International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 04 Issue 12 December 2021

DOI: 10.47191/ijsshr/v4-i12-19, Impact factor-5.586

Page No: 3601-3605

The Urgency of the Personal Data Protection Law as an Instrument to Prevent Misuse of Personal Data in *Start-Up* Companies

Dian Firja Ameliani[1], A Tulus Sartono[2], Fitriati[3]

[1,2]Master of Law, Faculty of Law, Universitas Diponegoro

[3]Faculty of Law, Universitas Eka Sakti Padang

ABSTRACT: The *E-Commerce* progress during the Covid-19 pandemic, has had an impact on the emergence of many *start-up* companies such as Tokopedia, Gojek, Traveloka, and Bukalapak. There are legal problems caused by the emergence of *these start-ups*. One of the serious problems it causes is maintaining consumer privacy from *start-up* companies. A large number of applications are used, making it easier for companies to obtain their consumers' data. This raises the possibility of leakage of consumer personal data, the possibility that will arise needs to be considered regarding the guarantee of transaction security and privacy, namely the protection of consumer personal data which can cause problems in the future if data leaks occur. The discussion in this article is how the problems with consumer personal data in start-up companies are and how important the Law on personal data protection is as an effort to protect consumer personal data for start-up companies. However, Indonesia still does not have a law that specifically regulates the protection of personal data, where this law is urgently needed at this time as a legal umbrella for the people of Indonesia.

KEYWORDS: Urgency, Personal Data Protection Law, Personal Data Leakage, *Start-Up* Companies

I. INTRODUCTION

The digital era during this pandemic is progressing very rapidly. The rapid development of technology has an impact on people's lives that cannot be separated from the use of the internet in everyday life. Cyberspace has become a medium for communicating, sharing information, buying and selling goods and services, and various other activities for everyone. This also has an impact on the business and trade development, namely electronic commerce (e-commerce). E-Commerce is a business process using electronic technology that connects companies, consumers, and the public, also the exchange/sale of goods and electronic information services in the form of electronic transactions. All legal relationships that occur in e-commerce transactions are carried out online, so the agreement is called an electronic agreement.[1]

With the advancement of E-Commerce, which later gave rise to many start-up companies that are growing along with the development of technology, such as Tokopedia, Gojek, Traveloka, and Bukalapak. To install the start-up application, consumers must register themselves by filling in their personal data such as full name, place and date of birth, telephone number, address, and others. Where in this case every start-up has our personal data as consumers. The requested personal data is a requirement that must be met by consumers before using the application.[2] So that consumers must fill in their personal data to be able to use or transact in e-commerce.

Every start-up offers its advantages by providing convenience in transactions. However, the advantages provided by these start-up companies do not rule out the possibility of problems. One of these serious problems is in maintaining the privacy of the start-up company's consumers. The possibility that will arise from these problems needs to be considered regarding the guarantee of security and privacy transaction, namely the protection of consumer personal data which can cause problems in the future if data leaks occur. Based on the foregoing, it can be stated that the emergence of start-ups is like 2 (two) sides of a sword, on the one hand, it provides convenience in transactions. On the other hand, there is the potential for misuse of start-up consumers' personal data.

[1] Lathifah Hanim, 'Pengaruh Perkembangan Teknologi Informasi Terhadap Keabsahan Perjanjian Dalam Perdagangan Secara Elektronik (E-Commerce) Di Era Globalisasi', *Jurnal Dinamika Hukum*, 11.1 (2011), 56–66. Hlm. 61.

[2] Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, 'Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia', *Refleksi Hukum: Jurnal Ilmu Hukum*, 3.2 (2019), 145–160, Hlm. 150. <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>.

