JURNAL JURISPRUDENCE
Vol. 11, No. 1, 2021, pp.82-99
p-ISSN: 1829-5045; e-ISSN: 2549-5615
Website: http://journals.ums.ac.id/index.php/jurisprudence

Law And Personal Data: Offering Strategies For Consumer Protection In New Normal Situation In Indonesia

Rina Arum Prastyanti
Universitas Duta Bangsa
Email: rina_arum@udb.ac.id

Istiyawati Rahayu
Universitas Duta Bangsa
Email: istie_wati81@yahoo.com

Eiad Yafi
Universiti Kuala Lumpur
Email: eiad@unikl.edu.my

Kelik Wardiono
Universitas Muhammadiyah Surakarta
Email: kelik.wardiono@ums.ac.id

Arief Budiono
Universitas Muhammadiyah Surakarta
areevahims@gmail.com

DOI: 10.23917/jurisprudence.v11i1.14756

Submission Track:

Received:

4 Juni 2021

Final Revision:

3 Desember 2021

Available online:

12 Januari 2021

ABSTRACT

Purpose of the study: The benefits of the internet during a pandemic bring opportunities for cybercrimes, such as online data theft and leakage of consumers' personal data. For this reason, the objectives of this study are 1) to determine the phenomenon of misuse of consumer's personal data amidst COVID-after19 in Indonesia and 2) to describe strategies in preparing consumer personal data protection as the key to the success of the new normal in Indonesia.

Methodology: This study used non-doctrinal research. To describe the phenomenon of misuse of consumers' personal data amidst COVID-19 in Indonesia, the data were collected by distributing questionnaires to internet users in Indonesia and applying qualitative methods employing survey data collection

Corresponding Author:
Name & Email Address
Rina Arum Prastyanti,
Email:
rina_arum@udb.ac.id
.

techniques with stratified multi-stage random sampling technique.

Results: It was found that the consumers' personal data in Indonesia is still unprotected, so the conception adopted by the European Union and the OECD can be used as a reference for Indonesia in making a Law on Personal Data Protection.

Applications of this study: To raise the people's awareness in protecting online personal data and encourage the government to educate society on cyber security through the National Cyber and Crypto Agency

Novelty/ Originality of this study: This paper analyzes the protection strategy of e-commerce consumers during the new normal situation in Indonesia. The originality is that it discusses amidst Covid 19 cyber security.

Keywords: data protection, human right, consumer protection, new normal

INTRODUCTION

COVID-19 pandemic has affected the world in many ways. From an economic point of view, there have been dramatic changes in consumer behavior. Although many businesses have experienced an unprofitable decline, online shopping has increased significantly in the United States, with a 91% increase (Krishnan, 2020). %) and Italy (31%) (Clapp, 2020); this is good news for e-commerce. The internet development in countries such as the United States, Britain, Germany, and the Netherlands has also made the internet a favorite marketing medium or channel (Nasution et al., 2018). In other words, the internet provides benefits during a pandemic. Besides, for academic purposes, the utilization of social media applications, such as Google meet and zoom, is beneficial, in which teachers can carry out online lectures and be supported by e-books. During times of pandemics, the government has also stipulated that the work of every employee from the public and private sectors be done at home. In this case, the internet makes work easier in many aspects (Vishwambar, 2020).

Specifically, the behavior of consumers or the community has adjusted the conditions to overcome a pandemic and survive during a pandemic (Sivarasa, 2014). People are no longer fixated on brands but are more focused on obtaining goods online. This condition brings opportunities for cybercrime. Criminal is directly related to using computers, illegal prohibitions against other people's computer systems or databases, manipulation or theft of

data stored online, or sabotaging equipment and data, known as cybercrime (Lubis, 2016). At least three dangers arise from the use of the internet regarding data storage, among others, an increase in the quantity of data that is not matched by an increase in data storage capacity, which results in a lack of accuracy when classifying data. Secondly, this interconnected electronic data means that many people can have access to some information and then use it for their own purposes. In the end, there will be very little control over who the data users are. Third, there is technocratic behavior that uses databases for the purpose of social control, such as taking medical databases to regulate people's behavior (Gellert, 2015). Therefore, the urgency of this research is the emergence of a problem amid government policies to protect the public from the COVID-19 pandemic with increased use of the internet, threatening personal data protection in several sectors, including:

a. Health sector

Singapore currently has an application called "TraceTogether" to monitor patients infected with COVID-19. Indonesia has also started using a similar application called "Peduli Lindungi". The government assures that the application's confidentiality is guaranteed as mandated in Government Regulation Number 71/2019 concerning Electronic Systems and Transactions, stating that the government is obliged to destroy application user data during the pandemic. The government also guarantees that the data will not be accessible to third parties. However, a phenomenon of cases in a 31-year-old woman and her 64-year-old mother from Depok, West Java, later became known as case 1 and case 2. WhatsApp and social media platforms identified the patients' personal details, including initials, age, photo, occupation, medical records, social media accounts and home addresses. Then, journalists crowded their residences, and the spectacle of hoaxes was uncertain. It can happen to all of us. Violation of the right to privacy and dignity in cases 1 and 2 have impacted their well-being, which is very important for recovery and public health efforts (Ardila, 2020).

