ALSA
ASIAN LAW STUDENTS' ASSOCIATION

VOLUME 9 • ISSUE NO. 1

ALSA LAW REVIEW MAGAZINE

PERSONAL DATA PROTECTION

JULY 2021

ASIAN LAW STUDENTS' ASSOCIATION

ALSA LAW REVIEW MAGAZINE

VOLUME 9 • ISSUE NO. 1

The ALSA Law Review Magazine (ALRM) is a student-edited academic law journal published by ALSA. ALRM aims to enhance the understanding of various nations' point-of-view on a particular legal issue. ALRM also endeavours to be a platform for ALSA members to improve their research and writing skills by engaging in dialogue regarding current legal issues of international interest. It serves to broaden the knowledge of readers including law students, with regards to the legal issues in Asia.

EDITORIAL ADRESS
Secretary Office of ALSA International
Faculty of Law Universitas Indonesia
Universitas Indonesia,16424, Indonesia, Kampus UI Depok
alsainternational.org

GREETINGS!

Griselda Audrey Chandra

President of
ALSA International Board
2020/2021

Greetings from ALSA International!

I am Audrey, the President of ALSA International Board 2020/21. I proudly present the first ALRM on "Personal Data Protection". Data privacy has always been important. It's why people put locks on filing cabinets and rent safety deposit boxes at their banks. But as more of our data becomes digitized, and we share more information online, data privacy is taking on greater importance. Data privacy isn't just a business concern. You, as an individual, have a lot at stake when it comes to data privacy. The more you know about it, the better able you'll be to help protect yourself from a large number of risks.

I also would like to thank the contributors for your outstanding works and for those who have not contributed yet, I am looking forward to seeing your active contribution.

Strong Inside and Leading Outside

ALSA, Always Be One

Greetings ALSA members far and wide!

As neighboring countries, we should be attentive toward the problems, changes, and advancements experienced in each country to serve as examples, lessons, and even precedences in order to advance toward a better Asia. This ALRM serves to bring you an analysis on the issue of Personal Data Protection in Asia.

We hope you are immersed and able to gain a new legal perspective through this publication.

Warm Regards,
Vishnu

Vishnu Varna

Vice President of
Academic Activities of
ALSA International Board
2020/2021

GREETINGS!

Nasya Ayudianti Ramadhani

Director of
Academic Publication of
ALSA International Board
2020/2021

Greetings from ALSA International!

In the digital era where access to information becomes easier, the issue of data privacy naturally arises. With the fast development of technology, there needs to be an adequate development of legal instruments, to protect said data privacy. That is why the theme of Personal Data Protection is chosen for this ALRM to further understand the current legal instrument of personal data protection from diverse countries in Asia.

Thank you for the author's contribution to the law review magazine.

ALSA, Always Be One!

"Civilization is the progress of a society towards privacy" -Ayn Rand

In the current technological zeitgeist, where information is not just conveniently disseminated and accessed but also transformed and commodified, there is a question of how such openness of information interplays with the fundamental right of privacy. The articles in this issue of ALSA Law Review explores how the various Asian jurisdictions address this question and offer nuanced legal perspectives on the ever-evolving concept of personal data privacy.

Franz Albert Lantin

Senior Editor of
ALSA Editorial Board
2020/2021

Antonio Castillo

Senior Editor of
ALSA Editorial Board
2020/2021

Greetings from ALSA International!

I would like to thank all contributors of ALRM for their hard work and participation in submitting the article.

We look forward to your contribution towards other ALSA academic publications!

ALSA, Always Be One!

GREETINGS!

Aaron Tan Kai Ran
Senior Editor of
ALSA Editorial Board
2020/2021

Greetings from ALSA International!

Hi everyone! I am happy to present to you the ALRM!

This edition features a collection of thoughtful pieces on personal data protection that the team feels captures a wide breadth of commentary on the subject. Personal data protection is a constantly growing and evolving issue and I hope you can take away as much I have from these articles!

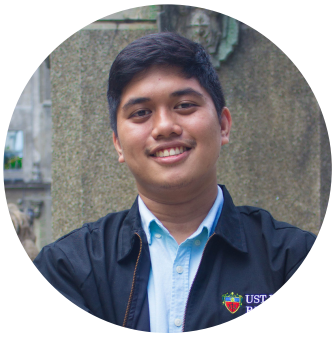
ALSA, Always Be One!

Greetings from ALSA International!

I hope that reading this magazine will have an impact on and encourage you to have an impact on others. We may never know how much our words or actions influence the lives of those around us, but we can choose daily to be a positive influence on others in a way that could change the rest of their lives even if it is just within the walls of where you work.

ALSA, Always Be One!

M. Izzhar Aiman Bin Hamdan
Senior Editor of
ALSA Editorial Board
2020/2021



Jyrus Buban Cimatu
Senior Editor of
ALSA Editorial Board
2020/2021

Greetings from ALSA International!

The process of publishing ALSA Law Review Magazine has been a very eventful one and I hope everyone enjoys this academic publication. Thank you very much to all authors of ALRM who have dedicated their time and effort in contributing to the publications.

ALSA, Always Be One!

ALRM REVIEWERS

1. **Dr. Izura Masdina**
   Faculty of Law, Universitas Malaya, Malaysia.
2. **Mr. Fajri Matahati Muhammadin, S.H., LL.M., Ph.D.**
   Faculty of Law, Universitas Gadjah Mada, Indonesia.
3. **Mr. Romel Bagares**
   Lyceum of the Philippines University College of Law, The Philippines.
4. **Dr. Syahirah Shukor**
   Faculty of Law, Universiti Sains Islam, Malaysia.

TABLE OF CONTENTS

THE CHALLENGES OF PERSONAL DATA PROTECTION AND PUBLIC INFORMATION DISCLOSURE IN INDONESIA

By Ridea Oktavia

This paper discusses the challenges of protecting personal data and public information disclosure in Indonesia. This paper examines extensively the challenges in ensuring the protection of personal data in Indonesia. This article will give readers an understanding of how important it is to maintain personal privacy in order to avoid the impact of the misuse of personal data which is very detrimental to the victim. The research undertaken to compile this paper is normative juridical research, based on primary data in the form of legislation, namely the Republic of Indonesia Law 1945 and the Law on Public Information Openness, and the secondary data, namely academic papers and journals. The data analysis was carried out by using a qualitative approach, namely the analysis that was formed indirectly in the form of statements and writing. Conclusions are drawn using deductive logic by analyzing the challenges of protecting personal data and their relation to public openness. Based on the results of the analysis, it can be concluded that the main challenge of protecting personal data lies in public understanding and awareness of the privacy data itself. The openness of public information basically has an objective that is mutually exclusive from and complementary to the protection of personal data, even though in its implementation there are clashes, therefore it is important to harmonize the regulations, both on the side of personal data protection and on the side of openness of public information so that it does not conflict in the future.

BACKGROUND

The development of information technology today is much different and very fast compared to its early days. The era of globalization has placed information technology in a very important position because it presents a world without borders, time and space and can increase productivity and efficiency. Information technology has changed the attitudes and behavior of people globally which has led to significant changes in the economic, socio-cultural, and legal framework.[1]

The role of technology is an inseparable part of all aspects of human life. In almost all activities, humans take advantage of technology, both simple technologies, and very sophisticated ones; even current technological developments can change the way or pattern of communication in the

[1] Ahmad M. Ramli, Cyber Law and Intellectual Property Rights in the Indonesian Legal System, Bandung: Armico, 1 (2013).

public. Communication is made easier with the internet through social media that can be accessed by all groups. This certainly has the potential for data misuse during interaction between social media users. For example, this can happen when personal data of a social media user is used by other parties who are considered to be disturbing and endanger the owner of the personal data himself.

In recent years, the right to privacy protection has become a subject that has been to be discussed in depth among academics, governments, and human rights activists. Discussions on the right to privacy protection surfaced with the widespread use of information technology and demands for information and data disclosure, especially those concerning information and data controlled by government agencies.

In the Indonesian context, privacy protection has actually been recognized for a long time. At least the Criminal Code contains several articles of criminal acts related to privacy, such as the prohibition of opening documents,[2] the prohibition of entering private land or property,[3] and other crimes related to occupation.[4] Although it has been around for a long time, only on August 18, 2000, did protection of the right to privacy become part of constitutional protection.[5]

The government's efforts to disclose its information and data deserve to be well appreciated, because disclosure can also suppress corruption in the public sector. But at the same time, openness also creates a conflict of interests, namely the interest of openness with the interest of protecting the right to privacy. Law No. 14 of 2008 on Freedom of Information also puts special emphasis on personal information and data that are classified as exempt information.[6] For this reason, these two rights must be balanced by making regulations or policies that protect information disclosure while also protecting the right to privacy.

ANALYSIS

The development of information technology today opens up great opportunities to obtain personal data information, but it also has a high potential for opportunities to violate the privacy rights of people in society. Threats occur not only due to the global development of information technology but also the resultant blurring of boundaries between national jurisdictions. Current developments also allow the transfer from one form of data to another.[7] On the other hand, information disclosure and the right to privacy are two important things that go hand in hand, and both play an important role in making the government responsible to its citizens.

Sociologically, Indonesian people are very open to personal information. The low level of public understanding regarding personal data privacy is the main reason. The Ministry of Communication and Informatics (Kominfo) found that public awareness of personal data is still lacking, even as 93 percent of the public shares their personal data digitally, through social media.[8] This has

[2] Criminal Code of Indonesia, art. 431.
[3] Criminal Code of Indonesia, art. 167(1).
[4] Criminal Code of Indonesia, Chapter XXVIII concerning Crimes of Position.
[5] 1945 Constitution of the Republic of Indonesia, art. 28G.
[6] Law No. 14 (2008) concerning Freedom of Information, art. 17(g) & (h).
[7] Electronic Privacy Information Center & Privacy International, Privacy and Human Rights: An International Survey of Privacy Laws and Practices, 4 (2006).
[8] Kominfo, Lindungi Data Pribadi, Jangan Pasang Aplikasi Sembarangan! (2020) *available at* https://www.kominfo.go.id/content/detail/28293/lind

the potential for misuse of personal data by irresponsible persons. Examples include submitting a loan request with someone else's identity, online fraud using a stolen identity, and other heinous acts.

However, the public generally has not placed personal data as part of the property that must be protected. This can be seen from the number of posts containing personal data content, both on a number of social media platforms as well as in various social networking groups. In addition, when using a number of electronic system platforms (e-commerce, online transportation, fintech, etc.), users generally do not fully understand the privacy policy, terms and conditions of service of each of these applications, especially those related to use of personal data. Protection of personal data is very important because if it is misused by data providers or third parties, then this can conflict with basic human rights to obtain privacy protection for personal data as well as losses arising from the misuse of data by these individuals. Unfortunately, the need for comprehensive personal data protection regulations has not been accompanied by a growing public awareness in protecting personal data.

In addition, if we look at the issue juridically, Article 28F and Article 28G(1) of the 1945 Republic of Indonesia Law apparently contradict. Article 28F reads:

> "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia".[9]

This article gives freedom to everyone to obtain information and even has the right to store, process and convey information. In contrast, Article 28G(1) reads:

> "Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuai yang merupakan hak asasi."[10]

In the article, it is stated that every person has the right to personal protection, including protection of data privacy. The next conflict is between article 28F which states the right of a person to obtain information, with the provisions of Article 28H paragraph (4) which regulates the provisions regarding the right to have personal rights where these rights cannot be taken arbitrarily. This personal right includes the right to a person's personal data. Thus there is a potential conflict between the right to information and the right to privacy in its implementation aspect. On one hand, the right to information prioritizes the individual's freedom to seek all the information he wants; on the other hand, the right to privacy exists and limits the space for individuals to seek certain information about a person's personal data. This certainly creates multiple interpretations and regulatory weaknesses, because the law does not state clear boundaries regarding what and who has the right to obtain, own, store, manage one's

ungi-data-pribadi-jangan-pasang-aplikasi-sembarangan/0/berita_satker (last visited July 7, 2021).