The Urgency of the Personal Data Protection Law as an Instrument to Prevent Misuse of Personal Data in *Start-Up* Companies

The issue of personal data leakage at start-up companies has occurred at the Bukalapak store. Bukalapak is reported to be one of the sites affected by hackers. Hackers are parties who commit acts against the law in cyberspace activities.[3] Many victim and user accounts were reportedly sold on a popular web marketplace called Dream Market.[4] Personal data has become a concern in Indonesia based on the way the government and private companies collect and process such personal data. Several cases of personal data leaks which then lead to fraudulent crimes which are cybercrimes are a strong reason for the urgency of protecting one's personal data, this is a form of the government effort to protect the privacy of every citizen.

II. PROBLEM FORMULATION

1. What are the consumer personal data problems in start-up companies?
2. How important is the personal data protection law as an effort to protect start-up company consumer personal data?

III. RESEARCH METHODS

The research approach used was normative juridical, by basing the analysis on statutory regulations. This research was also supported by an empirical juridical approach. An empirical juridical approach is an approach that emphasizes the legal aspects in the field associated with the applicable rules.[5] The sources of legal materials in this study consisted of primary legal materials and secondary legal materials. Primary legal materials are legal materials that have general binding power obtained from statutory regulations. Secondary legal materials are materials sourced from literature studies such as books, legal materials collected from the internet that have a relationship with the object of this research.[6] The information obtained was then analyzed qualitatively. The analytical approach used was descriptive-analytical, which describes the legislation relating to legal theories and the practice of implementing positive law concerning research problems.[7]

IV. DISCUSSION

A. Consumer Personal Data Problems in Start-Up Companies

The use of the term Personal Data varies in many countries. The European Union uses the term Personal Data in the General Data Protection Regulation (GDPR) or the Regulation (EU) 2016/679. ASEAN member countries (Malaysia, Singapore, Philippines, and Thailand) also use the same term, namely Personal Data. In addition to using the term personal data or personal data, some countries use the term personal information, such as the United States, Canada, Japan, and South Africa. What makes the difference is the coverage of personal information or data in each of the regulations in these countries. Indonesia itself uses the term personal data in a number of its regulations. Personal data becomes the object of legal protection because it involves the personal security of every community in Indonesia.[8]

Personal data is any data about a person either identified and/or can be identified separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems. This definition is also contained in the Personal Data Protection Bill which has been included in the 2020 Priority National Legislation Program. Furthermore, the expansion of the meaning and scope of the personal data phrase also concerns confidential data from a legal entity, such as companies and cooperatives in Indonesia, which are also objects of legal protection that are included in the phrase personal data.[9]

Referring to Law No. 23 of 2006 concerning Population Administration *jo.* Law No. 24 of 2013 concerning the amendment, personal data is certain personal data that is stored, maintained, and kept true and is confidentiality protected. The same definition is also applied in the Regulation of the Minister of Communication and Information (Permenkominfo) No. 20 of 2016 concerning Personal Data Protection. However, the definition of personal data is different in Government Regulation no. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). According to this regulation, personal data is any data about a person either identified and/or can be identified separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems. The same definition is also stated in the Personal Data Protection Bill.

The definition given by PP PSTE is much broader than the Population Administration Law. The definition is similar to the definition in the General Data Protection Regulation (GDPR). Both definitions are equally applicable in Indonesia. Where the

[3] Bambang Hartono, 'Hacker Dalam Perspektif Hukum Indonesia', *Masalah-Masalah Hukum*, 43.1 (2014), 23–30. Hlm. 24.
[4] inews.Id, "Diretas, Bukalapak: Tidak Ada Data Penting yang Bocor", https://www.inews.id/amp/techo/internet/diretas-bukalapak-tidak-ada-data-penting-yang-bocor, diakses pada 27 Maret 2021.
[5] Yulianto Achmad Mukti Fajar, *Dualisme Penelitian Hukum Normatif Dan Empiris* (Yogyakarta: Pustaka Pelajar, 2017). Hlm. 51.
[6] Soerjono Soekanto, *Pengantar Penelitian Hukum* (Jakarta: UI Press, 1986). Hlm. 81.
[7] Zainal Askin Amirudin, *Pengantar Metode Penelitian Hukum* (Jakarta: Raja Grafindo Persada, 2012). Hlm. 58.
[8] Ridha Aditya Nugraha, 'Perlindungan Data Pribadi Dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data', *Jurnal Mimbar Hukum*, 30.2 (2018), 262–276. Hlm. 267.
[9] Wisnu Prabowo, Satriya Wibawa, and Fuad Azmi, 'Perlindungan Data Personal Siber Di Indonesia', *Padjadjaran Journal of International Relations*, 1.3 (2020), 218–239. Hlm. 221. <https://doi.org/10.24198/padjir.v1i3.26194>.