b. E-commerce sector

The use of e-commerce has increased since starting activities at home and PSBB (Large-Scale Social Restrictions). Marketplaces, such as Tokopedia, experienced a significant increase in transactions (Wardoyo, 2020). It triggered a data security issue that stated that hackers had stolen and leaked 15 million Tokopedia user data, consisting of email, hashed passwords, and the full name of the account owners (Kumparan, 2020). ShinyHunters claims to have user data from 10 digital companies. Total user data collected reached 73.2 million, of

which 1.2 million were said to be data users from Bhinneka.com. The data were sold on the internet black market site for illegal products on the dark web, at 18,000 US dollars or IDR 266 million for the entire user database of 73.2 million. ShinyHunters also sold user data from each service separately. For 1.2 million Bhinneka users, the official price was US $ 1,200 or around IDR 17.8 million (Pertiwi, 2020).

c. Telecommunication sector

The pandemic of COVID-19 has caused the government to implement a policy of work and study at home, impacting the need to use video conferencing. The use of video conferencing applications in Indonesia includes zooms (257,853), Skype (71,155), Hangouts Meet (10,454), GoTomeeting (8,748), and Cisco Webmeeting (977) (Statqo Analytic, 2020). The use of zoom is in great demand not only because it can accommodate up to 100 meeting participants, but also it can store all conversations. This condition brings the opportunity for security problems. More than 500 thousand zoom accounts are traded on cybercrime sites (dark web) and hacker forums. This data leakage was reported by internet security expert Bleeping Computer. The transacted information includes the email, the personal meeting URL, and the user's HostKey. This data cost US $ 0.002 or around IDR 31 per account, and there were even accounts offered for free to other hackers. It is a prank called Zoomboombing (Annur, 2020). Even the Zoomboobing case also occurred in Indonesia; anonymous accounts participated in a discussion organized by the National Information and Communication Technology Council (Wantiknas).

Issues related to personal data security are not ordinary problems. In the digital era, personal data protection is vital, considering consumers/society are experiencing a period of rapid change, where digital transformation provides new technology, business models, transactions, and various innovative goods and services. Nevertheless, many consumers do not realize the importance of personal data security in transactions. Consumers also do not know that irresponsible parties use their personal data. It signifies that personal data protection in Indonesia is still weak. For this reason, the objectives of this study are 1) to determine the phenomenon of misuse of consumer’s personal data amidst COVID-19 in Indonesia and 2) to describe strategies in preparing consumer personal data protection as the key to the success of the new normal in Indonesia.

RESEARCH METHOD

This study used non-doctrinal research. The non-doctrinal approach allows the researchers to analyze the law from other scientific disciplines' perspectives and employ those disciplines in drafting the law (Salim, 2017). It has grown in design and significance over the years (Creswell, 2003; Tashakkori & Teddlie, 1998, 2003). In this study, to describe the misuse of consumers' personal data amidst COVID-19 in Indonesia, the data were collected from distributing questionnaires to internet users in Indonesia and qualitative methods using survey data collection techniques with stratified multi-stage random sampling technique. The population of this survey was Indonesian citizens in nine major cities.

The number of samples in this survey was 400 respondents with a margin of error of +/- 4.9% at a 95% level of confidence. Concerning stratification, the voter population was grouped by regency/city. Furthermore, the samples were selected in stages in each stratum (district/city). In stage 1, the primary sampling unit (PSU) in this survey was randomly selected at the proportionate village/kelurahan level in each regency/city. In stage 2, from each selected village/*kelurahan*, the existing RT (Neighborhood Association) population was registered to be randomly selected. Survey data collection (determination of respondents and interviews in the field) was carried out on November 1-9, 2020. Data sources used were primary data sources and secondary data sources. The data validity employed triangulation, and the data analysis technique utilized qualitative data analysis.

RESULTS & DISCUSSION

Results

Protection of Consumer's Personal Data in Indonesia

As a strategic country in international trade, Indonesia has pretensions to have adequate personal data protection regulations following international standards. However, despite being part of APEC, to date, Indonesia has never had any special rules regarding personal data protection. In fact, Article 28 of the 1945 Constitution of the Republic of Indonesia concerns the development of personal rights, family, honor, dignity, and property. To see these provisions as provisions regarding privacy and personal data, privacy is the right to enjoy life and respect feelings and thoughts. It corroborates Warren and Brandeis's opinion in the book *"The Right to Privacy"* (Greneaf, 2014).

