EQUALEGUM
International Law Journal
E-ISSN 2986-0873

Original Article

REGULATION ON PERSONAL DATA PROTECTION IN THE USE OF E-COMMERCE SERVICES

Domi Dwi Kurniasandi[1)*], Sherly Nanda Aprilia[1)], Nobella Indradjaja[2)], Chamdani[2)]
[1)]Faculty of Law, Prigen Campus, University Wijaya Putra, Indonesia
[2)]Faculty of Law, Benowo Campus, University Wijaya Putra, Indonesia
*Corresponding Author, E-mail: domidwikurniasandi12@gmail.com

ABSTRACT

Background. To realize legal certainty in business, the State protects consumer rights. Consumer rights become a proper subject of research due to the rapid technological advancement impacting the use of electronic devices, which also become a place of business transactions through e-commerce. To be able to use marketplace services, service users must fill out personal data and verify it. The data will be saved in the Big Data by the e-commerce service provider, and there is a potential for data misuse and leak as how they more frequently occur nowadays. This research aims to observe consumer personal data protection in Indonesia.

Research Method. The normative legal method reviews several laws and regulations.

Findings. There have been various regulations related to personal data protection, specifically Law No. 27 of 2022 regarding Personal Data Protection. However, several issues remain that become a basis for the researchers' suggestions.

Conclusion. The Consumer Protection Law states that consumers have the right to safety and security in consuming goods and/or services but does not specifically regulate consumer data protection.

Keywords: Consumer, E-commerce, Marketplace, Personal Data.

BACKGROUND

The impact of rapid technological development has penetrated all aspects of human life, including business transactions or buying and selling activities that utilize breakthroughs, namely marketplaces on electronic devices that become a forum for e-commerce transaction activities. To be able to use marketplace services, service users generally have to fill in personal data in an electronic form and verify it to ensure the validity of the data. In addition to creating an account, consumer data is also obtained through various surveys and data track records (cookies) to measure not only the personal data of service users but also consumer behavior. With the acquisition of consumer personal data, businesses have an obligation or obligation to protect consumers from misuse of their data [1].

In the storage and analysis of consumer data that has been obtained, economic actors use big data technology or Big Data, which is a mechanism for processing data in very large volumes, very large growth speeds, and very varied types. Data arranged in big data can be structured data, namely data with a defined format, or unstructured, namely data with

a format that can change such as data from e-mail, blogs, social media, audio, video, and URL logs. Once obtained, these data are analyzed to determine public responses to various products, trends on platforms and electronic media, and media user behavior. Equipped with knowledge about customer behavior and[2] marketplace conditions, business people can make decisions that are effective, efficient, and expected to benefit their business.

On the other hand, this Big Data mechanism utilizes massive amounts of customer data, so guarantees are needed for consumer data security to protect consumers. In 2023, there have been several alleged data leaks, including government and banking institutions, such as BPJS Ketenagakerjaan, Islamic banks, passport data, Dukcapil data, and voter data[3]. Meanwhile, various marketplace applications that support e-commerce activities are increasingly emerging, so that the flow of data and datasets never stops and even gets faster. This shows the urgency of strict legal protection related to consumer personal data protection.

Based on this background, researchers formulated a problem, namely: how do regulations in Indonesia regulate personal data protection? The formulation of this problem will be examined by first understanding what e-commerce, big data, and consumer protection are. Then, the discussion continued by reviewing regulations related to consumer personal data protection.

RESEARCH METHOD

This research was conducted by applying normative juridical methods, namely the discussion of doctrines or principles in the field of legal science using primary and secondary legal materials. Primary legal materials include laws and regulations related to the subject of study, while secondary legal materials used include journals, books, papers, and articles obtained online through search engines. The statute approach is used to create an understanding of hierarchy in relevant laws and regulations. Furthermore, the analysis was carried out using a descriptive method that uses explanations to examine consumer protection in terms of business people who use big data and how the regulation is implemented in business practices that occur. Primary and secondary legal material are: Code of Civil Law, Law No. 8 of 1999 concerning Consumer Protection, Law No. 38 of 1999 concerning Human Rights, Law No. 19 of 2016 concerning Information and Electronic Transactions, Law No. 27 of 2022 concerning Personal Data Protection, Government Regulation no. 80 of 2019 concerning Trading Through Electronic Systems, Government Regulation no. 71 of 2019 concerning Implementation of Electronic Systems and Transactions.