Population Administration Law applies in the context of personal population data, while the PP applies in the context of data contained electronically and non-electronically within its scope under the auspices of Law No. 11 of 2008 concerning Information and Electronic Transactions.

The existence of the definition of personal data in Indonesia means that there are regulations for the protection of personal data in Indonesia. However, the presence of the Personal Data Protection Bill indicates that the regulation of personal data protection in Indonesia is still far from expectations. The development of information technology has made it easier for many areas of people's lives. Especially the convenience provided by the Internet. However, not only providing convenience but the Internet also raises a problem, including in the legal field, namely legal issues related to the protection of personal data.

The digital society's interaction in using the Internet is very dependent on the availability *(availability)*, integrity *(integrity)*, and confidentiality *(confidentiality)* of the information in cyberspace,[10] for example in making a transaction or registering an application, the person concerned must send certain personal data. People in the modern economic era have liked buying and selling transactions that are easy and fast to do. Electronic transaction activities are increasing along with advances in information technology. This gives rise to a new commodity in the modern economic era, namely electronic commodities[11] including personal data that is performed electronically.

Several cases of theft and sale of consumer personal data of start-up companies in Indonesia, namely, cases of hacking into the Tokopedia *e-commerce* user database by hackers. A total of 91 million user data and more than 7 million Tokopedia merchant data were sold on illegal sites for 5,000 US dollars or around Rp. 75 Million.[12] Tokopedia user data sold include gender, location, username, user's full name, e-mail address, mobile number, and password. Where the data has been collected by hackers since March 2020.

Then the case of data leakage in the rewards application and e-commerce curator from Singapore, ShopBack, occurred in September 2020. ShopBack claimed to have found illegal access to the system containing user data. The Reddoorz user data sales case which was sold for 2,000 US dollars amounted to 5.8 million data. The data is sold on the Raid Forum website which can be openly accessed. The leaked user data includes names, e-mails, passwords, profile photos, gender, and cell phone numbers.[13]

The problem of managing personal data and information by start-up companies needs the attention of the Indonesian government. Leakage or breach of personal data and information will lead to misuse of personal data and information by irresponsible parties. Leaks and breaches of personal data and information occur due to weak supervision from these start-up companies who do not know how to properly manage data and also secure it. Personal data and information should be kept, managed, monitored, and stored properly and securely. However, the case of selling consumer personal data, shows that the management of personal data and information is not properly maintained.

B. The Urgency of the Personal Data Protection Law as an Instrument of Consumer Personal Data Protection in *Start-Up* Companies

In principle, all Indonesian people are consumers, so realizing consumer protection in Indonesia is the same as protecting all Indonesian people. This is in accordance with the goal of the Indonesian state, namely to protect all Indonesian people and all Indonesian bloodshed.[14] Furthermore, Article 28G paragraph 1 of the 1945 Constitution becomes the highest legal umbrella for the protection of personal data. Personal data has existed since someone was born until he died. Personal data is stored by many agencies or institutions that store data. Each agency has its own rules in protecting personal data. Especially for electronic data or documents, the Minister of Communication and Information (Permenkominfo) No. 20 of 2016 concerning Personal Data Protection and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) is quite significant in providing protection.