Privacy protection is closely related to fulfilling personal data rights. The relationship regarding privacy and personal data protection is emphasized by Westin, defining privacy as the right of an individual, group, or institution to determine whether information about them will be communicated to other parties. The definition put forward by Westin is called information privacy since it involves personal information.

Privacy protection is part of personal data protection directly mandated by the Constitution of the Republic of Indonesia, which contains respect for human rights values and equality of individual rights; thus, laws are required. This legal basis should provide more privacy and personal data security to ensure a conducive business climate. It is because, in the digital economy era, telecommunication infrastructure and activities are the backbones of information exchange and electronic transactions between people. Law Number 11 of 2008 concerning Electronic Information and Transactions as well as protection of personal data, especially in Article 15 paragraph (1), states that every Electronic System Operator is required to operate an Electronic System reliably and safely and is responsible for the operation of Electronic Systems. "Safe" in Article 15 paragraph (1) of Law Number 11 of 2008 concerning Electronic Transactions means that Electronic Systems are physically and non-physically protected.

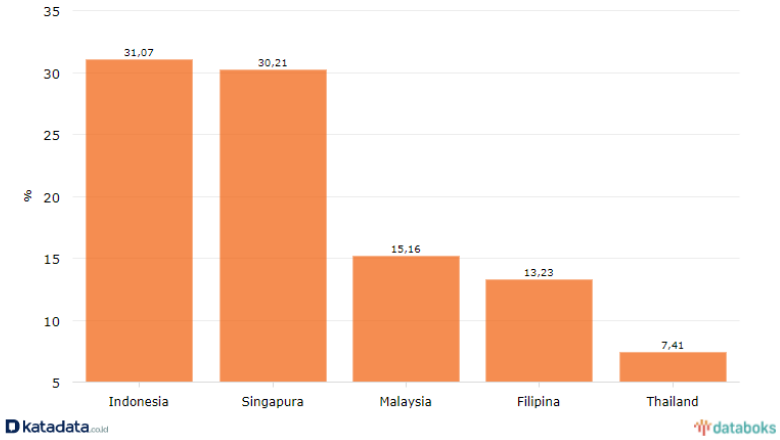

Figure 1. Phishing Trends in ASEAN During Semester 1 of 2019 (The International Criminal Police Organization, 2020)

A 2020 report from the International Criminal Police Organization (Interpol) revealed Southeast Asia targeted cybercriminals trying to infect networks and devices through phishing tricks. Indonesia became the highest target during the first semester of 2019 with 31.07% phishing attempts. The next position was Singapore (30.21%), Malaysia (15.16%), the

Philippines (13.23%), and Thailand (7.41%). The report said the most popular phishing targets were financial institutions, email services and internet service providers. Compared with other countries, especially in Southeast Asia, which are members of ASEAN, Indonesia is the country most left behind in preparing privacy data protection tools for its citizens, both in terms of time and variations in protection. Thus, this research was conducted using two indicators to see consumer data security on the internet (CISSREC, 2017). The first indicator is consumer satisfaction with security privacy on the internet, and the second is consumer awareness of information security.

a. Consumer Satisfaction with Security Privacy on the Internet

1). Have you ever posted your personal photos on social media?

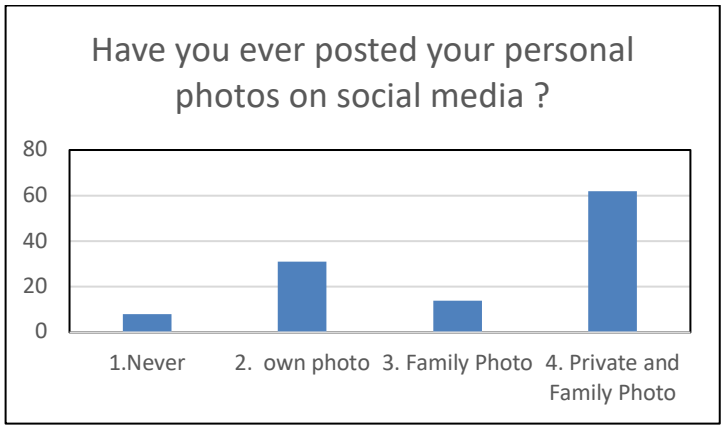

Figure 2. Whether respondents have posted personal photos on social media

62% of respondents answered that they had uploaded personal and family photos on social media. 31% answered that they uploaded personal photos, 14% answered that they had uploaded family photos, while 8% answered that they never uploaded personal photos on social media.

2). What kind of data is posted on the internet?