[9] 1945 Constitution of the Republic of Indonesia, art. 28F.

[10] 1945 Constitution of the Republic of Indonesia, art. 28G(1).

personal data, so this is a great opportunity for individuals to misuse someone's personal data. Therefore, both must be limited and implemented in a balanced manner for the realization of security and convenience of interaction between the government and citizens and among fellow citizens.[11] Limitation can be done by making a legal product in the form of a law that contains more detailed regulations related to the protection of personal data, where this regulation will clearly and precisely determine the restrictions so as not to create ambiguity, this is the urgency of the enactment of the Personal Data Protection.

CONCLUSION

Based on the results of the above analysis, the authors conclude that there are several challenges in protecting personal data and public information disclosure in Indonesia. First, the public is very open to personal information, especially on social media. The low public awareness of personal data privacy is one of the main causes and challenges, so it is necessary to increase the literacy of personal data protection to provide understanding as to what kind of data can be shared and vice versa and the impact in the event of misuse of personal data.

Second, at the constitutional level there are several clauses that have contradictory meanings, namely in article 28F, 28G paragraph (1), and 28H paragraph (4) of the 1945 Constitution of the Republic of Indonesia. Article 28F provides for the freedom to obtain information and the right to obtain information to store, process and convey information; however, Article 28G paragraph (1) states that everyone has the right to personal protection, including protection of privacy data. Furthermore, Article 28H paragraph (4) regulates the provisions regarding the right to have personal rights where these rights cannot be taken arbitrarily, which includes the right to personal data. This raises ambiguity because the articles do not include clear limitations and open up greater opportunities regarding the misuse of someone's personal data which of course causes harm to the victim. Therefore, it is important to provide limitations on a provision so that regulations can be understood and can be firmly enforced. The way that can be done for this restriction is to legalize the Draft Law on Personal Data Protection so that it has a standard and comprehensive rule to ensure the protection of personal data of Indonesian citizens.

[11] Dani Primary Huzaini, Kebebasan Informasi Versus Hak Warga Negara atas Privasi (2018), *available at* https://www.hukumonline.com/berita/baca/lt5a810824d134a/kebebasan-informasi-versus-hak (last visited July 7, 2021).

DUAL CHALLENGES IN KOREA ARISING FROM CURRENT DATA GOVERNANCE REGULATIONS

By Bo Hyun Kim

1. INTRODUCTION

The National Assembly passed amendments to Korea's three main data privacy laws (effective August 5, 2020), paving the way for a digital economy under the Moon administration's Korean New Deal plans. Marking a shift from previously stringent regulations, such changes appear to be highly beneficial. They create favorable regulatory conditions for the domestic data market, whose growth had been sluggish compared to its global counterparts.

However, recent events have raised tides of concern regarding data governance. It began with the data leak dispute involving 5 million users from Korea's popular GPS location service, Kakao Map. The second tide surged when Luda, a deep learning AI chatbot, collected without the consent of 10 billion user conversations on Kakao Talk, the nation's no. 1 messenger application. Against this backdrop, the challenge here is two-fold. On the domestic level, there are several questions that have to be answered. What constitutes 'reasonable grounds' for personal data use without the data subject's express consent under the amendments? What is the scope of 'personal information' within the meaning of current privacy laws? On the international level, what are the implications of the amendments on the ongoing EU-Korea dialogue related to the EU's adequacy decision?

This article seeks to offer a framework for answering the above questions. First, it will provide a tour d'horizon of the current stance of the three main Korean data privacy laws. Second, it will examine whether recent controversies can be adequately addressed by existing normative regulations. Lastly, it will provide proposals to foster accountability of data-driven sectors without subjecting them to unduly burdensome compliance of privacy laws.

2. RECENT AMENDMENTS TO THE THREE MAJOR DATA PRIVACY LAWS

Korea's three major data privacy laws are: the Personal Information Protection Act ("PIPA"), the Act on Promotion of Information and Communications Network Utilization and Information Protection ("Network Act"), and the Credit Information Use and Protection Act ("Credit Information Act").

2.1. General Legislation: the PIPA

The PIPA is a general legislation that purports to regulate the use of data by prescribing the processing and protection of personal

information. Under the amendments, the PIPA conferred centralized power to the Personal Information Protection Commission ("PIPC"), elevating its status to an independent, ministerial-level regulatory body under the auspices of the Prime Minister's Office. The PIPC (i) implements and facilitates consultation on personal information protection among pertinent central administrative agencies, (ii) assesses data breach incident factors and investigates violations, (iii) imposes payment of penalty surcharges on the violator as necessary, (iv) develops guidelines on implementation plans, sub-plans by sector, policies, etc. related to personal information protection, and (v) oversees the Dispute Mediation Committee charged with mediating and settling individual and collective disputes related to personal information.[12]

Another principal amendment to the PIPA is that it permits data controllers' use of personal data without the data subject's consent 'within a scope reasonably related to the initial purpose of collection.'[13] The ambiguity underlying this language regarding the extent of reasonable scope of data use without consent implicates interpretative questions as will be discussed in later sections. Also noteworthy are the special provisions regarding the processing of anonymized information under the PIPA. Anonymized information refers to personal information processed in a way that the data is no longer identifiable to an individual without some use or combination of additional information. Such data may only be used without the data subjects' consent for statistical information, scientific research, or for public record keeping and does not extend to use for commercial or business purposes. While the concept of anonymized data purports to foster flexible data use, it is not without attendant risks because mischaracterization of 'personal data' as 'anonymized data' may subject the violator to criminal sanctions, such as fines up to 3% of its total revenue.[14]

2.2. Sector-Specific Legislations: The Network Act and the Credit Information Act

The Network Act and the Credit Information Act pertain to sector-specific data protection legislations. The Network Act previously included provisions governing personal data protection by information and communications service providers. However, such provisions were transferred to the PIPA after the amendment.[15] Finally, the Credit Information Act, which was enacted to establish sound credit transactions by promoting efficient management and preventing misuse of credit information, saw an expansion in its scope of applicability to encompass not only financial institutions, but also all commercial companies under the amendments.[16] Such extensive changes seem to be a conscious response to achieving compliance with the GDPR, which the Korean data privacy regulatory framework is modeled after.

3. THREE ISSUES RAISED BY THE KAKAO MAP AND LUDA CONTROVERSIES

Pertaining to the aforementioned Kakao Map and Luda controversies, a review of case law reveals an absence of precedents on (1) the requisite specificity of language and proper

[12] Act No. 16930 of the Republic of Korea (2020), art.7
[13] *Id.* at art. 15(1)(6)
[14] *Id.* at art. 28-6(1).
[15] Act No. 16930 of the Republic of Korea (2020), Ch. VI.
[16] Exec. Order No. 17354 of the Republic of Korea (2020).

means of obtaining users' consent in collecting personal information; (2) the interpretation of 'reasonable scope'[17] for collecting personal data without express consent; and (3) the scope of 'personal information' within the meaning of current data privacy laws. These three issues will be examined in connection with the two events, followed by an analysis in light of current legislations and pertinent case law.

3.1. The Concept of 'Proper Means' of Obtaining Users' Consent

First, the Kakao Map controversy illustrates grey areas arising from questionable consent clothed with a "fig leaf." Kakao Map Favorites, a popular feature of the location service application, allows users to save frequently visited sites, such as their workplaces, children's schools, friends' homes, and favorite restaurants. Following the leak of data collected from the feature, Kakao Map denied having violated any personal information protection laws on grounds that they had provided clear guidelines before obtaining users' permission to collect such data.[18]

However, Kakao Map users pointed out that the verification message regarding the disclosure of information for public access may be inconspicuous or hardly recognizable depending on users' mobile phone displays.[19] When saving a place on the application for the first time, the application generates a pop-up window seeking consent that may not be immediately visible if, for instance, it is covered by keyboard layouts. Accordingly, the oblivious user that swipes "next" would automatically be subjected to the default setting allowing disclosure of its information.[20] Hence, this raises the first point as to whether the service provider's specific method of collecting information was explicit and in a manner easily identifiable by average users.

3.2. The Interpretation of 'Reasonable Scope' of Collecting Personal Data and 'Personal Information' under the PIPA

Likewise, the Luda controversy invokes the second and third issues on statutory interpretation. The initial input data for the conversational AI Chatbot, Luda, was based on conversation patterns between young couples from actual KakaoTalk message data retrieved from the application, Science of Love launched by Scatter Lab, Luda's developer. Launched in 2016, Science of Love provides dating advice by analyzing the degree of affection between its users as manifested in their text exchanges.[21] Catter Lab apologized, commenting that it had attempted to adhere to guidelines for personal information use but did not "sufficiently communicate" with its data subjects which amounted to 750,000 users since its launch.[22] Scatter Lab further stated that in developing the chatbot, it had admittedly failed to remove all personal data depending on the context, despite efforts to render all data unidentifiable to individual users by removing sensitive personal

[17] Act No. 16930 of the Republic of Korea (2020), art. 15(1)(6).
[18] Hae-yeon Kim, Kakao Map faces user data leak dispute, The Korea Herald (Jan. 15, 2021, 5:42 PM), http://www.koreaherald.com/view.php?ud=20210115000801.
[19] *Id.*
[20] *Id.*
[21] Eun-jung Kim, (News Focus) Chatbot Luda controversy leave questions over AI ethics, data collection, Yonhap News Agency (Jan. 13, 2021, 2:22 PM), https://en.yna.co.kr/view/AEN20210113004100320.
[22] *Id.*

information (names, addresses, phones numbers) via filtering algorithms.[23]

Accordingly, Scatter Lab utilized such data without notice and prior consent from users to channel their data into developing its new AI chatbot business. Thus, this addresses the first and second issues regarding the specificity of language or lack thereof in obtaining users' consent and in assessing justifiable grounds proffered by businesses in interpreting the 'reasonable scope' of personal data collection without express consent.

Moreover, although Scatter Lab has obtained comprehensive consent from end users regarding personal information use for marketing and advertising purposes, its failure to obtain consent for personal information use from a third party that does not use its services may constitute an invasion of privacy. This is because in transmissions of electronic communications data, a chat room participant on the other end of the conversation may be as much a data subject as the chat user from which express consent has been obtained.[24] Therefore, this directly relates to the third issue: defining 'personal information' within the meaning of current privacy laws and whether it encompasses such third parties that could inevitably be involved, depending on sector-specific treatment of data. At present, there is no relevant case law. However, ascertaining whether collecting data without consent from chat room participants on the other end of the conversation thread likewise brings it within the proscriptions of the PIPA is a matter warranting attention for service providers.