In the criminal aspect, six laws regulate criminal sanctions for leaking personal data, namely Law No. 8 of 1999 concerning Consumer Protection, Law No. 7 of 1992 jo. UU No. 10 of 1998 concerning Banking, Law No. 11 of 2008 jo. Law No. 19 of 2106 on ITE, Law No. 14 of 2008 on Public Information Disclosure, Law No. 40 of 2014 on Insurance, and Law No. 23 of 2006 jo. UU No. 24 of 2013 on Population Administration. The heaviest prison sentence is in the ITE Law where the criminal sanction for data leakage is a maximum of 10 years in prison. Meanwhile, the heaviest fine is in the Banking Law, where the maximum fine that can

[10] Hidayat Chusnul Chotimah, 2019, Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara, Jurnal politica, Vol. 10, No. 2, Halaman 114.

[11] Sri Redjeki Hartono, *Perspektif Hukum Bisnis Pada Era Teknologi* (Semarang: Badan Penerbit Universitas Diponegoro, 1995). Hlm. 61.

[12] https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all diakses pada 6 April 2021 18.17

[13] https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020?page=all diakses pada 6 April 2021 21.34

[14] Janus Sidabalok, *Hukum Perlindungan Konsumen Di Indonesia* (Jakarta: Citra Aditya Bakti, 2010). Hlm. 61.

be imposed is Rp. 10 billion to Rp. 200 billion. In the Civil aspect, there are several legal instruments with civil mechanisms for someone who feels aggrieved due to the leakage of personal data. This mechanism can be done inside or outside the court. Consumer protection regulations, the financial services sector, ITE, and e-commerce provide the relevant instruments.

However, in the case of returning leaked personal data, when the personal data is electronic, almost no regulations are governing its execution. The electronic leaks are easily duplicated on a massive scale and how then can this data be returned to be "one" so that the data is no longer misused by other parties who may not be involved or do not have any interest in someone's personal data. To protect personal data, there are three steps, namely the first short-term step, which depends on the discussion and ratification of the Personal Data Protection Bill. In the short term, the optimization of existing regulations for law enforcement and dispute resolution should be carried out by authorized institutions or law enforcement in accordance with their respective duties and functions. From the aspect of protection substance, the current regulations are still reliable.

Second, the Intermediate Step, through socialization and *awareness* regarding the importance of confidentiality and protection of personal data must continue to be echoed. Institutions or companies that manage personal data must continue to improve the standards of their security and use. In the long term, the government and the Representative House (DPR) must immediately discuss and complete the discussion of the bill. The third step is the ratification of the Personal Data Protection Bill. The drafting of the Personal Data Protection Law in Indonesia is arguably too late. Until now, Indonesia still does not have regulations that specifically regulate personal data. This lags behind other countries in ASEAN such as Singapore, the Philippines, Thailand, and Malaysia which already have personal data protection laws. The bill on the protection of personal data is still under discussion by the DPR and the Government and is included in the agenda for the 2021 Priority National Legislation Program (Prolegnas).

The number of leaks and breaches of personal data requires the government to pay attention to the importance of protecting personal data. Cases of burglary and sale of personal data and information will continue to occur if there is no management of personal data and information so that it can be easily misused by some irresponsible persons. Freedom of start-up companies in accessing information through the data listed on the Identity Card (KTP). The Directorate General of Population and Civil Registration (Dukcapil) provides access to the Population Identification Number (NIK) and KTP to companies that are invited to cooperate. The data is claimed to be used to support the company's services. Several studies have shown that Indonesian people's awareness of the protection of their personal data on the internet is still low. As a result, the Indonesian people do not take seriously the cases of violations of the protection of personal data. The absence of regulations or rules regarding cybercrime and also crimes against misuse of personal data and information is one of the causes of the high number of cases of misuse of data and information in Indonesia. The government needs to consider securing information infrastructure and the digital economy. Protection and protection efforts also need to be mobilized.[15]

The problem regarding cases of leakage and burglary of personal data shows that the data and personal information management sector in Indonesia is still vulnerable to theft/burglary or buying and selling of personal data and information. So to overcome this problem, a system that regulates data and information management is needed in Indonesia.