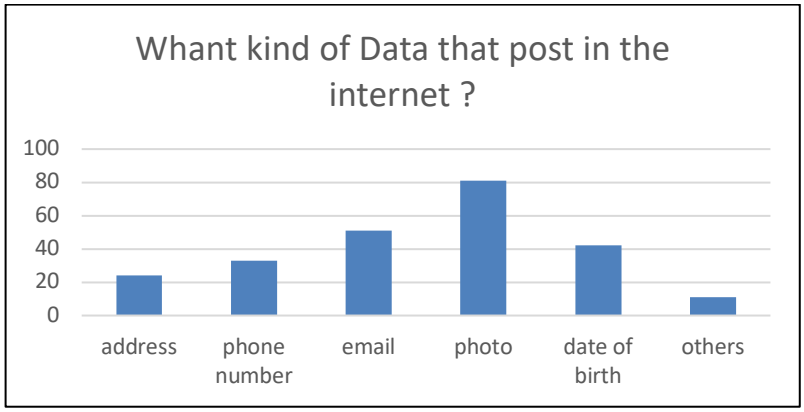

Figure 3. The type of data respondents posted online

Almost all respondents (81%) uploaded their photos on the internet. 51% listed their email address, 33% listed phone numbers, and 24% listed their address.

3). Are you aware that entering personal data online will have the potential to interfere with your privacy?

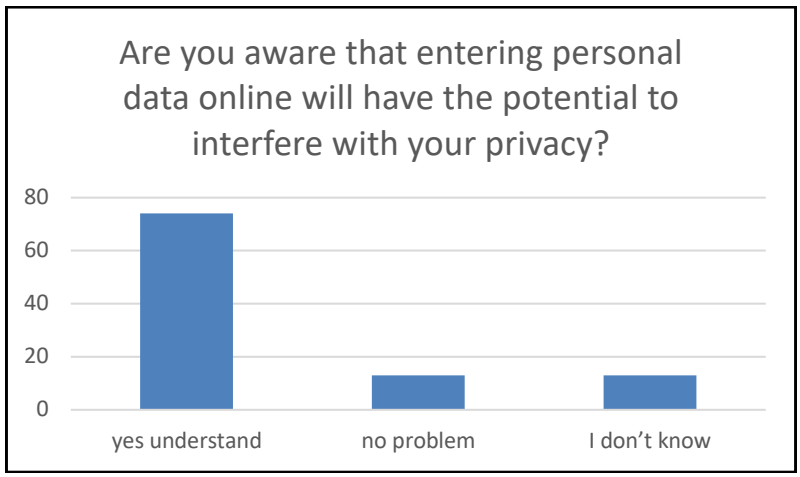

Figure 4. The respondents' awareness on entering personal data online

74% of respondents stated that they understood and were aware that entering personal data into online applications or services has the potential to interfere with privacy. 13% said it was OK, while the remaining 13% said they did not know.

4). Did you read the user's privacy policy in every online service?

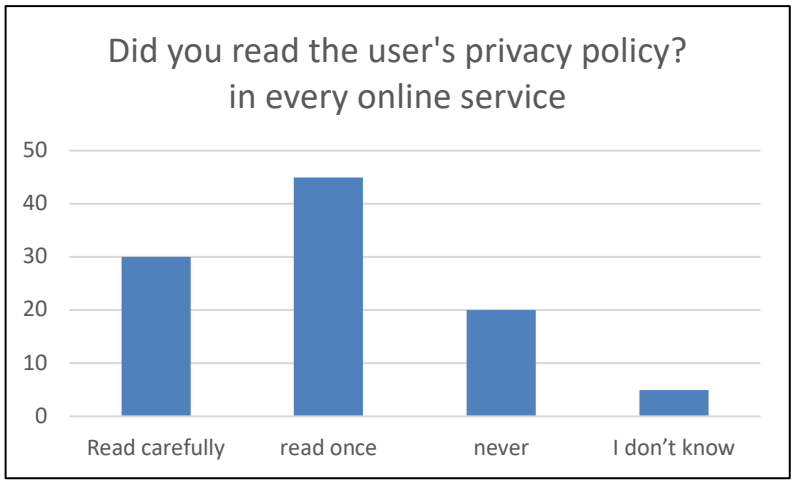

Figure 5. Whether respondents have read the user's privacy policy

45% of respondents answered that they only occasionally read the privacy policies of users of each online service. Only 30% of the respondents answered that they read carefully. 20% answered that they never read at all. Meanwhile, 5% answered that they did not know.

5). Do you know about personal data protection regulations?