FINDINGS

Understanding the concepts of e-commerce, Big Data, and Consumer Protection

As explained in the introduction, e-commerce is a commercial field that occurs electronically, precisely through the use of electronic devices such as mobile phones and laptops where service users can access applications or websites through these devices. Sales of products and services through e-commerce are initiated by business actors to build closeness with customers, promote products, build communication with customers, and provide customer satisfaction[4]. The sectors covered by e-commerce services are not only the direct trade of products and services, but also the health, education, finance,

and other sectors that utilize technology to conduct electronic transactions. After 2020, the use of e-commerce has increased to boost the community's economy during the COVID-19 pandemic[5].

Meanwhile, the platform used to conduct e-commerce transactions is called the marketplace. A marketplace is a virtual market that, like a traditional market, brings together sellers and buyers of products and services to conduct commercial transactions, only in this case it is done electronically (e-commerce)[6]. Marketplace can be in the form of applications or websites that make it easy for potential buyers and sellers to access, sort, select, and compare products and services until later to the transaction and feedback stage. In using marketplace services, users enter their data through the registration process, profile updates, and transactions. These data include the user's name, email address, phone number, photo, self-description, shipping address, bank account number, and credit card. In addition, data is also obtained in the activity of using the marketplace platform, namely search data, product preferences, interactions with sellers or products, and cookies that collect other user data related to activities carried out on the platform.

Then, the data that has been collected is regulated in the mechanism of big data or Big Data, which helps organize the data that is so massive. The characteristics of big data include 3V, which is a very large volume or size of data, Velocity which is related to the speed of processing data along with the rapid growth of the amount of data, and Variety, which is a diversity of complex data from various formats and forms[7]. Big data not only talks about storage but also analysis, the results of which become a strong consideration in decision-making by business people. Supported by evidence of data that comes directly from users and analytics, business people can predict trends and user behavior to then advance their business[8].

Of course, this puts consumers' data in the hands of others, so legal protection is needed that protect consumers from misuse of their data. According to Law No. 8 of 1999 concerning Consumer Protection (Consumer Protection Law), consumers are defined as users of goods and/or services, whether for their interests, the interests of their families, others, or the interests of other living beings and do not trade these goods and/or services. The Consumer Protection Law describes consumer protection as all efforts that ensure legal certainty to protect consumers, by upholding the principles of fairness, benefits, certainty, and balance of laws that regulate and guide the application of consumer protection. In article 4 of the Consumer Protection Law, it is also stated that the security and safety of consumers in consuming goods and services is their right.

DISCUSSIONS

Regulations related to Consumer Data Security Assurance as a Form of Consumer Protection

In general, as described above, consumer protection is regulated by the Consumer Protection Law. However, consumer protection in this case is a broad context and includes other aspects such as consumer safety in the use of goods and services, quality of products and services, and others. Indirectly, consumer rights protection is a manifestation of Human Rights, in line with Article 29 of Law No. 38 of 1999 concerning Human Rights (Human Rights Law), which states recognition of the protection of self, family, dignity, honor, and the rights of everyone. Article 31 of the Human Rights Law also states the guarantee of secret freedom in communication through electronic means,

except by order of a judge or other legitimate authority by the provisions of the law.

Regarding the guarantee of consumer data security itself, there are several relevant laws and regulations, namely the Civil Code (KUH Percival), Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law), Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems (PP PMSE), and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). Based on the Second Book of the Civil Code, there are 4 categories of objects, namely tangible and intangible objects and movable and immovable objects, where the person or party who controls an object is entitled to the object. Absolute property rights are protected from other third parties. In this case, personal data can be categorized as objects[9], precisely intangible objects, and can have economic value that can be traded in the hands of third parties. Regarding data ownership, according to PP PMSE Article 58 paragraph 1, personal data is treated as the personal property of the Business Actor concerned.

Seeing that the scope of this issue is in the realm of electronic systems and media, the ITE Law, PP PMSE, and PP PSTE are relevant regulations, and in these three laws and regulations, personal data protection efforts have begun to appear through their provisions. For example, in Article 26 of the ITE Law, it is explained that the use of any personal data must be carried out with the consent of the person concerned. If the provision is violated, the person whose rights are violated can bring a lawsuit related to the losses incurred. In addition, the party administering the electronic system must also delete irrelevant information at the request of the person concerned and provide a mechanism to delete such information.