4. SEEKING THE DATA SUBJECT'S CONSENT AND CONSTRUING "FRAUD, IMPROPER OR UNJUST MEANS" AS DEFINED IN THE HOMEPLUS CASE

4.1 The Homeplus Case and its Analytical Framework

Notwithstanding the absence of a case in point, the Homeplus case[25] may shed some light, suggesting the determinative issue to be whether information was acquired by "fraud, improper or unjust means" in violation of Article 59 of PIPA.[26] In Homeplus, the defendant, Homeplus Co., Ltd. organized 11 giveaway events from 2011 to 2014, collecting 7.12 million items of personal information, of which roughly 6 million items were sold to third party insurance companies for KRW 11.9 billion. Prizes for the giveaways ranged from a Mercedes-Benz car, a diamond ring, to Samsung air conditioners. The defendant advertised the event via multiple channels of marketing such as fliers, online channels, and even receipts. The advertisements included images of the prizes along with the phrases, "14th anniversary festival," "celebration of the group's 5th anniversary," "rooting for victory in the Brazil World Cup Games," etc. Raffle tickets for the events printed details in 1mm-sized font the following provisions: "[Consent to Collection, Management, Entrustment, and Use of Personal Information] The purpose of the collection and use of personal information is to send notices on giveaway events and winners, provide information for insurance marketing

[23] *Id.*

[24] In Hae Sohn, '개인정보 유출 논란' 이루다 개발사, '고지·안전조치 의무 위반' 쟁점[Developer of Luda mired in 'dispute over personal information leak' faced with 'violations of notification requirements and procedural safeguards'], News1 (Jan. 15, 2021, 7:20 AM), https://news1.kr/articles/?4181567.

[25] 2016Do13263, Supreme Court Library of Korea (2017).

[26] Act No. 16930 of the Republic of Korea (202), art. 59(1).

purposes, and promote products and services of the company's partners."[27]

The barely legible fine print on the back of the raffle tickets and promotional website included a "[Provision of Personal Information to Third Parties]" listing recipients of the personal information and informing customers that the information collected "will be used for marketing purposes such as telephone marketing of insurance products."[28] The acquired information was sold for KRW 1,980 each, pursuant to a business partnership agreement with two insurance companies.

The Court held that despite seeking consent in acquiring and managing personal information from its customers, the defendant had used "fraud or unjust means" to do so under Article 72(2) of the PIPA.[29] Hence, its conduct constituted a violation of the PIPA when it acted with a hidden intent to collect and sell its customers' personal information to insurance companies for a price, rather than for legitimate purposes such as increasing sales by attracting a wider customer base. It reasoned that the defendant (a) printed the details related to personal information collection and management in barely readable 1mm-sized font; (b) took full advantage of the hectic atmosphere during the period of the event to lure participants with images of expensive prizes on its advertisements; and (c) had participants provide consent without knowledge of the third party provision regarding information acquisition and management, deceiving or misleading customers into perceiving it as a mere thank-you event.[30]

Moreover, the Homeplus Court established that a personal information manager's act of seeking consent thereof should not be the sole factor in determining the use of false or other unlawful means to obtain consent on acquisition or management of personal information. Rather, it provided a non-exhaustive list of factors to take into account when examining the personal information manager's obtaining consent:

> (i) motive and purpose of collecting, etc. personal information; (ii) relevance between the purpose of collection and personal information to be collected; (iii) specific method used to collect, etc. personal information; (iv) compliance with relevant statutes such as the PIPA; and (v) contents and volume of personal information acquired, namely, whether sensitive and unique identification information were acquired.[31]

Thus, such a list of inquiries laid the foundation for further expansion in progeny cases.

4.2 Implications of the Homeplus Case on the Two Controversies

Applied here, the lack of an easily identifiable method of personal information collection in the Kakao Map controversy; the attenuated relevance between the initial purpose of collection and subsequent use of personal information in the Luda controversy; and Homeplus' transfer of personal information collected under the pretense of a giveaway event may all constitute failure to obtain lawful consent without justifiable grounds.

[27] 2016Do13263, Supreme Court Library of Korea (2017).
[28] *Supra,* note 16, at Na(2)(4).
[29] *Id.* at Na(3)(3).
[30] *Id.*
[31] *Id.*, at Na(1).

4.2.1 Reflecting on Active Consent and Consumer Sovereignty through Kakao Map

In Homeplus, the barely legible 1mm-sized fine print on the back of raffle tickets was one of the pertinent factors in the Court's decision. This is because the provision of personal information to third parties (i.e. insurance companies) was a critical element that could have influenced a consumer's decision to participate or not in the giveaway event.[32] Likewise, due to the lack of visibility of the pop-up window verifying consent, Kakao Map users had unwittingly consented to disclosing their personal information for public access. Had the message been clearly disclosed and communicated to consumers, it would have prevented them from blindly proceeding to the next step in using the application feature. Such a method of obtaining consent seemingly falls short of an explicit method average users can easily identify with, or one that would ensure them that their personal information would be collected based on their express consent.[33]

Further, the fact that the default setting was preconfigured to allow public disclosure of information even without users' active consent is a point of concern. In response, Kakao Map raised the defense that location data pertains to information open to any member of the public, and that information added to the list of favorite places would not necessarily fall under personal information because location data alone, without more, cannot be used to identify an individual. Nevertheless, Kakao Map proceeded to change its default settings to private shortly thereafter. Some professionals and users opined that depending on the circumstances, location data may also be used to identify individual users;[34] Hence, location data would also fall within the scope of personal information. As such, adopting regulations or platforms enabling consumer sovereignty in data processing like Personal Information Management Systems (PIMS) may be a prudent solution to privacy issues companies face in their current data management practices in their roles as data collectors.

Meanwhile, regulations such as the EU GDPR require privacy by default, ensuring that only the data necessary to achieve the purpose specified and informed beforehand is disclosed, while minimizing accessibility to personal data. Cases such as Planet 49 GMBH[35] are illustrative of this point. There, an internet user was confronted with two checkboxes before pressing the 'participation button' in order to participate in a lottery organized by Planet49.[36] The pre-checked boxes required the user to accept contact for promotional offers and to consent to the installation of cookies, which the user left checked per the default setting. The Court of Justice of the European Union ("CJEU") dealt with the issue of whether the user's action of leaving the boxes checked could be deemed consent. The CJEU found there was no "valid consent" under Articles 2(f) and 5(3) of the e-Privacy Directive[37] of the European Parliament. It emphasized consent as a feature underlying EU data protection

[32] *Supra,* note 16, at Na(3)(1).
[33] 2014Du2638, Supreme Court Library of Korea (2016).
[34] Jong Hyun Lee, 이루다,카카오맵 개인정보 유출…데이터 활용 기조가 흔들린다 [Luda and Kakao Map Personal Information Leaks…Shifting Trends in Data Use], Digital Daily (Jan. 19, 2021) http://www.ddaily.co.kr/news/article/?no=208085.
[35] Case C-673/17, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V., ECLI:EU:2019:801 (Mar. 21, 2019).
[36] *Id.* at paras. 26-28.
[37] Directive 2002/58/EC, arts. 2(f), 5(3), 2002 O.J. (L 201) 43, 44.

law, which stipulates that the data subject indicates its wishes with active, rather than passive behavior, such that it has unambiguously given consent.[38] Thus, the user's declaration of consent was found insufficient because it had been pre-formulated.

In light of the fundamental principles of personal information protection prescribed by the GDPR, it may seem reasonable to implement measures ensuring that the strictest privacy settings apply by default. On the other hand, industry professionals have also pointed out that 'opt-out' methods, wherein users provide comprehensive consent while objecting to use of data for certain purposes, have proven more advantageous for big data service providers launching new services.[39] This is because the current big data era inevitably relies upon tailored content created by amalgamating different data. Considering this, subjecting domestic businesses to regulations differing from their global counterparts may decrease their competitiveness in the market.[40]

4.2.2 Luda and the Collection of Information Disparate from its Original Purpose

The Homeplus case suggests that the mere seeking of consent in obtaining personal information for the possibility of using collected data to develop new services may not be able to take the case out of the proscriptions of the PIPA. Homeplus sought consent and obtained personal information under the pretenses of giving away free prizes as part of a consumer appreciation event. Likewise, Scatter Lab collected personal information like the users' name, sex, age, marriage status, which users had deemed to be purely for purposes of providing paid dating advice.[41] While Scatter Lab did include a minor provision informing users their information would also be used for purposes of developing new services and marketing, the provision was ambiguous on its face regarding the possibility of utilizing their personal chat room data as the basis of a deep-learning algorithm platform.[42] This is because it may be found to have misled Science of Love users by collecting and reusing such information for a purpose disparate from its original one. Consequently, such practices may constitute "a violation of the principle of safe-guarding personal information and relevant obligations under the PIPA...as well as relevant provisions under the PIPA which provide for a personal information manager to collect only the minimum information necessary to achieve the relevant purpose … ".[43]

Because the aforementioned issues have yet to be adequately addressed by the Korean judiciary, it is expected that seminal precedents will be established for future cases, should the two much-debated incidents proceed to court.

[38] *Id.* at para. 52.
[39] Mi Seon Kang et al., 동의 받으면 또 동의 버튼, 국내기업은 괴롭다 [Consent after consent, a hassle for domestic businesses], Money Today (Oct. 4, 2019, 4:30 AM), https://news.mt.co.kr/mtview.php?no=2019100319315152455.
[40] *Id.*
[41] Min Seon Kim, 개인정보 유출 논란 '이루다' DB 및 대화 모델 폐기 ['Luda' to discard DB and deep learning algorithms after personal information leak], ZDNetKorea (Jan. 15, 2021, 2:23 PM), https://zdnet.co.kr/view/?no=20210115114216.
[42] *Id.*
[43] 2016Do13263, Supreme Court Library of Korea (2017).

5. OUTLOOK ON FUTURE REGULATORY DEVELOPMENTS IN KOREA

In response to such ramifications, general regulatory safeguards would likely be fortified, rather than limit penalization to a case by case basis. While privacy should not be overlooked incidental to technological development, the consensus seems to be that regulations should not go too far as to inhibit growth.[44] Rather than exploit loopholes by foregoing processes of obtaining consent, private actors must clearly notify end users regarding data management procedures so privacy protection may accord with, rather than diverge from, technological advancement. In the meantime, it would be prudent for businesses to closely monitor the PIPC's administerial and enforcement activities, re-evaluating and revising their compliance measures at appropriate intervals.

Of note is the PIPC's announcement to conduct investigations on approximately 400 infringement cases during the first half or third quarter this year, including the Kakao Map and Luda incidents.[45] Based on the investigation results, it intends to issue regulations on AI personal information protection in March to serve as guidelines for big data service providers.[46] The regulations will embody the following three principles: (1) 'legality,' allowing users to clearly recognize the purpose of collecting personal information and consent in advance; (2) 'safety,' dealing with mechanisms such as encryption and de-identification of personal information; and (3) 'transparency,' in relation to the scope and duration of personal information use and AI service operations.[47]

By reverse token, AI technology will not only be subject to regulation, but will also be utilized for regulation. In its recent press release, the PIPC announced plans to develop an 'AI personal information infringement prevention support system' to evaluate whether only a bare minimum of strictly necessary personal information is legitimately being collected under current bills and ordinances.[48] Unlike legislations, bills and ordinances are not subject to mandatory assessments by central administrative agencies in determining whether they infringe personal information,[49] forming a blind spot for regulating personal information management. However, with the implementation of the new system, the PIPC seeks to prevent excessive collection of personal information by the government and public sector actors. This globally unprecedented AI system will be utilized to (1) analyze whether new and current bills and ordinances involve personal information infringement risks, (2) recommend analogous precedents to assess infringements and suggest new standards based on processes driven by

[44] Jong Hyun Lee, 이루다,카카오맵 개인정보 유출…데이터 활용 기조가 흔들린다 [Luda and Kakao Map Personal Information Leaks…Shifting Trends in Data Use], Digital Daily (Jan. 19, 2021, 7:58 AM), http://www.ddaily.co.kr/news/article/?no=208085.