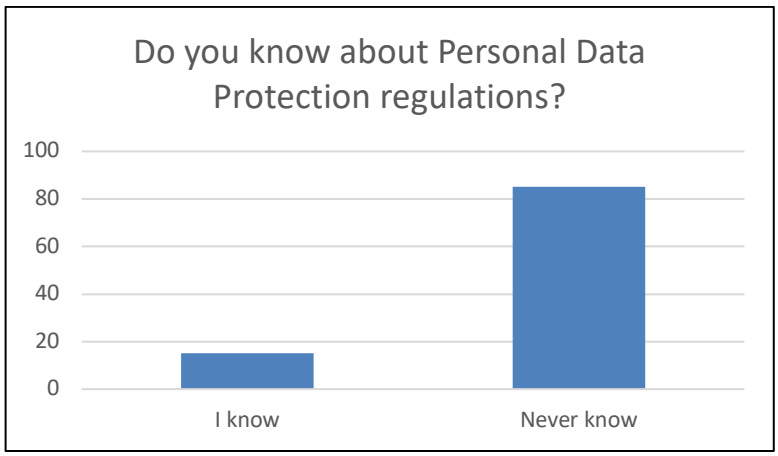

Figure 6. Whether respondents know about personal data protection regulations

85% of respondents answered that they did not know about personal data protection regulations. Only 15% of respondents answered that they knew the regulations to regulate personal data protection.

Based on the above data exposure, it can be seen that internet service users' concerns about the insecurity of SMS/internet banking in Indonesia were not followed by awareness to explore further the regulations governing personal data protection. Entering personal data into applications or online applications should be done with awareness and understanding of the risks. In this study, understanding the risks was not followed by understanding the user's privacy policy in each online service used.

b. Consumer Awareness on Information Security

1). How often do you change the online application password?

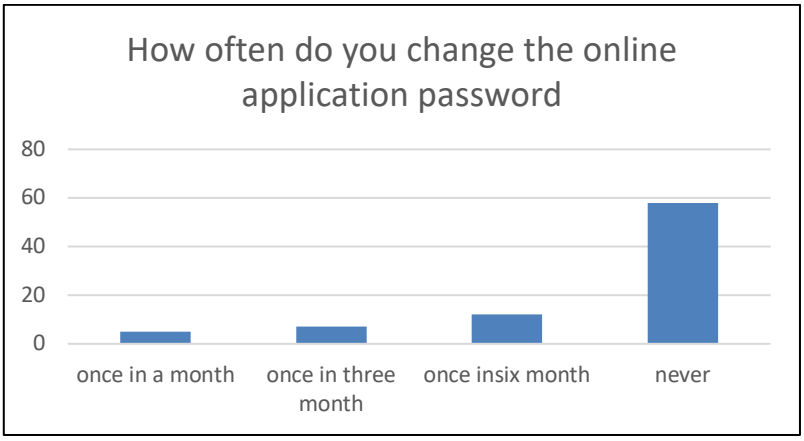

Figure 7. The frequency in changing passwords

Respondents who changed the passwords for applications or online services used were 58%. 7% of them answered that they changed them every three months, 5% answered that they changed them every month, and 12% answered that they changed them every six months.

2). Do you use the same password in every online service application?

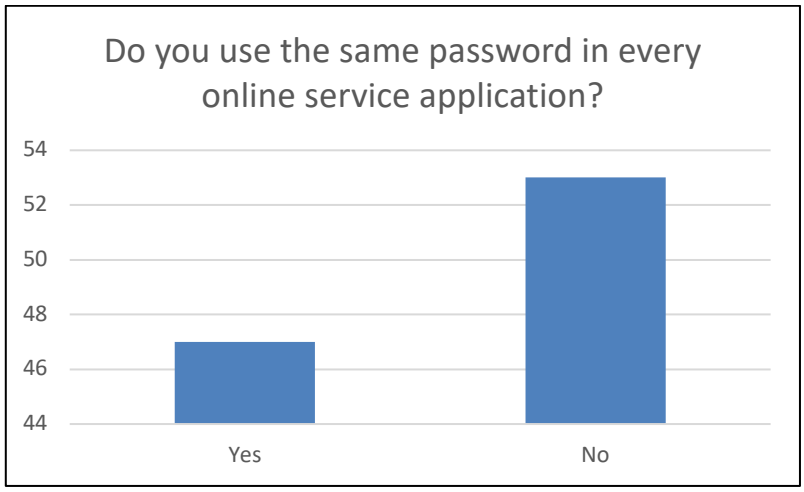

Figure 8. Whether the passwords used are the same.

Then, 47% of respondents used the same password for every application or online service, while 53% answered that they did not use the same password for every application.

2). Are you sure about the security of e-commerce in Indonesia today?