Furthermore, in the PP PSTE related to the implementation of electronic systems and transactions, Articles 14 to 18 have regulated the protection of personal data, which broadly includes the processing of personal data, consent of the owner of personal data, and deletion of personal data. Then, in the PP PMSE which specifically regulates trade through electronic systems, there is a special section, namely Chapter XI which regulates the Protection of Personal Data, Articles 58 and 59. These articles regulate the obligations of Business Actors to comply with the rules of personal data protection related to the deletion of personal data.

From a number of these provisions, it begins to appear that there is legal protection for personal data, but there are still things that have not been described in the legislation, such as what types of data are included in personal data, especially if various types of data are combined, resulting in confusion and legal uncertainty to protect consumer personal data[10]. In addition, descriptions of the purposes and processing of the use of personal data generally carried out by business actors are often informed to users of marketplace and e-commerce services with long and difficult-to-understand document media (such as in the Privacy Policy, Terms and Conditions)[11]. There is often a phenomenon where users only check the statement "I have read and agree to the Privacy Policy/Terms and Conditions" without first reading it because the description of the service provider is presented in difficult and convoluted technical language.

Finally, in 2022, Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) was enacted and promulgated. Apart from being a nationally enforced law, the PDP Law also addresses the two problems above. Various types of data have been categorized as personal data in Article 4 of the PDP Law, namely full name, nationality, gender, religion, marital status, health data, biometrics, genetics, children, personal finance, crime records,

and even personal data combined or combined to identify a person. Regarding the issue of consent to the processing of personal data described in difficult technical language, it has also been "answered" in Article 22 of the PDP Law which states that consent to the processing of personal data must be carried out in a format that is easy to understand, clear and easy to distinguish, and with clear and simple language.

When viewed from the layman's eye, it can be seen that the PDP Law has regulated the protection of consumers' data in great detail, including the types of personal data, personal data processing, as well as distinguishing the terms Personal Data Subject, Personal Data Controller, and Personal Data Processor as parties involved in handling personal data. The PDP Law in Chapter IX of Institutional Articles 58 to 61 also stipulates that the Government participates in implementing consumer data protection through the existence of institutions. The agency will establish policies and strategies to implement personal data protection, oversee the course of personal data protection, enforce administrative laws on violations of the PDP Law, and facilitate the resolution of related disputes outside the court. The institution is targeted to be operational in October 2024[12].

However, according to some researchers and legal practitioners, there are still some weaknesses in the newly formed PDP Law. First of all, Article 56 of the PDP Law states that the Personal Data Controller may transfer personal data to an overseas controller/processor without the phrase "with the consent of the personal data subject." Thus, the absolute rights of data owners are neglected and even contradict the PDP Law. Moreover, if a dispute occurs later and leads to an international arbitration court with a stronger legal standing, defeat occurs on the Indonesian side. Personal Data Controllers in Indonesia cannot force overseas controllers/processors to comply, so their authority is very limited[13].

Second, some specific types of data are not yet part of the personal data as stipulated in Article 4, such as transaction data and data on sexual orientation and political views. The exclusion of transaction data in personal data can be a gap that can be exploited for misuse of personal data. For example, in the transaction information of an object and its nominal, personal data is discarded and the rest is still used as basic advertising data so that it does not violate the PDP Law[14]. Meanwhile, data such as sexual orientation and political views have not been included as part of personal data, even though these data are prone to be used to discriminate against certain groups, which is contrary to human rights principles.

Third, the PDP Law has not specifically specified the protection of personal data of children and persons with disabilities[15]. In Article 25, it is explained that the processing of children's data must obtain the consent of the child's parents or guardians by the provisions of laws and regulations. This seems common, considering that many apps and websites already set age limits for their users. But in fact, the phenomenon of sharenting[16,17] or share-parenting where parents often upload information about children online is increasingly rife. This has a dangerous impact, not only related to cyber or online identity theft but also on the formation of the child's identity psychologically because parents narrate who the child is and do not allow the process to occur in the child. Sharenting also allows child sexual predators to access online information about children[18]. In the scope of e-commerce, this phenomenon does not occur as often as on social media, but it does not rule out the possibility because there are still services or products that concern children, and children's information can still be displayed through product reviews and so on.

In addition to children, the processing of disability personal data is also determined to be carried out specifically, carried out in a certain way, and with the consent of the person and/or his parent or guardian by the provisions of laws and regulations by Article 26 of the PDP Law. Law No. 8 of 2016 concerning Persons with Disabilities Article 8 letter e states that personal data, correspondence, and other forms of communication from persons with disabilities are protected confidentially. However, there is no specific regulation on the personal data of people with disabilities, considering the vulnerability of leakage and misuse of this data can lead to discrimination and even decent livelihood (for example difficulty in finding a job and becoming unemployed due to discrimination), and so on[19].