[45] Hong Seop Lee, 개인정보위 "밀린 사건 400건 상반기에 정리…이루다 관련 다각도로 검토 중" [PIPC to deal with 400 cases pushed back in the first half of this year…Luda controversy and its attendant issues under review from a macro perspective], Edaily (Feb. 24, 2021, 3:44 PM), www.edaily.co.kr/news/read?newsId=04073766628953800&mediaCodeNo=257&OutLnkChk=Y.

[46] *Id.*

[47] *Id.*

[48] Press Release, Personal Information Protection Commission (PIPC), PIPC to enhance personal information protection of Korean citizens using AI-driven technology, (Feb. 24, 2021).

[49] *Id.*

machine-learning, and (3) draft infringement evaluation reports and resolutions.[50]

6. KOREA-EU GDPR DEVELOPMENTS AND ITS IMPLICATIONS FOR DOMESTIC ACTORS

On the international level, coherent coordination seems to be taking place toward enhancing prospects of receiving the much-awaited adequacy decision from the European Commission ("EC") which will provide the requisite legal basis for data transfer pursuant to Article 45 of the GDPR. This is due, in part, to recent legislative changes and transformation of the PIPC into a centralized privacy regulatory authority which the EC previously found lacking.[51] Indeed, such centralization will greatly enhance efficiency in promoting compliance by businesses, and in ensuring the PIPC's independence in administering data protection tasks.[52] Once the EC approves the level of Korean data protection, cross-border data transfers and Korean businesses' collection of data from EU residents will be facilitated and accelerated to a greater degree.

6.1 Regulatory and Business Implications

Meanwhile, businesses should systemize measures to address pervasive challenges by establishing cross-functional teams to engage in regular monitoring of data subjects on a large scale. Designating a Data Protection Officer pursuant to Article 37 of the EU GDPR would facilitate compliance not only with internal policies and GDPR, but also with other EU data protection laws, while enhancing cooperation with supervisory authorities. Moreover, periodic exchanges of internal reports tracking GDPR infringement cases from other jurisdictions and implementing changes that are found necessary upon re-evaluating their practices, would ensure compliance with the GDPR. This is particularly important in the face of special events like mergers and associated cost-cutting that may potentially trigger cyber breaches. The Marriott case[53] is illustrative of practical considerations for regulators and senior business managers in this regard.

In 2014, an estimated 339 million guest records worldwide from the Starwood Group were leaked, of which approximately 30 million were residents of 31 countries in the European Economic Area at the time, including 7 million UK residents. However, the data breach was only revealed in 2018, after Marriott acquired Starwood Group ("Starwood") in 2016. Where a case involves cross-border data processing as in Marriott, "the supervisory authority of the main establishment…of the controller or processor" is designated to act as a lead supervisory authority under Article 56 of the GDPR.[54] Accordingly, in that case, the UK's Information Commissioner's Office ("ICO") acted as the lead supervisory authority on behalf of all EU authorities since the breach occurred before Brexit.[55] The ICO ultimately issued a monetary penalty notice, fining Marriot £18.4 million (mitigated from an initial £99 million) on grounds that it had failed to process personal data in a manner

[50] *Supra,* note 48.
[51] Nicola Casarini, EU-Korea Security Relations (Nicola Casarini ed., 1 ed. 2021).
[52] *Supra,* note 40.
[53] COM0804337, ICO v. Marriott International, ICO Penalty Notice (2020).
[54] Council Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119).
[55] *Supra* (Nicola Casarini), at 2.19.

ensuring appropriate security of the personal data pursuant to Articles 5(1)(f) and 32 of the GDPR. Namely, it identified several security failures on the part of Marriott, including, inter alia, insufficient monitoring of privileged accounts that would have detected the breach and failure to apply wider encryption to other categories of non-payment related personal data (e.g. passport numbers).

Marriott later pointed out that during its acquisition of Starwood, it had only been able to conduct limited due diligence on Starwood's data processing systems and databases. Additionally, it was revealed that to save costs stemming from the merger, most staff, including IT and cybersecurity professionals, had been dismissed. However, while acknowledging that there may be circumstances where in-depth due diligence of a competitor may not be possible during a takeover, the ICO held that the period relevant to its finding of infringement was when the GDPR entered into force. At that point, the question turned on Marriott's adequate management of Starwood systems. Hence, as the controller of its guests' personal data within the meaning of Article 4(7) of the GDPR, Marriott's infringements constituted a serious failure to comply with the GDPR because it had been retaining and continuing to use Starwood's IT systems post-acquisition without securing the requisite technical and organizational measures.

Considering the foregoing, it has been suggested that to ensure transparency, regulators may consider compelling boards of directors to make representations on the cybersecurity exposure of their company or to impose disclosure requirements about the company's plan to protect the data infrastructure after a takeover.[56] Moreover, a prospective purchasing firm could hedge its risk by implementing due diligence questionnaires with a chain of inquiries regarding the IT, security, compliance, and other crucial areas controlled by the target company, binding the latter with warranties to those questions. Even after the purchasing firm acquires the target company, it should exert reasonable efforts to conduct an examination verifying whether any potential risks have indeed been adequately addressed, thereby avoiding risks of inheriting liabilities from the acquired business as in Marriott.

6.2 Other Emerging Trends

Another emerging trend in the CJEU's preliminary judgments is that whereas the majority of cases involving GDPR infringements were previously concentrated amongst EU Member States, recent cases increasingly impose hefty fines for violation of regulations relating to personal data transfers to a third country.[57] Accordingly, the national profiles of regulated companies are becoming more diverse as it relates to data controllers and processors.[58]As such, data exporters and importers should identify and document all cross-border data transfer and assess whether the third country's legislation allows adequate protection compliant with GDPR and CJEU judgments.

---

[56] Shivaram Rajgopal & Bugra Gezer, The Marriott Breach Shows Just How Inadequate Cyber Risk Disclosures Are, Harv. Bus. Rev. (Mar. 5, 2019), https://hbr.org/2019/03/the-marriott-breach-shows-just-how-inadequate-cyber-risk-disclosures-are.

[57] *See, e.g.*, PS/00059/2020, Resolución de Procedimiento Sancionador [Resolution of Sanctioning Procedure] re Vodafone España, S.A.U (2020).

[58] Kyu Yub Lee & Jun Hyun Eom, A Study on CJEU Cases on GDPR and Their Implications for Korea. 102. (2020).

Moreover, current data privacy regulations tend to impose broad-sweeping liabilities, requiring managers to secure organizational and technical measures to negate attendant risks even for incidents which they may fall victims to, thus rendering them non-compliant with the GDPR, including, but not limited to, cyber-attacks, data theft, and cyber fraud.[59] For instance, the French data protection authority recently issued an enforcement action against a data controller (EUR 150,000) and its data processor (EUR 75,000) for failure to take adequate security measures related to credential stuffing[60]. Contractual measures may also be taken in conjunction with organizational and technical measures, via language including obligations for data importers to employ necessary measures to protect transferred data.[61] Therefore, raising cyber security awareness would be key to integrating such measures into practice, and may be achieved by implementing internal policy actions and educational programs to fill in the gaps.

Finally, last November, the EC published a Proposal for a Regulation on European data governance (Data Governance Act) facilitating the reuse and sharing of data across sectors and Member States, thus building a European single market for data.[62] While the proposal is still undergoing debate by the European Parliament, it adds a layer of uncertainty for businesses, for instance, in the context of non-personal data. This is because under the proposal, non-personal data subject to the rights of others "should be transferred only to third-countries where appropriate safeguards for the use of data are provided" to "ensure the protection of fundamental rights…of data holders."[63] Ascertaining the level of appropriateness will be challenging, while it is unclear whether model contract clauses from the EC will be provided to ensure the requisite standards are met. This is pertinent as model clauses add complexity, considering that they have been the frequent subject of legal disputes.[64]Future developments should be closely monitored in anticipation of the adoption of the Act.

7. Conclusion

Notwithstanding transformative changes to privacy laws compliant with the data era, practice reveals weak procedural safeguards and ambiguity in statutory interpretation, contributing to a lack of accountability for data processing. This calls for a heightened understanding of the obscure risks inherent in personal data use. While current case law may be insufficient to account for such unprecedented challenges, the Homeplus case carries meaningful implications for a burgeoning shift from a business-centric to a user-centric data governance model that may serve as a guidepost in revamping regulatory

[59] *See, e.g.*, IN-19-1-1, Decision of the Data Prot. Comm'n in the matter of Twitter Int'l Co. (2020).
[60] Commission Nationale Informatique et Libertés, «Credential stuffing»: la CNIL sanctionne un responsable de traitement et son sous-traitant ["Credential stuffing": CNIL sanctions a data controller and its data processor] (Jan. 27, 2021), www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant.
[61] Eur. Data Prot. Bd., Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (2020).
[62] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM (2020) 767 final (Nov. 11, 2020).
[63] *Supra,* note 51, at par. 15.
[64] Matthew Newman & Mike Swift, SCC guidance in wake of Schrems II decision landing 'very soon,' EU official says, mlex (Oct. 27, 2020, 10:09 PM) https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/scc-guidance-in-wake-of-schrems-ii-decision-landing-very-soon.

schemes. Further, as it relates to EU-Korea GDPR compliance, recent developments are corroborative of a positive alignment of a common understanding between the two parts. Nonetheless, substantive and diverse means of bilateral cooperation and coordination may be further enhanced.

HEALTH DATA AND THE INTERNET OF THINGS IN INDONESIA: NEW LEGAL CHALLENGES

By Nuzul Quraniati Rohmah

1. INTRODUCTION

The terms of the Internet of Things were first mentioned by Kevin Ashton in 1999 when he was doing a presentation when he worked at Procter & Gamble.[65] The Internet of Things (IoT) is a new concept of the internet, where devices around us can link to each other by using internet networks. An example is a smartphone that connects with wearable devices, this gives the impression that the devices can communicate or understand each other. However, the Internet of Things (IoT) spread its wings and is able to cover all sectors, such as education, business, agrotechnology, and health.

The use of the Internet of Things (IoT) in the health sector is a renewal from clinical medical activities and the intention of relying on this technology in the health sector to increase efficiency and effectiveness related to health service. The form of the Internet of Things (IoT) that is often found is EHR (Electronic Health Record), EHR is a renewal from the use of paper that is still often used to fill in and store health data.[66]The Electronic Health Record (EHR) is a digital version of the health data files, which is efficient for medical staff in finding patient's data in thousands of files of other patients. However, behind the convenience, there remains a threat there is potential for personal data leakages.

In the General Data Protection Regulation (GDPR), All data personal is defined as any information relating to an identified or identifiable person, must be collected in accordance with Article 5 of the GDPR, data must contain:

1. Collected for specified, lawful and explicit purposes and not processed in a manner incompatible with it.

2. Processed legally, fairly, and transparently.

3. Processed to ensure proper data security. fair, relevant and limited to what is required in relation to the purpose for which it is processed.

4. Accurate and up to date.

5. Stored in a form that allows identification of data subjects no longer than that required for processed purposes.

[65] Somayya Madakam R, *Internet of Things (IoT) : A Literature*, 3 Journal of Computer and Communication 1-10, (2015).

[66] Nina Rahmadiliyani, Putri, Rina Gunarti, *Implementation of Electronic Health Record (EHR) in Outpatient Polyclinic at the General Hospital of Ratu Zalecha Martapura*, IX Indonesia Health Journal, 1-10, (2019).