V. CONCLUSION

Based on the discussion above, the following conclusions can be drawn; That the specific regulation for the protection of personal data is important to prevent and overcome the occurrence of crimes due to misuse of personal data. Personal data is very important to protect its privacy, it needs a firm legal umbrella to avoid cybercrime due to the company's negligence in protecting the personal data of its consumers. That the management of personal data and information in Indonesia is considered very important to be monitored and managed with a good and guaranteed security system to minimize the crime of theft or theft of data and information as well as the crime of buying and selling data and information online in Indonesia, because the impact of these crimes is the existence of misuse of personal data and information by irresponsible parties, in addition to the need for supervision and certainty of good and proper management, a regulation related to cybercrime and the protection of personal data and information is also needed in Indonesia.

REFERENCES

Book and Journal

1) Amirudin, Zainal Askin, Pengantar Metode Penelitian Hukum (Jakarta: Raja Grafindo Persada, 2012)
2) Bambang Hartono, 'Hacker Dalam Perspektif Hukum Indonesia', Masalah-Masalah Hukum, 43.1 (2014), 23–30
3) Benuf, Kornelius, Siti Mahmudah, and Ery Agus Priyono, 'Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia', Refleksi Hukum: Jurnal Ilmu Hukum, 3.2 (2019), 145–60 <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>

[15] Ririn Aswendi, 2020, Perlindungan Data dan Informasi Pribadi melalui Indonesia data Protection System (IDPS), Jurnal Legislatif, Vol. 3, No. 2, Halaman 177.

4) Hartono, Sri Redjeki, Perspektif Hukum Bisnis Pada Era Teknologi (Semarang: Badan Penerbit Universitas Diponegoro, 1995)
5) Hidayat Chusnul Chotimah, 2019, Tata Kelola Keamanan Siber Dan Diplomasi Siber Di Indonesia Dibawah Kelembagaan Badan Siber Dan Sandi Negara, Jurnal politica, Vol. 10, No. 2.
6) Lathifah Hanim, 'Pengaruh Perkembangan Teknologi Informasi Terhadap Keabsahan Perjanjian Dalam Perdagangan Secara Elektronik (E-Commerce) Di Era Globalisasi', Jurnal Dinamika Hukum, 11.1 (2011), 56–66
7) Mukti Fajar, Yulianto Achmad, Dualisme Penelitian Hukum Normatif Dan Empiris (Yogyakarta: Pustaka Pelajar, 2017)
8) Prabowo, Wisnu, Satriya Wibawa, and Fuad Azmi, 'Perlindungan Data Personal Siber Di Indonesia', Padjadjaran Journal of International Relations, 1.3 (2020), 218–39 <https://doi.org/10.24198/padjir.v1i3.26194>
9) Ridha Aditya Nugraha, 'Perlindungan Data Pribadi Dan Privasi Penumpang Maskapai Penerbangan Pada Era Big Data', Jurnal Mimbar Hukum, 30.2 (2018), 262–76
10) Ririn Aswendi, 2020, Perlindungan Data dan Informasi Pribadi melalui Indonesia data Protection System (IDPS), Jurnal Legislatif, Vol. 3, No. 2.
11) Sidabalok, Janus, Hukum Perlindungan Konsumen Di Indonesia (Jakarta: Citra Aditya Bakti, 2010)
12) Soerjono Soekanto, Pengantar Penelitian Hukum (Jakarta: UI Press, 1986)

Website:

1) inews.Id, "Diretas, Bukalapak: Tidak Ada Data Penting yang Bocor", https://www.inews.id/amp/techo/internet/diretas-bukalapak-tidak-ada-data-penting-yang-bocor, diakses pada 27 Maret 2021.
2) https://tekno.kompas.com/read/2020/05/05/19080067/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all diakses pada 6 April 2021 18.17
3) https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020?page=all diakses pada 6 April 2021 21.34