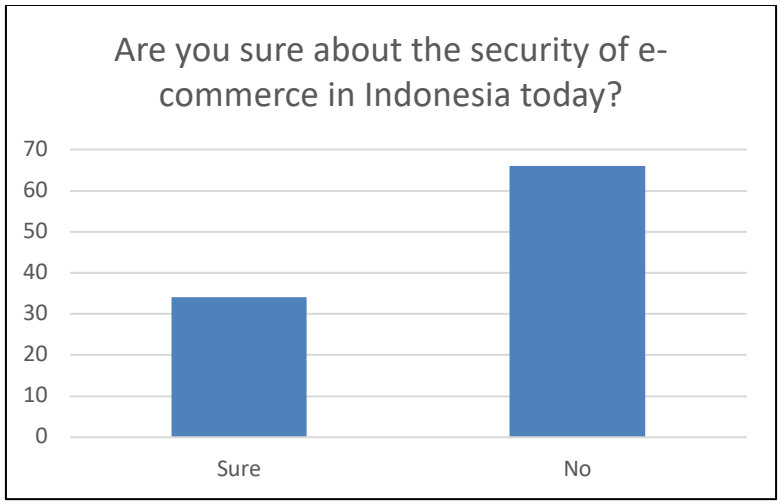

Figure 9. Certainty of e-commerce security in Indonesia

It is shown that 66% answered that they were not sure about the security of e-commerce in Indonesia. Meanwhile, 34% of respondents felt confident about the security of e-commerce in Indonesia.

Based on the above research results, it can be seen that awareness of the importance of privacy was not followed by an awareness of maintaining privacy in online applications or services (data backup or changing passwords periodically). Awareness of the importance of privacy was also not accompanied by a desire to know the regulations governing personal data. In addition, the security of SMS/internet banking or e-commerce in Indonesia was not accompanied by efforts to avoid misuse of personal data. This lack of awareness to protect privacy occurred since users had not experienced the abuse of personal data in online applications or services.

Comparison of Consumer Personal Data Protection in Indonesia and Other Countries

The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, emphasized the need for every country to have laws, which clearly describe the limitation of individuals' right to privacy in certain situations. Regulations regarding this matter must be based on a special decision made by the state in accordance with the law (UN Doc.A/HRC/17/27, 2011) para. 58-59). In its development, the UN Human Rights Council established a report about human rights on March 24, 2015, through Resolution 28/16. This resolution is a follow-up to the UN General Assembly Resolution 68/167 on the Right to Privacy in the Digital Age, issued earlier in December 2013. Outside Indonesia, several laws protecting the privacy and personal data, such as in the European Union Directive, distinguish between 'sensitive' and 'non-sensitive' data based on the level of harm that will be felt to an individual if it is accessed by irresponsible parties (EC Data Protection, 2011). Moreover, several international legal instruments govern internationally recognized privacy principles and personal data. These principles are the foundation of modern national data protection law. One of the international instruments organized by Economic Co-operation and Development (OECD) is to protect the privacy and personal data. The international organization issued privacy guidelines, which are not legally binding but have long been recognized as guidelines for establishing privacy protection norms for OECD member states (Diggelman, 2014).

The United States, Canada, and Australia use the term personally identifiable information (PII), while countries in Europe and Indonesia (Article 26 paragraph (1) of the ITE Law) use the term personal data. Furthermore, it is not only the use of the term that is different; the interpretation of the terminology of personal data also contradicts the legal

system in the United States and Europe. They do not have specific instruments that rigidly interpret the meaning of personal data, but they provide three opportunities for an approach to describe the term: by using a tautological approach, a non-public approach and a specific type of approach) (Schwartz and Solove, 2011). Meanwhile, the European region already has a legal rumen called the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data 1981 (Convention 108) (Djafar, 2019) and Directive 95/46/EC or known as the European Union Data Protection Directive 1995 (DP Directive) (Djafar, 2019), which point of Article 2 letter (a) of these two instruments describes personal data as "information relating to an identified or identifiable one."

Discussion

On the one hand, the internet has provided many benefits that increase development and information opportunities. On the other hand, it also provides new vulnerabilities for interventions in privacy. Circulation data in a digital format that no longer recognizes spatial and territorial boundaries makes it easier for a person's personal data to be exposed or transferred arbitrarily without the control of the data owner. Several cases related to the leakage of someone's personal data are rife.

For example, there is rampant product promotion, ranging from property, insurance, loan facilities, and credit cards. There are also many cases of violation of privacy, especially personal data, leading to fraud, even though consumers have never submitted their personal data to the product's producer concerned. The unclear nature of the perpetrator of the leakage or sale of personal data and the unclear legal mechanism provided by the law makes it difficult to complain about the losses suffered. Therefore, the discourse on strengthening personal data protection, including its mechanisms, is crucial to implement. However, even though the intrusion of personal data has become an actual and real problem, privacy violations have not yet become a popular issue among Indonesians. Even though as one of the countries with the largest active internet users globally, the Indonesian community should be encouraged to have more awareness of their privacy rights. The fact is that the majority of the public in Indonesia has not made personal data part of the property and human rights that must be protected, so it is often found that someone unconsciously indulges his privacy, including personal data about himself.