6. Controlled by controllers who are in charge of data and are able to demonstrate compliance.[67]

The technological development is also followed by the development of crimes, the cases of leakages and misuse of personal data continues to increase every year, especially during COVID -19 Pandemic. In June 2020, the public was shocked by the news of the leakage of the Indonesian COVID-19 patient data. An account on the dark web named "Database Shopping" is known to have 230.000 Indonesian COVID-19 patient data, where the data was found to contain personal information of the patients such as their name, telephone number, PCR results, and the place that patient is treated.[68] Following this incident, the government has received plenty of public criticism, the government has perceived to have neglected patient rights as regulated in Article 32 of Law No.44 of 2009 mentioned the right of every patient to obtain privacy and confidentiality of the illness, including medical data.[69]

This is not the first time that Indonesia has experienced data leakages. There has been a leak of personal data concerning e-commerce users of Tokopedia amounted to 91 million in July 2020.[70] The incidence of leakages of personal data is continuously happening in Indonesia, but there is no action that the government addresses to prevent and minimize data leaks in Indonesia. Furthermore, Indonesia doesn't have a comprehensive regulation regarding personal data protection until these days. The current regulations are still sectoral and do not adequately protect personal data, even the Personal Data Protection Bill is still being discussed in the House of Representatives.[71] If this situation is continuously allowed without any completion, it will harm constitutional value considering Indonesia is a constitutional state as stipulated in Article 1 Paragraph 1 the 1945 Constitution. A constitutional state is closely related to legal certainty because most of the constitutional state applies one principle known as *"nullum delictum nulla poena sine praevia lege poenali"* which means that an act cannot be punished if there is no regulation governing it.[72] The other issue is related to how strict the government is in supervising providers when they manage people's personal data, it is intended to prevent the sale of personal data by providers.

2. ANALYSIS

2.1. The Impact of Internet of Things (IoT) on the Indonesian Health Sector

The use of this technology in the health sector aims to increase the efficiency and effectiveness between the patient, medical staff, and healthcare facilities. The Internet of Things (IoT) has revolutionized healthcare by empowering not only medical professionals

[67] The General Regulation Data Protection (GDPR) 2016/679, art 5.
[68] Vina Fadhrotul Mukaromah Covid-19 Patient Data Suspectedly Leaked, Why Could This Happen? (2020), *available at* https://www.kompas.com/tren/read/2020/06/20/180500065/data-pasien-covid-19-diduga-bocor-mengapa-hal-ini-bisa-terjadi?page=all (last visited July 7, 2020).
[69] Law No.44 of the Republic of Indonesia (2009), on Hospital, art.32.
[70] Mohammad Bernie, 91 Million Tokopedia User Data Leaked and Spread on Internet Forums (2020), *available at* https://tirto.id/91-juta-data-pengguna-tokopedia-bocor-dan-disebar-di-forum-internet-fNH1 (last visited July 7, 2020).
[71] Sulaeman, Jokowi's Government Rushes to Discuss The Personal Data Protection Bill (2021), *available at* https://www.merdeka.com/uang/pemerintah-jokowi-kebut-pembahasan-ruu-perlindungan-data-pribadi.html (last visited July 7, 2020).
[72] Sri Rahayu, *Implications of the Principle of Legality on Law Enforcement and Justice*, 7 Innovative Journal, 1-12 (2014).

but also medical devices, opening up wide opportunities in all medical fields, and it will speed up healthcare service, diagnose illnesses, and communicate with patients. The Internet of Things (IoT) certainly has changed people's lives, the technology enables constant monitoring of health conditions, and with this technology, the community is able to obtain medical information through devices or the internet.[73]

In Indonesia, the use of the Internet of Things (IoT) in the health sector is still unequal and only can be accessed in areas with internet connections and well-equipped health facilities. However, the use of the Internet of Things (IoT) in the health sector was started in 2012 by the Ministry of Health and was named "Telemedicine." Telemedicine consists of several items that aid for medical examination such as Tele-ECG to measure blood pressure, Tele-radiology to view radiological results, Tele-USG (simple) to view the digital development of the fetus, and Tele-consultants.[74] The examination results are then sent to smartphones, PCs, laptops, and tablets. This allows for greater convenience for medical staff as it enables easier determination of the next medical treatment, as well as the transparency of the results of the patient examination itself.

In the medical services, the medical staff definitely have patient health data which contains personal information, disease diagnosis, medical records, and prescribed drugs. The health data is usually done in writing by medical staff, but over time this is not effective given that the number of patients is not proportional to the number of medical staff in health facilities. In response to the need to improve the situation, Indonesia has started to implement the Electronic Health Record (EHR). Electronic Health Record (EHR) is an electronic database consisting of a collection of patient health data and an information system that has a broader framework and fulfills a set of health data functions that integrates health data from various sources, collects data at health service, and supports service providers in decision making.[75] The use of Electronic Health Record (EHR) has been found to be more effective and efficient in healthcare delivery. Additionally, the use of EHR is advantageous both for patients and medical staff as it reduces medical errors, reduces time spent on test results, accurate diagnosis, medical interventions, and saving costs from using paper for record-keeping.

Currently, there is a form of Internet of Things (IoT) in the health sector that is being used by the community, one of which is Electronic Health (E-Health). Electronic Health (E-Health) is an online health service used to make appointments or to consult a doctor, obtain medical results, and order medicine.[76] Electronic Health (E-Health) aims to facilitate access to health services, improve the quality of health services, and save the cost of health services in health facilities. Currently, there are many types of E-health applications used by the public such as

[73] Oleksandr Gersymov, *Internet of Things in Healthcare*, (27 February 2020) https://codeit.us/blog/internet-of-things-in-healthcare

[74] Ministry of Electronic Information and Transaction, Implementation of the Internet of Things for the Health Sector (2016).

[75] Prihartono & Muhamad Fadhil Nurdin, *Medical Records and Health Information Based on Information Technology*, http://pustaka.unpad.ac.id/wp-content/uploads/2015/12/MEDICAL-RECORDS-AND-HEALTH-INFORMATION-BASED-ON-INFORMATION-TECHNOLOGY.pdf.

[76] Handryas Prasetya Utomo, Elisatris Gultom, Anita Afriana, *Urgention of Legal Protectiom of Patient Personal Data in Technology-Based Health Serbice in Indonesia*, 8 Galuh Justisi Scientific Journal, 168-185, (2020).

consumer informatics, medical informatics, and bioinformatics. However, behind the convenience provided by E-Health there are some usage-related issues, one of which is how strict the security on the E-Health application is, considering that so many cases of data leakage have happened in Indonesia recently.

2.1. The Privacy of Health Data in Indonesia

The patient can be categorized as a consumer in health services at health facilities. Law No.8 of 1999 concerning Consumer Protection in Article 4 describe the rights that can be obtained by patients and obligation that must be fulfilled by the hospital as a health service provider,[77] consist of :

1. The right to comfort, security, and safety in consuming goods and/or services.

2. The right to choose goods and/or services and earn the goods and/or services are appropriate with exchange rates and conditions the guarantee promised.

3. The right to correct, clear, and honest information regarding the conditions and guarantee of goods and/or services.

4. The right to be heard and complaints about goods and/or services used.

5. The right to get advocacy, consumer protection, and efforts to properly resolve consumer protection disputes.

6. The right to receive consumer guidance and education.

7. The right to be treated or served correctly and honestly and not to discriminate.[78]

Health data is a set of medical information that is stored and collected in a document and used for diagnosis, medical examination, and medical treatment. Health data is sensitive personal data, which in the data contains several private information such as medical examination results, lab results, history of the disease, and list of the drugs.[79]Health data, called sensitive data due to contains a lot of information that directly links with patients, that is why health data only can be accessed by the relevant medical staff and must be authorized by the patient. The issue is then, whether the data we provide is guaranteed privacy, which will not take any other action than that offered considering that health data contains sensitive information.

According to Black's Law Dictionary, the right to privacy is defined as several protected rights of human freedoms, including government interference or intervention in personal matters, whether it is family matters or how to organize parties with other parties.[80] The opinion of Warren and Brandeis in their work entitled "The Right to Privacy" states that privacy is the right to enjoy life and the right to respect one's feelings and thoughts.[81] The right of privacy in Indonesia is implicitly stated in Article 28G of the 1945 Constitution "Everyone has the right to

[77] Andrea Sukmadilaga, Sinta Dewi Rosadi, *Legal Efforts On Violation Of Internet Of Things (Iot) Implementation In Health Services According To Provisions Of Personal Data Protection*, 21 Journal of the Voice of Justice, 205-221, (2020).

[78] Law No.8 of the Republic of Indonesia (1990), on Consumer Protection, art 4.

[79] Ministry of Health Decree No.269 of 2008 on Health Record, art.1.

[80] Black Henry Campbell, Black's Law Dictionary, Fifth Edition, USA, 1979, hlm. 1075.

[81] Samuel D. Warren, Louis D. Braindes, *The Right To Privacy*, 4 Harvard Law Review, 193-220, (1890).

personal protection, family, honor, dignity, and property under their control, and are entitled to a sense of security and protection from the threat of fear to do or not do something that is a human right".[82] Accordingly, within the realm of personal health data, every person has the right to obtain protection for health data, given that health data contains sensitive information that could pose a threat in the event of a leak. Furthermore, the privacy of health data is one of the patient rights that must be fulfilled by health facilities and medical staff, both during and after medical treatment.

Privacy of health data in Indonesia has been regulated in Law No. 36 of 2009 concerning Health in Article 57, "Every person has the right to the confidentiality of his personal health condition that has been disclosed to the health service provider and the right to claim damages for mistakes or negligence in the health services he receives."[83] It is clearly stated that health providers have an obligation to keep health data confidential, and if there is any leakage due to the negligence of health service providers, the patient can sue compensation to the health service providers. Furthermore, Article 38 Law No. 44 of 2009 concerning hospitals also affirm that health data only can be accessed for patient's health, requests from law enforcement agencies for law enforcement, and based on statutory provisions.[84] And we can conclude that the privacy of health data must be well-maintained, and no one can access the patient's health data without the patient's permission and by statutory provisions.

The obligation of medical staff to keep health data confidential also stated in Minister of Health Decree No.36 of 2012 concerning Medical Secret, in Article 1 mentioned, "Medical secret is data and information about the health of someone who acquired health personnel at the time of running work or profession."[85] and in Article 3 regulated that medical secrets include data and information regarding:

a. Patient identity;

b. Patient's health includes the results of the history, physical examination, investigations, diagnosis, and medical treatment; and

c. Other matters concerning the patient.

In the Internet of Things (IoT) era, health data is not only used in public health facilities such as hospitals. Currently, there's a lot of internets provides that provide online health facilities or platform and applications that currently that not just asking about our basic personal information but also our sensitive personal information such as a history of the disease, allergy, physical information (height, weight, bust, and thigh circumference), and this information considered same as health data that used in health facilities. And this information is considered the same as health data due to this information being related to our physical condition, and not just anyone can get this information.[86]

Indonesia currently does not have comprehensive regulations both on the protection of health data and personal data.

[82] Undang-Undang Dasar 1945 [UUD 1945] [Constitution] Aug.18,1945, art 28G.
[83] Law No. 36 of the Republic of Indonesia (2009), on Health , art.57.
[84] Law No. 44 of the Republic of Indonesia (2009), on Hospital, art 38.
[85] Ministry of Health Decree No. 36 of the Republic of Indonesia (2012), on Medical Secret, art.1.
[86] Sinta Dewi Rosadi, *Implication of Implementing E-Health Programs Linked to Personal Data Protection*, 9 Legal Arena, 403-418, (2017).

