protection of Cloud Computing: Literature Review Perspective. *Journal of Law Review*, 3(2), 30-40.

Negara, D. S., Darmawan, D., & Saktiawan, P. (2022). Privacy Violations on Social Media and Interpersonal Trust Among Young Generations. *Journal of Social Science Studies,* 2(2), 151-156.

Raditio, R. (2014). *Aspek Hukum Transaksi Elektronik Perikatan, Pembuktian dan Penyelesaian Sengketa*. Graha Ilmu.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Sekretariat Negara, Jakarta.

Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185. Sekretariat Negara, Jakarta.

Republik Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58. Sekretariat Negara, Jakarta.

Sjahputra, I. (2010). *Perlindungan Konsumen dalam Transaksi Elektronik*. PT. Alumni.

Soekanto, S. (2017). *Pengantar Penelitian Hukum*. Rajawali Pers.

Usman, R. (2017). Karakteristik Uang Elektronik dalam Sistem Pembayaran. *Yuridika*, 32(1), 134.

Van Dijk, N., Tanas, A., Rommetveit, K., & Raab, C. (2018). Right Engineering? The Redesign of Privacy and Personal Data Protection. *International Review of Law, Computers & Technology*, 32(2-3), 230-256.

***Baraja, M. U., R. Saputra, P. Saktiawan, F. Dirgantara, S. Waskito. (2023). Implementation and Supervision of Personal Data Protection Law on Online Platforms, *Journal of Social Science Studies*, 3(1), 101 – 108.**