Moreover, data protection implies that individuals have the right to determine whether they will share or exchange their personal data. In addition, individuals have the right to

determine the conditions for implementing the data transfer. It is vital that cases of violations of the right to privacy, especially personal data, are very frequent. In his report, the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, emphasized the need for states to have laws that clearly describe the limitation of the right to privacy of individuals in certain situations.

The rules regarding this matter must be based on a special decision made by the state in accordance with the law. The increasing penetration of internet users in Indonesia, including the increasingly varied use of this technology in the development of electronic systems in the context of trade, banking, and public services such as health, makes the existence of personal data protection laws is increasingly important. Of course, understanding personal data protection is inseparable from the meaning of "data," which can be classified as "personal data," and what forms of protection can be given to the personal data concerned. Literally, data is the plural form of the word "datum," which means a piece of information in Latin or, in other words, data can be understood as a collection of datums that give birth to information. Data must also contain a group of facts in the form of symbols [such as alphabets, numbers, images, or other special symbols] that represent ideas, objects, conditions, or situations, which can be compiled to be processed in the form of data structures, file structures, and databases.

Along with the development of data collection methods, various data type variables, among other things, are primary-secondary data, qualitative-quantitative data, and personal data emerged automatically. Especially in the context of personal data, nowadays, every country worldwide uses different terms between "personal information" and "personal data". However, substantively, the two terms have almost the same meaning, so the two terms are often used interchangeably. The United States, Canada, and Australia use the term personally identifiable information (PII) (Rosadi, 2009), while countries in Europe and Indonesia use the term personal data. Thus, for the purposes of this paper, the authors refer to the term personal data.

Furthermore, it is not only the use of different terms (OECD Guideline 1980). Based on the above research results, the personal data of consumers in Indonesia is still not protected so that, in line with the OECD's interpretation that sees personal data as identified or identifiable information regarding a person's personal, the conception of personal data adopted by the European Union and the OECD can be used a reference for Indonesia in drafting the Law on Personal Data Protection. Indonesia also can refer to the concept of personal data as outlined

in Article 1 paragraph (1) of the following Draft Law on Personal Data Protection, stating that "personal data is any data that is identified and/or identifiable, either directly or indirectly via electronic or non-electronic." Although referring to the two instruments mentioned above, in fact, the content related to the conception of personal data in the Draft Law on Personal Data Protection is different from one another. In the Draft Law on Personal Data Protection, added values are not found in legal instruments in the European Union and OECD.

The provisions of the Draft Law on Personal Data Protection expressly contain a clause "either directly or indirectly" and provide a limit on personal data whether formed "through electronic or non-electronic [means]." A comprehensive understanding of this added value is absolutely necessary so that the meaning of personal data is not obscure. Apart from the Draft Law on Personal Data Protection, the conception of personal data is interpreted differently by Article 1 paragraph (27) of Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions (PP PSTE). The regulation defines data as certain individual data stored, maintained, and kept and its confidentiality protected. In terms of personal data protection, at least two methods are known to protect personal data, namely, first by physically safeguarding the personal data itself. In addition, the second method that can be taken to protect personal data is through the regulatory side, which aims to guarantee privacy against the use of personal data.

Regarding the second method, history has recorded that personal data protection or known as "data protection," was first used in laws in several countries in mainland Europe, namely Germany, Sweden, and France, in the 1970s. The personal data protection in several countries is entirely based on the urge to guarantee the right to privacy of each individual against such data, in line with the development of information and communication technology, and then the scope of its regulation extends to the public administration aspects.

CONCLUSION

In this study, concerns of internet service users about the insecurity of SMS/internet banking in Indonesia were not followed by awareness to explore further the regulations governing personal data protection. Entering personal data into applications or online applications should be done with awareness and understanding of the risks. However, understanding the risks was not followed by understanding the user's privacy policy in every online service used. Awareness of the importance of privacy was also not followed by an

awareness of maintaining privacy in online applications or services (backup data or changing passwords regularly). Besides, awareness of the importance of privacy was not accompanied by a desire to know the regulations governing personal data. The security of SMS/internet banking or e-commerce in Indonesia was also not accompanied by efforts to avoid misuse of personal data. This lack of awareness to protect privacy occurred since users had not experienced the abuse of personal data on online applications or services. In other words, consumers' personal data in Indonesia is still unprotected. Therefore, in line with the OECD's interpretation of seeing personal data as identified or identifiable information regarding a person's personal details, the conception of personal data adopted by the European Union and OECD can be used as a reference for Indonesia in making the draft Law on Protection of Personal Data. Through the National Cyber and Crypto Agency, the government is obliged to encourage cyber security education in the community. It is because, in big cities, awareness of cybersecurity risks exists but has not been followed by preventive steps by the community itself. Through the National Cyber and Crypto Agency, the government must also standardize cybersecurity, especially for state institutions, banking, and other strategic sectors in the country, to ensure security for the public. Concerning this, there needs to be a cultural approach by including cybersecurity education early.