But related to the use of personal data in media electronic has been regulated in Law No.19 of 2016 in Article 26 Paragraph 1 mentioned "Unless otherwise stipulated by the Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned."[87] All the activities related to personal data must be done with the person's permission, and if found to be a violation of the data, then the person has the right to file a lawsuit for the losses incurred.

2.3. Health Data Protection in Indonesia

The GDPR divides the regulated legal subjects into (two), namely a Personal Data Controller / Controller and a Personal Data Processor / Processor. A controller is a person or legal entity, public authority, private sector, or other body that determines the purpose and means of data processing independently or in collaboration with others.[88] In the meantime, a processor is a person or legal entity, public authority, private, or other entity that processes personal data on behalf of the controller. As a result, the existence of a processor is dependent on the decisions made by the controller. Related to the use of the Internet of Things (IoT), the hospital is definitely categorized as a personal data controller because of their determinants of policy directing in determining data processing, but a hospital not necessarily a personal data processor because it is possible to hospital to give this authority to external parties to process data.[89] Indonesia has a similar legal subject as in GDPR, which is called Electronic System Operator (ESO). ESO is every Person, state administrator, Business Entity, and the public who provide, manage and/or operate Electronic Systems individually or collectively to Electronic System Users.[90]

Health data protection in medical activities is stipulated in Article 79 of Law No. 29 of 2004 concerning Medical Practice, "Shall be punished with imprisonment of 1 (one) year or a maximum fine of Rp. 50.000.000,00 (fifty million rupiahs), each a doctor or dentist who deliberately does not fulfill the obligations, the obligation that referred is to keeps everything that doctor, dentist, and medical staff know about the patient, even after the patient has died."[91] Then it can be concluded that doctors, dentists, and medical staff have an obligation to keep the patient data confidential, and if doctors, dentists, and medical staff have been found to not fulfill their obligations, they will be subjected to the section covered under Article 79 of Law Number 29 of 2004. Furthermore, the current issue is how strict the protection of health data is in electronic media or online health providers, considering that many health applications already use health data as a requirement.

Indonesia currently does not have specific regulation governing health data protection in electronic media, and if there is misuse of data then it is adjusted to the provisions in Law No. 11 of 2008 concerning Electronic Information and Technology. Protection of

[87] Law No. 19 of the Republic of Indonesia (2016), on Electronic Information and Technology, art 26.
[88] The General Regulation Data Protection (GDPR) 2016/679, art 4.
[89] Andrea Sukmadilaga, Sinta Dewi Rosadi, *Legal Efforts On Violation Of Internet Of Things (Iot) Implementation In Health Services According To Provisions Of Personal Data Protection*, 21 Journal of the Voice of Justice, 205-221, (2020).
[90] Government Regulation No.71 of 2009, art.1 Regulation of the Implementation of Law No. 16 of 2019 on Electronic Information and Technology.
[91] Law No. 29 of the Republic of Indonesia (2004), on Medical Practice, art. 79.

personal data in electronic systems includes protection against the collection, processing, analysis, storage, appearance, announcement, transmission, distribution, and destruction of personal data.[92] However, the regulations regarding the protection of personal data are still separate from several regulations. One of the regulations that govern related to personal data protection is contained in Law No. 11 of 2008 in Article 30, [93]

1. Any person who knowingly and without right or unlawfully accesses other people's computers and/or electronic systems in any way.

2. Any person who knowingly and without right or against the law accesses computers and/or electronic systems in any way to obtain Electronic Information and/or Electronic Documents.

3. Any person who knowingly and without right or unlawfully accesses computers and/or electronic systems in any way by violating, breaking through, bypassing, or breaking into security systems.

Subsequently, if we relate these provisions to the leakage of patient data COVID-19 in June 2020, we can conclude that the perpetrator has committed an act against the law by accessing electronic systems by violating, bypassing, and breaking into the security system, and even the perpetrator distributes and trades the data publicly on the dark web, and of course, the perpetrator's actions have violated the law and disturbed the society.

Then, it would be appropriate sanctions on perpetrators as described in Article 30, was regulated in Article 46 of Law No.11 of 2008 concerning Electronic Information and Transaction that is, shall be punished with imprisonment for a maximum of 6 (six) year until 8 (eight) year and maximum fine from Rp. 600.000.000,00 (six hundred million rupiahs) until Rp. 800.000.000,00 (eight hundred million rupiahs)[94] Related to the protection of health data by the internet providers or health providers was regulated in Minister of Communication and Information Technology Regulation No.20 of 2016 in Article 36, "Every person who obtains collects, processes, analyzes, stores, displays, announces, sends, and/or disseminates personal data without rights or not following the provisions of this ministerial regulation or other statutory regulations will be subject to administrative sanctions following the provisions of laws." The administrative sanctions are done by an oral warning, written warning, temporary suspensions of activities, and announcements on the website online.[95]

Furthermore, what if there is data leakage by a failure of the Electronic System Operator (ESO) to protect the data. The Electric System Operator (ESO) has obliged to inform the owner of the personal data in writing.[96] The failure that is referred to here is the cessation of part or all of the functions of an essential electronic system so that the

[92] Bernadetha Aurelia Oktavira, Legal Basis for Internet User Personal Data Protection, (4 August 2020) https://www.hukumonline.com/klinik/detail/ulasan/lt4f235fec78736/dasar-hukum-perlindungan-data-pribadi-pengguna-internet/.

[93] Law No.11 of the Republic of Indonesia (2008), on Electronic Information and Technology, art.30.

[94] Law No.11 of the Republic of Indonesia (2008), on Electronic Information and Technology, art.46.

[95] Law No.16 of the Republic of Indonesia (2019) on Electronic Information and Technology, art.36.

[96] Government Regulation No.71 of the Republic of Indonesia (2009), Regulation of the Implementation of Law No. 16 of 2019 on Electronic Information and Technology, art.14.

electronic system does not function properly.[97] And one of the factors that often arises is the failure of Electronic System Operator (ESO) is the resulting escalation of cybercrime. Judging from the type of activity, cybercrime can take the form of hacking, cracking, phishing, identity theft, and so on. The impact of this activity is losses that arise including personal data leakage, data manipulation, privacy breaches, system damage.[98]

The advancement of technology and information, whether in IoT-based application development or other technologies, must be accompanied by comprehensive regulation and also strict oversight by the government. On a global economic level, Indonesia is a country with a strategic position in international trade, including electronic transactions that allow for the greater distribution of personal data in Indonesia.[99] The technical standardization of tools and equipment for IoT has been regulated in the Regulation of the Minister of Communication and Information Number 35 of 2015 concerning Technical Requirements for Near Distance Telecommunication Tools and Equipment, but only in the form of an explanation of which components are required to be used, implying that there is insufficient clarity. Related to IoT implementation in the health sector or other fields, The government should strictly monitor both health care facilities and electronic system operators (ESO). This supervision can be carried out by the Ministry of Communication and Information or by another institution with a supervisory authority. In terms of data processing, standardization should include not only component devices but also data processing flow and data security.

3. CONCLUSION

The current development of the internet has an impact on various sectors, one of which is the health sector, the use of this technology in the health sector was already started in 2012 by the Ministry of Health named Telemedicine. Health data is one of the data that is prone to be used because it contains important information, starting from the personal information and financial information of the owner of the data, and if there is any leakage or misuse, it will have a profound impact on the victim. Especially at this time, there are numerous cases of data misuse via electronic media. Therefore, a comprehensive regulation is required to address issues relating to this personal data.

Currently, health data has become important because it contains several sensitive information related to the patient's condition, such as the history of disease, medical result, and list of drugs used. The misuse of health data has occurred several times in Indonesia, but it seems that it has not been taken seriously by the government, disregarding regulation and data management for internet providers and health providers. The government should strictly monitor both health care facilities and electronic system operators (ESO) and the supervision can be carried out by the Ministry of Communication and Information or by another institution with a supervisory authority.

---

[97] Government Regulation No.71 of the Republic of Indonesia (2009), Regulation of the Implementation of Law No. 16 of 2019 on Electronic Information and Technology, art.24.

[98] Jenis, *Types Of Cyber Crime And Legal Protection*, https://www.legalku.com/jenis-jenis-cyber-crime-dan-perlindungan-hukumnya/.

[99] Andrea Sukmadilaga, Sinta Dewi Rosadi, *Legal Efforts On Violation Of Internet Of Things (Iot) Implementation In Health Services According To Provisions Of Personal Data Protection*, 21 Journal of the Voice of Justice, 205-221, (2020).

LEGAL ISSUE ON DATA PROTECTION IN MALAYSIA: A WAY FORWARDS

By Sea Jia Wei

BACKGROUND

'Cyberspace' is defined as a virtual computer world, and more accurately, is an electronic medium which is being utilised to create a global computer network to allow and to facilitate online communication.

[100] Due to the rapid development of technologies, the Internet has been given a hugely unregulated landscape and enormous overseas access to the information of the whole world. In 2019, Malaysia's Communications and Multimedia Minister announced that the government is currently reviewing the PDPA to ensure it is in line with global developments. The Ministry is keen to incorporate key points of the EU General Data Protection Regulation into the PDPA.[101]

In dealing with cybercrimes, the role of Internet Service Provider ('ISP') should also be considered. ISP refers to a company that provides Internet access to its subscribers. S.43B of Copyright Act 1987 ('CA1987') defines the terms 'service provider' widely to include both companies that provide access to the Internet and entities that provide facilities for online services. [102] The former refers to ISPs such as Digi, Maxis and Celcom, whereas the latter refers to the operators of websites such as Facebook, YouTube and Twitter. In this paper, we will discuss the legal issues of cyberspace and also give recommendations to solve the unsettled legal issues so as to strengthen data protection in Malaysia.

ANALYSIS

Generally, the Malaysian Communications and Multimedia Commission ('MCMC') was set up pursuant to the enactment of the Malaysian Communication and Multimedia Act of 1998 ('CMA1998'). The body acts as a regulator, that is to say, it governs the communications and multimedia industry in Malaysia.[103] S.3(3) provides that nothing in the Act shall be taken to permit the censorship of the Internet.[104] It is pertinent to note that this section has always been wrongly interpreted by many people. They have the tendency to assume that anyone can say whatever he or she likes

[100] Technopedia, What does Cyberspace Mean? (2020), *available at* https://www.techopedia.com/definition/2493/cyberspace (last visited July 7, 2021).
[101] Jillian Chia Yan Ping, Malaysia - Data Protection Overview (2021), *available at* https://www.dataguidance.com/notes/malaysia-data-protection-overview (last visited July 7, 2021).
[102] Act 332 of Malaysia (1987), Copyright Act 1987, §43(B).
[103] Act 588 of Malaysia (1998), Malaysian Communication and Multimedia Act1998.
[104] Id., §3(3).

so long as it is done through the use of the Internet. If past legislations were to be taken into account, then this specific interpretation is not necessarily wrong as the earlier restraint against publication has already been removed. "Earlier restraint" here may be defined as the need to be subjected to censorship or the requirement to obtain a permit.[105] However, there are already such laws in place which will be given more scrutiny in the latter part of this discussion. As such, there are several legal problems which are being addressed by the CMA, namely dissemination of obscene and false materials.