The three problems above show that Indonesia's current PDP Law is still unable to protect all Indonesian people completely, so follow-up actions are needed such as changes related to the transfer of personal data to personal data controllers/processors abroad, the addition of sexual orientation and political views as part of personal data, and the regulation of personal data of children and persons with disabilities specifically. Thus, in the use of marketplace services for e-commerce transactions, the public has not been fully protected, especially in conducting transactions abroad, in marketplace platforms that collaborate with data controller vendors from outside Indonesia, platforms that involve specific data beyond what is categorized as personal data, as well as for children and people with disabilities.

Given that various marketplace platforms are generally very easily accessible to anyone anywhere with a frequency that continues to increase with the times, there needs to be socialization and education related to personal data security and the latest legal mechanisms related to personal data protection. The legal mechanism issued by the Government is an effort to protect the public, but this still needs to be supported by the social, educational, and business ethics fields, because there is still uneven public awareness of the importance of securing their data, and many business actors take advantage of all forms of loopholes to misuse consumer data. To support the Government's efforts from the legal side through the existence of positive laws to protect people's personal data, technology education efforts are needed for the community, supervision from the personal data protection authority agency will be formed, and strict law enforcement against all forms of violations that occur.

Relevant regulations related to consumer personal data are contained in the Civil Code which defines categories of objects, the ITE Law, the PSME Law, and the PSTE Law. Meanwhile, personal data protection is specifically regulated in the PDP Law which has answered the problems in other laws and regulations, regulates the limits and mechanisms of personal data protection in detail, and stipulates that there must be a personal data protection authority institution.

Some of the lingering issues related to the PDP Law are (1) limitations on the rights of the owner and authority of the data controller over data transferred to the personal data controller/processor; (2) the addition of specific types of data such as transaction data, sexual orientation data, and political views data as personal data; and (3) there is no special regulation on the personal data of children and persons with disabilities. This is the basis of the researcher's proposal for changes related to personal data transferred to personal data controllers/processors outside Indonesia, the addition of transaction data, sexual orientation, and political views as protected personal data, as well as special arrangements related to personal data of children and persons with disabilities. This is so

that positive laws related to personal data protection can provide fair and equitable legal certainty for all Indonesian people because their rights to personal data are a manifestation of upholding human rights.

CONCLUSION

Through the discussion above, it can be understood that the use of marketplace services that support e-commerce transactions involves obtaining consumer personal data, through registration, profile updates, transactions, and other interactions on the marketplace platform. Personal data is then collected in big data mechanisms to be analyzed and used as a basis for the consideration of business decisions. The Consumer Protection Law states that consumers have the right to safety and security in consuming goods and/or services but does not specifically regulate consumer data protection.

REFERENCES

[1] Mulyawati, Putri, Nabila Shafira, dan Diah Pudjiastuti. "Analisis Perlindungan Data Konsumen pada E-commerce oleh Pelaku Usaha." Wacana Paramarta Jurnal Ilmu Hukum 21, no. 1 (15 Juni 2022): 35–42.

[2] Maryanto, Budi. "Big Data dan Pemanfaatannya dalam Berbagai Sektor." Media Informatika 16, no. 2 (2017): 14–19. https://jurnal.likmi.ac.id/Jurnal/7_2017/0717_02_BudiMaryanto.pdf.

[3] CNN Indonesia. "Daftar Dugaan Kebocoran Data 2023, Termasuk Data Pemilih dan Bank." CNN Indonesia, 31 Desember 2023. https://www.cnnindonesia.com/teknologi/20231231054937-192-1043657/daftar-dugaan-kebocoran-data-2023-termasuk-data-pemilih-dan-bank.

[4] Alwendi. "Penerapan E-Commerce dalam Meningkatkan Daya Saing Usaha." Jurnal Manajemen Bisnis 17, no. 3 (31 Agustus 2020): 317. https://doi.org/10.38043/jmb.v17i3.2486.

[5] Handayanti, Asih, Dea Sukma Agachi, dan Winda Fadillah. "Peran E-Commerce di Masa Pandemi COVID-19." ProListik Jurnal Ilmu Komunikasi 7, no. 1 (April 2022): 27–34. http://ojs.uninus.ac.id/index.php/ProListik/article/view/2342/1319.