REFERENCES

Annur, C. M. (2020). Zoomboombing terjadi di RI, rapat online disuguhi foto & video porno (Zoombombing happened in Indonesia, pornographic photos and videos were sent during online meeting). Retrieved from: https://katadata.co.id/berita/2020/04/16/zoomboombing-terjadi-di-ri-rapat-online-disuguhi-foto-video-porno

Annur, C. M. (2020). Data 500 ribu lebih akun zoom dijual di dark web dan forum peretas (The data of more than 500 zoom accounts were sold in the dark web and in hacker forums). Retrieved from: https://katadata.co.id/berita/2020/04/16/data-500-ribu-lebih-akun-zoom-dijual-di-dark-web-dan-forum-peretas

Annur, C. M. (2020). Indonesia menjadi target phishing tertinggi di ASEAN (Indonesia becomes the highest phishing target in ASEAN). Retrieved from: https://databoks.katadata.co.id/datapublish/2020/09/28/indonesia-menjadi-target-phishing-tertinggi-di-asean#

CISSReC. (2017). Tingkat kesadaran masyarakat tentang keamanan informasi (The people's awareness level on information security). Retrieved from: https://www.cissrec.org/download.html

Clapp, R. (2020). E-Commerce Shopping More Frequent because of COVID-19. Retrieved from: https://www.warc.com/content/paywall/article/WARC

Diggelmann, O. & Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review, 14*.

Djafar, W. & Santoso, M. J. (2019). *Perlindungan data pribadi mengenali hak-hak subjek data, serta kewajiban pengendali dan prosesor data (Personal data protection, knowing the rights of data subjects and the obligations of data controllers and processors).* South Jakarta: Lembaga Studi dan Advokasi Masyarakat (LSAM) and Australian Government Department of Foreign Affairs and Trade (DFAT).

EC Data Protection Working Party. (2011). Geolocation Services on Smart Mobile Devices. Retrieved from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pd

Gellert, R. (2015). Understanding data protection as risk regulation. *Journal of Internet Law, 18*(11).

Krishnan, A. (2020). COVID-19 and the new normal for e-commerce. Retrieved from: https://securityboulevard.com/2020/05/covid-19-and-the-new-normal-for-e-commerce

Kumparan. (2020). *15 juta data pengguna dilaporkan bocor, Tokopedia akui ada upaya pencurian (15 million user data were reported to be leaked, Tokopedia admits there is an attempted theft).* Retrieved from: https://kumparan.com/kumparantech/15-juta-data-pengguna-tokopedia-dilaporkan-bocor-1tL0ntUNJEX/full

Lubis, A & Siahaan, A. P. U. (2016). Network forensic application in general cases. *IOSR Journal of Computer, 18*(6), 41–44.

Nasution, M. D. T. P., Siahaan, A. P. U., Rossanty, Y., Aryza, S. (2018). The phenomenon of cyber crime and fraud victimization in online shop. *International Journal of Civil Engineering and Technology (IJCIET), 9*(6), 1583–1592. Article ID: IJCIET_09_06_178 Retrieved from: http://www.iaeme.com/ijciet/issues.asp?JType=IJCIET&VType=9&IType=6

Pertiwi, W. K. (2020). *Hacker klaim punya data 1,2 juta pengguna Bhinneka.com (Hacker claims to own 1,2 million user data of Bhinneka.com).* Retrieved from:

https://tekno.kompas.com/read/2020/05/10/21120067/hacker-klaim-punya-data-12-juta-pengguna-bhinnekacom

Rosadi, S. D. (2009). *CyberLaw: perlindungan privasi atas informasi pribadi dalam e-commerce menurut hukum internasional (CyberLaw: privacy protection on personal information in e-commerce according to international law).* Bandung: Widya Padjadjaran.

Salim et al. (2017). Legal research of doctrinal and non-doctrinal. *International Journal of Trend in Research and Development, 4*(1). ISSN: 2394-9333.

Schwartz, P. M. & Solove, D. J. (2011). The PII problem: privacy and a new concept of personally identifiable information. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1790262

Wardoyo, S. (2020). Corona & PSBB untungkan e-commerce RI, benarkah? (Do corona and large-scale social restrictions bring profit to Indonesian e-commerce?). Retrieved from: https://www.cnbcindonesia.com/tech/20200505181156-37-156534/corona-psbb-untungkan-e-commerce-ri-benarkah