First, dissemination of obscene material. To briefly define the term "obscene" in its literal sense, it relates to a narrow category of pornography that goes against contemporary societal standards and has absolutely no artistic, literary or scientific value.[106] In addition, the term will be discussed later in its legal sense using the Hicklin test. Basically, pornography on the Internet can be categorised into two: adult pornography as well as child pornography. In relation to this, it is also of paramount importance to identify the possible classes of victims of obscenity. They comprise minors, unsuspecting viewers, women put at risk of violence or discrimination, pornography users, and lastly all of us. The vulnerability of these victims can be traced back to two sources: (i) websites – they collectively serve as a pornography platform; and (ii) the trading of pornography – child or adult pornography.

With regard to the former, the MCMC has already taken some drastic moves by compelling most Internet service providers (ISPs) to block or ban porn websites such as Pornhub, xHamster and Brazzers to name a few. The government's battle against porn is due to the fact that pornography is becoming a more pressing issue in the nation, affecting mainly children (cases of statutory rape and sexual assaults) and adults (issues of sperm count and fertility due to excessive masturbation). Industry sources also stated that the MCMC blocks approximately 4,000 websites each year. [107] In the case of the latter source, it involves the sale of pornography in the form of compact discs ('CDs') to customers who are interested. The relevant authorities have also cracked down on these black-market operations. One similarity that can be inferred from both these sources is their objective to obtain profits illegally, considering these operations are cash cows. Nonetheless, there are more serious consequences of the dissemination of pornography to be highlighted such as the loss of human dignity and exploitation of civil rights.

In the case of *R v Hicklin*[108], one Henry Scott resold copies of an anti-Catholic pamphlet entitled "The Confessional Unmasked". When the pamphlets were ordered to be destroyed, Hicklin, the Recorder, revoked the order of destruction and held that Scott's purpose had not been to corrupt public morals but to expose problems within the Catholic's Church. On appeal, it was held that Scott's intention was immaterial if the publication was obscene in fact. Here, the

[105] B. Singh, Enforcement is key when it comes to the net, The Star Online (2015) *available at* https://www.thestar.com.my/opinion/columnists/law-for-everyone/2015/08/13/enforcement-is-key-when-it-comes-to-the-net (last visited July 7, 2021).

[106] David L. Hudson, Obscenity and pornography (2009) *available at* https://www.mtsu.edu/first-amendment/article/1004/obscenity-and-pornography (last visited July 7, 2021).

[107] F.S. Nokman, MCMC engages ISPs in battle against porn, NST Online (2015) *available at* https://www.nst.com.my/news/2015/09/mcmc-engages-isps-battle-against-porn (last visited July 7, 2021).

[108] *Regina v. Hicklin* (U.K. Jurisprudence), LR 3 QB 360 (1868).

Hicklin test being laid down dictates that whether the impugned matter tends to deprave and to corrupt a person's moral. If the matter had a tendency to corrupt and to deprave a person's morals, the matter is then held to be obscene.[109] However, the Hicklin test is not a good test as it is deemed to be very subjective.

The judgement in the case of *Mohamed Ibrahim v Public Prosecutor*[110] is the landmark case that initiates the application of the Hicklin test in Malaysia and has provided for the meaning and scope of the term "obscene" as stated in S.292 of Penal Code ('PC'). Here, the appellant was charged for possessing 65 copies of an obscene book entitled "Tropic of Cancer" intended for sale. The book consisted of the description of the male lead's acts of sexual intercourse with numerous prostitutes. The learned Chief Justice applied the Hicklin test in determining whether the tendency of the said book was to deprave and to corrupt those whose minds were open to such immoral influences and into whose hands it might fall. In other words, the purpose of S.292 of PC was to protect the general public, particularly the younger ones who may be tempted to purchase and so expose themselves to the corrupting influence of obscene materials. As such, the appeal was accordingly dismissed.

Apart from the aforementioned laws, there are S.211 as well as S.233 of CMA1998 whose functions are more or less similar to each other. Both these sections provide that any person who posted an offensive content or material must have had the intention to annoy, abuse, threaten or harass another person. The punishment provided by these sections is also the same whereby a convicted person is liable to a fine not exceeding RM50,000 or to a jail term not exceeding 1 year or to both and shall also be liable to an additional fine of RM1,000 for every day or part of a day during the continuance of the offence after conviction. On top of that, there is also another relevant provision besides S.292 of PC. For instance, S.293 of PC further specifies the former section whereby it makes the sale of any obscene object or document to a person under 20 years of age punishable with a jail term up to 5 years, or with a fine, or with both.[111]

It is often said that with a change of time, the requirement of law changes. However, Malaysian laws do not seem to keep up with the changing times as the Hicklin test which is rendered obsolete by other countries is still in use by the courts. The Hicklin test has attracted widespread criticism as it not only allowed obscene works to be judged based on isolated passages, but it also focused on particularly susceptible persons rather than reasonable persons. The application of such broad tests has led to the suppression of free expression.

The leading test for obscenity in the US has been laid down in the case of *Miller v California*[112]. The court has formulated a three-fold test to replace the Hicklin's test and the Roth test: (1) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interests; (2) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state work; and (3) whether the work, taken as a whole, lacks

[109] M. Cooray, The 'tendency to deprave and corrupt morals' in R v Hicklin and the law of obscenity in Malaysia, 1 M.L.J. 148 (2017) 3-4.
[110] (Malaysian Jurisprudence), 29 MLJ 289 (1963).
[111] Act A327 of Malaysia (1976), The Penal Code, *as revised by* Act 574 (1997).
[112] (U.S. Jurisprudence), 413 U.S. 15 (1973).

serious literary, artistic, political, or scientific value. Additionally, in the Australian case of *Crowe v Graham*[113]the court has rejected Hicklin's test and replaced it with a community-standards test which dictates whether the impugned material offends against the modesty of an average man, or the contemporary community standards. Compared to the Hicklin's test, the courts in US and Australia have adopted an objective approach to deal with obscenity.[114]

Second, the rapid transmission of information has indirectly encouraged the spreading of false information on the Internet, and this has become a major global concern as the amount of false information in circulation has created confusion among Internet users, misleading many of them to believe false information as true due to its widespread coverage. In Malaysia, the term "fake news" carries the definition of any news, information, data and reports, which is or are wholly or partially false, whether in the form of features, visuals or audio recordings or in any other form capable of suggesting words or ideas.[115] Dissemination of false information normally revolves around politics, religion, health and crime in Malaysia and most of the time, it causes a huge impact before it disintegrates with time. For example, a company received a huge financial blow when religious concerns were manipulated to damage their business. The renowned shoe company Bata suffered a loss of more than RM158,000 within the period of one month, and was forced to take down 70,000 pairs of shoes from 230 branches after a false news about them selling shoes with the Arabic word "Allah" on the soles of its shoes broke out.[116] Dissemination of false information is detrimental to a country as it may distort people's perceptions and divert them from the path of truth. In Malaysia, this is in fact used commonly as an incitement tool due to the deteriorating tolerance of the people on religious, racial and sexual orientation issues. Should this issue be left unchecked, then our country will only face a greater peril in the future?

S.233 of the CMA comes in handy when dealing with dissemination of false information as the provision criminalizes the use of network facilities or network services by a person to transmit any communication that is deemed to be, inter alia, false. [117] Due to its widely drafted wordings, former Prime Minister Dato' Seri Najib Tun Razak's administration favoured this provision as an approach to target political opponents. Nevertheless, the present government has vowed to revise and tighten the scope of this section to prevent further abuse of its ambiguous terms.

The laws in Malaysia seem to have an edge over those in the UK as the CMA1998 is commonly used to tackle cases of dissemination of false information while on the other hand, the UK has no specific provision to do the same. Moreover, the

[113] (Australian Jurisprudence), 121 CLR 375 (1968).

[114] Australian Law Reform Commission, History of censorship and classification (2011), *available at* https://www.alrc.gov.au/publication/national-classification-scheme-review-dp-77/2-the-current-classification-scheme/history-of-censorship-and-classification/ (last visited July 7, 2021).

[115] Library of Congress, Initiatives to counter fake news (2020), *available at* https://www.loc.gov/law/help/fake-news/malaysia.php (last visited July 7, 2021).

[116] M. Mohd Yatid, Truth tampering through social media: Malaysia's approach in fighting disinformation & misinformation, 2 IKAT 2 (2019), *available at* https://www.researchgate.net/publication/330450786_Truth_Tampering_Through_Social_Media_Malaysia's_Approach_in_Fighting_Disinformation_Misinformation (last visited July 7, 2021).

[117] Act 588 of Malaysia (1998), Malaysian Communication and Multimedia Act 1998, §233.

MCMC is entrusted with legal powers to enforce laws specifically related to fake news. It has been reported that MCMC opened 40 investigating papers related to fake news in 2017 and 4 cases even reached the court of law for adjudication.[118] In comparison, the UK has communication regulators like Ofcom which regulate broadcast media and the Independent Press Standards Organisation (IPSO) and Impress which regulate online and offline newspapers, but none of these regulators are vested with legal powers thus no significant action has been taken to deal with the dissemination of false information. [119]

Besides, copyright protection in Malaysia is governed by the CA1987. CA punishes any unauthorised access to or dissemination of protected works. S.7 of CA1987 states that the works such as literary works, musical works, artistic works, films, sound recordings and broadcasts are eligible for copyright. However, in order for literary, musical or artistic work to be eligible for copyright, there must be sufficient effort and the work must be reduced into material form. All these works shall be protected regardless of their quality and purpose. There are two types of copyright infringement under S.36 of CA1987, that is, direct infringement and indirect infringement. Direct infringement occurs when someone does an act which is deemed to infringe the rights of the owner and these acts are done without the licence of the owner. On the other hand, the examples of indirect infringement are stated under S.36(2), that is, selling, distributing or exhibiting the article in the public without the consent of the owner of the copyright. In order to amount to copyright infringement, a whole or substantial part of the copyrighted work must be copied. In *Autodesk Inc v Dyason*[120], the defendant had infringed copyright in the 'Autocad' that was owned by the plaintiff by cracking the code and reproducing a substantial part of the program, 'Autokey', in the device.

One of the critical issues that has been raised is whether the Internet user's act of copying the author's works constitutes an infringement of the author's copyright. [121] By comparing Malaysian legislation with US legislation on the right of reproduction of a work in cyberspace, the laws seem to be better in the US. This is because it is easier for the copyright owner to prove that the copyright over software has been infringed. In *Games Corporation v Nintendo of America Inc*[122], the court held that even though only limited copyright protection was provided for certain works, verbatim copying would still amount to an infringement. This statement signifies and emphasises on two important points where there will be no impediments for the plaintiff to prove that the two works are 'substantially similar' in an internet copyright infringement and this test might be reduced to a virtual nullity in cases of verbatim software copying. Besides, with regards to public performance

[118] K. Buchanan, Initiatives to counter fake news (2019), *available at* https://www.loc.gov/law/help/fake-news/malaysia.php#_ftn52 (last visited July 7, 2021).

[119] G. Moir, Regulation of online falsehoods: 'Fake news' – The UK, Singapore And Europe (2019), *available at* http://www.mondaq.com/uk/x/808480/Media+Entertainment+Law/Regulation+Of+Online+Falsehoods+Fake+News+The+UK+Singapore+And+Europe (last visited July 7, 2021).

[120] (Australian Jurisprudence), HCA 2; 173 CLR 330 (1992).

[121] N. Ahmad, *Copyright protection in cyberspace: A critical study with reference to Electronic Copyright Management Systems (ECMS)* in COMMUNICATIONS OF THE IBIMA (2009), 7, *available at* https://ibimapublishing.com/articles/CIBIMA/2009/873738/873738.pdf (last visited July 7, 2021).