[6] Yustiani, Rini, dan Rio Yunanto. "Peran Marketplace sebagai Alternatif Bisnis di Era Teknologi Informasi." Komputa: Jurnal Ilmiah Komputer dan Informatika 6, no. 2 (23 Oktober 2017): 43–48. https://doi.org/10.34010/komputa.v6i2.2476.

[7] Dewi, Athanasia Octaviani Puspita. "Big Data di Perpustakaan dengan Memanfaatkan Data Mining." Anuva: Jurnal Kajian Budaya, Perpustakaan, dan Informasi 4, no. 2 (9 Juni 2020): 223–30. https://doi.org/10.14710/anuva.4.2.223-230.

[8] Syira, Syahdina Damayari, Achmad Fauzi, Choiroel Woestho, Laurencia Vilani, Prado Dian Firmansyah, Demas Rizky Pratama, Atun Dwi Apriliana, Naufal Shafly Abdul Ghaffar, dan Dhea Amelia Putri. "Pemanfaatan Big Data dalam Peningkatan Efektivitas Strategi Komunikasi Marketing Terpadu pada Perusahaan E-Commerce." Jurnal Ekonomi Manajemen Sistem Informasi 4, no. 5 (30 Mei 20231): 891–900. https://dinastirev.org/JEMSI/article/view/1511/939.

[9] Fikri, Muhammad, dan Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi:

Kajian Hukum Posistif Indonesia." Ganesha Law Review 5, no. 1 (Mei 2023): 39–57. https://ejournal2.undiksha.ac.id/index.php/GLR/article/view/2237/1159.

[10] Delpiero, Maichle, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, dan Nafisah Muthmainnah. "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data." Padjadjaran Law Review 9, no. 1 (12 Agustus 2021): 1–22. https://jurnal.fh.unpad.ac.id/index.php/plr/article/view/509/378.

[11] Rizkinaswara, Leski. "Pahami Kebijakan Privasi di Media Sosial untuk Lindungi Data Pribadi." Direktorat Jenderal Aplikasi Informatika, 13 Mei 2019. https://aptika.kominfo.go.id/2019/05/pahami-kebijakan-privasi-di-media-sosial-untuk-lindungi-data-pribadi/.

[12] Septiani, Lenny. "Lembaga Perlindungan Data Pribadi Akan Dibentuk Pertengahan 2024." Katadata.co.id, 26 Januari 2024. https://katadata.co.id/digital/teknologi/65b357325c434/lembaga-perlindungan-data-pribadi-akan-dibentuk-pertengahan-2024.

[13] Atmasasmita, Romli. "Beberapa Kelemahan UU Nomor 27/2022 tentang Perlindungan Data Pribadi." Sindonews.com, 27 Oktober 2022. https://nasional.sindonews.com/read/923975/18/beberapa-kelemahan-uu-nomor-272022-tentang-perlindungan-data-pribadi-1666815001/10.

[14] Wahyuni, Willa. "Sejumlah Kritik Penyusunan dan Potensi Problematika UU PDP." Hukum Online, 20 Desember 2022. https://www.hukumonline.com/berita/a/sejumlah-kritik-penyusunan-dan-potensi-problematika-uu-pdp-lt63a19975d931b/?page=2.

[15] Fridha, Merry, dan Rahmat Edi Irawan. "Eksploitasi Anak Melalui Akun Instagram (Analisis Wacana Kritis Praktek Sharenting oleh Selebgram Ashanty & Rachel Venya)." Komuniti : Jurnal Komunikasi dan Teknologi Informasi 12, no. 1 (9 Juni 2020): 68–80. https://doi.org/10.23917/komuniti.v12i1.10703.

[16] Ramadhanti, Galuh Aulia, Dadang Rahmat Hidayat, dan Pandan Yudhapramesti. "Analisis Wacana Kritis Objektivikasi Anak Perilaku Sharenting di Instagram Risa Saraswati." Komunikologi: Jurnal Pengembangan Ilmu Komunikasi dan Sosial 7, no. 2 (2023): 150–64.

[17] Hidayati, Novi, Fitri Meliani, dan Aan Yuliyanto. "Sharenting dan Perlindungan Hak Privasi Anak di Media Sosial." Research in Early Childhood Education and Parenting 4, no. 1 (23 Juni 2023). https://doi.org/10.17509/recep.v4i1.58181.

[18] EDRi. "Why privacy is particularly crucial for people with disabilities." European Digital Rights (EDRi), 4 December 2019. https://edri.org/our-work/why-privacy-is-particularly-crucial-for-people-with-disabilities/