[122] (U.S. Jurisprudence, Court of Appeals) 975F.2d, 832 (1992).

and display rights of computer software, the term 'display' is not defined under US legislation. By referring to the terms 'public performance' and 'communication to the public, if one displays the computer software or the operation of the computer software over the Internet, it will be deemed to display to the public and this amounts to a violation of the right of the copyright owner under the statute. US legislation can be one of the good references for us to improve our provision and reduce loopholes in our law.

Lastly, the issue of privacy based on Personal Data Protection Act 2010 (PDPA). [123] Personal information of a person may be obtained through the Internet in order to obtain exploitation or benefit. Internet users may be exposed to danger of violation of their privacy right as cyberspace seems to reach everyone and become increasingly sophisticated.[124] More legal issues will arise due to the increasing amount of people engaging online by interacting in aspects regarding social, economic and even political issues. For instance, one may face the risk of their email addresses, banking passwords, hand phone numbers, physical addresses being exposed to others including undesired marketers, hackers or even scammers. [125]Legal issue of privacy in cyberspace is said to be a subset of data privacy in the larger world. It involves personal privacy covering storage, collection, repurposing, collection, use as well as display of personal information via the Internet generally.[126] Privacy in cyberspace is pertaining with exposure of personal information on the Internet either through sharing of data, collection of data, cyber security threat and tracking as well.[127] There are many issues relating to attempt to invade one's privacy in cyberspace by stealing one's identity as well as monetary assets. Furthermore, they may be subjected to Internet attacks and software which is harmful. Crimes such as phishing, spyware, web bugs and others are an intrusion to the privacy of Internet users. For example, web bugs often are being placed in email or webpages to track views of a person's online activity with the objective to learn passwords of the person while phishing involves the process of attempting to obtain names, passwords, banking information of users through targeted attacks.[128] Thus, establishment of laws and regulations with the purpose to protect privacy as well as data of Internet users is of utmost importance especially in modern day as cyberspace reaches enormous amounts of people. The recognition of right to privacy can be seen in the case named *Campbell v. MGN Limited*[129] where the judgement of the court stated that misuse of personal and private information was established when Mirror newspaper published articles in regard to a famous model

[123] Act 709 of Malaysia (2010), Personal Data Protection Act 2010, §233.

[124] Mark S. Kende. The issue of email privacy and cyberspace personal jurisdiction (2002), *available at* https://scholarship.law.umt.edu/cgi/viewcontent.cgi?article=2251&context=mlr (last visited July 7, 2021).

[125] Thomson Reuters, Internet privacy laws revealed - how your personal information is protected online (2015) *available at* https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online (last visited July 7, 2021).

[126] Anne Meredith Fulton, Cyberspace and the Internet: Who Will Be The Privacy Police?, (2018), a*vailable at* https://scholarship.law.edu/cgi/viewcontent.cgi?article=1033&context=commlaw (last visited July 7, 2021).

[127] Thomson Reuters, Internet privacy laws revealed - how your personal information is protected online (2015) *available at* https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online (last visited July 7, 2021).

[128] Jose Rivera, Cyberspace Law (2019), a*vailable at* https://www.legalmatch.com/law-library/article/cyberspace-law.html (last visited July 7, 2021).

[129] (U.K. Jurisprudence), UKHL 22 (2004).

attendance at Narcotics Anonymous meetings as well as her efforts to solve the problem of addiction to drugs and drinks. It shows that this tort basically aims to protect information which is considered private. Individual's privacy should be respected.[130]

In Malaysia, Personal Data Protection Act 2010 (PDPA) is an act gazette in the date of June 2010 with the purpose of regulating and protecting personal data regarding commercial transactions.[131] It is a legislation that mainly governs data protection. Data generally means information. Personal data generally refers to data about identification of individuals or any information to which other organizations can access it. It can be a term relating to specific information that includes private details of a person such as names, address, telephone numbers and others.[132] In relation to Section 2(1) of PDPA 2010, [133] it provides application of such Act to the persons who process, control as well as authorize processing of personal data. There are three parties involved in obligations in respect to data which is considered as private and personal including data users, data processors as well as data subject. Data user is also known as a controller which has been defined as any individual who controls or authorizes processing personal data. If we see from another perspective, a data processor means an individual who processes data on behalf of the data users. Procession of data is not for his or her own purpose while data subject means individual who is considered as subject of personal data.[134]

According to Section 5(1) of PDPA 2010, punishment of fine of RM 300 000 or imprisonment for a term maximum 2 years will be imposed on data users if Personal Data Protection Principle does not comply with when coming with processing of personal data which is stated under Section 6 to 12 of such Act. Section 6 of such Act provides general principles where processing of personal data requires consent unless it falls under Section 6(2) where processing is necessary for various conditions including to perform the contract, administer justice, protect data subject's interest and others. On the other hand, Section 7 of PDPA 2010 requires data users to notify data subjects about objective data being collected as well as right to request access to such data. This is known as the notice and choice principle. Protection of personal data can be seen from Section 8 of such Act which provides disclosure principle. This provision states that personal data cannot be disclosed in absence of approval of the data subject. On the other hand, Security Principle is provided in Section 9 of such Act where it provides practical steps that should be used by data users for the purpose of protecting personal data from modification, loss, alteration and others. Moreover, Section 10 and Section 11 of such Act provide retention and data integrity principle. Retention principle provides reasonable steps should be taken so that accuracy can be ensured and data current may be maintained for the purpose it was collected for. Last data protection principle is provided in Section 12 of PDPA 2010 that is the access

[130] Foong Cheng Leong, Right to Privacy in Malaysia: Do we have it? (2011) a*vailable at* https://www.loyarburok.com/2011/02/21/right-to-privacy-in-malaysia-do-we-have-it/ (last visited July 7, 2021).

[131] Glenda Eng Hui Sian, Personal Data Protection Act 2010 (PDPA) (2013), *available at* https://www.pwc.com/my/en/services/assurance/pdpa.html (last visited July 7, 2021).

[132] Act 709 of Malaysia (2010), Personal Data Protection Act 2010, §4.

[133] *Id.*, at §2(1).

[134] Deepak Phillai, Malaysia: Data Protection (2019), *available at* https://iclg.com/practice-areas/data-protection-laws-and-regulations/malaysia (last visited July 7, 2021).

principle where power to correct as well as access to such personal data is given to the data subject. [135] There are some exemptions from Data Protection Principles which are expressly stated in Section 45 and 46 of PDPA 2010. Exemptions for objectives of personal, family or household affairs of individuals including recreational purposes are provided in Section 45 while Section 46 of such Act gives power to the Minister in order to make further exemptions upon recommendation of Commissioners. [136]

Furthermore, Section 34 of PDPA 2010 states that the right of correcting personal data in presence of data is inaccurate and incomplete as well as misleading. Section 35 of such Act provides certain data correction requests that need to be complied with. On the other hand, Section 36 of such Act states circumstances where data users refuse to accord with it. Where a data user refuses to accord with it, notification of refusal to comply with data access request should be issued by him under Section 37 of such Act. [137]

CONCLUSIONS

The vast development in cyberspace had led to several negative legal implications to the users and despite laws and regulations being specifically made to curb such issues, unfortunately it was able to solve the matters only to a certain extent as the laws and regulations by itself have some loopholes and flaws within it. To this date, issues which are often deemed as the tip of the iceberg have been taken into consideration and solved but there are more underlying issues which are yet to be resolved on whole due to its complexity in nature. As such, more concerns have to be given by relevant authorities as well as the users of cyberspace to legal issues discussed earlier such as the unresolved copyright infringement and the liability of Internet Service Provider (ISP), concerns on privacy as well as obscenity.

The threat to copyright since the emergence of digital technology, especially the Internet, has been a persistent issue till date and no decisive solution has been taken to curb this issue overall. As per the survey conducted by Raven's site auditor over 200 million Internet pages from the year 2013 till 2015, 29% of the pages are an copy of another[138] and this figure is expected to only increase as not all netizens are aware that the Internet isn't a public domain overall and there are several contents which are protected under the copyright law. The indications that the site is protected under copyright law often can be seen under the headings such as "term of use" and "copyright" but this leads to the question on how many people actually take initiative to notice those and abide by the copyright law? Studies clearly established that in fact majority of netizen tend to skip those and this can be seen in the experiment conducted by two professors where they made several students to sign up for the fake social network called "Namedrop" and hundreds of them signed up without realizing the existence of clause in the terms and conditions which states they must name their first child as Namedrop[139]. This is

[135] Yong Shih Han, Malaysia: Data Protection (2019), *available at* https://iclg.com/practice-areas/data-protection-laws-and-regulations/malaysia (last visited July 7, 2021).
[136] Act 709 of Malaysia (2010), Personal Data Protection Act 2010.
[137] *Id.*
[138] Neil Patel, How To Deal With Duplicate Content Issues (Including Those Created By Your CMS), *available at* https://neilpatel.com/blog/how-to-deal-with-duplicate-content-issues-including-those-created-by-your-cms/ (last visited July 7, 2021).
[139] David Berreby, Click To Agree With What? No One Reads Terms Of Service, Studies Confirm. The

the harsh reality of netizens today where the tendency to neglect the existence of copyright in a particular site is huge.

To overcome the problem stated earlier, merely enforcing the copyright laws in Malaysia wouldn't be sufficient if the Internet users are not even aware or perhaps neglect the existence of previous laws to protect the Internet sites. Thus before taking into the consideration of enforcing the laws, steps needed to be taken to change the mindset of the netizen overall. The ideal suggestion will be to modify the websites to alert the Internet users regarding their site and the materials they publish are being protected by copyright laws of the respective countries. Just like "pop-up advertisement", a similar concept can be used to alert the users on the importance of not duplicating the protected sites whenever the Internet users access the website. Certain people may argue that the use of "ad blocker" software can prevent the users from seeing the notice but that argument can be rebutted since some websites are designed in a way that it can only be accessed if the ad blocker software is inactive. The usage of ad-blocker software is indeed legal and this was established in the regional court of Hamburg, Germany where a couple of publishers were not satisfied with the existence of a software called "Adblock Plus". However, using such software will be indeed turn illegal if the creator of the sites decided to come up with an access-control technologies to prevent the Internet users with ad block software from accessing the copyrighted materials in their website without the accompanying advertisement[140]. Under section 36A of Copyright Act (CA) 1987[141], circumvention of access control is prohibited thus it will be an offence if ad blocker is used when accessing the site which is built in access-control technologies.

If the Internet users still hesitate or fail to comply with the copyright laws despite being alerted multiple times then the court would have no second thought to find the users since a reasonable man wouldn't be doing an illegal action after being alerted multiple times. When more cases emerge, the public will be more aware of the importance of copyright law in protecting internet sites and materials. Another solution to be looked upon is whether copyright holders can opt to sue the ISP which holds indirect liability to allow infringement of copyright to occur instead of suing individual Internet users who infringed the copyright. The drawback of applying this solution in Malaysia is section 36(1) of the CA 1987[142] vague in nature where the literal interpretation of the words in the provision only leads to vicarious liability and nothing more than that. Even the doctrine of vicarious liability under section 36(1) of the CA 1987 is complicated where "full knowledge" from the defendant's side must be established according to the case of Television Broadcasts Ltd & Ors v Mandarin Video Holdings Sdn Bhd[143] unlike US doctrine of vicarious liability where the defendant's knowledge of infringement is immaterial. The theories of contributory and inducement liability is not adopted by the courts in Malaysia which lessen the scope of holding the particular firm which infringes copyright to be liable. Malaysian courts should

Guardian (2017), *available at* https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print (last visited July 7, 2021).

[140] Ben Williams, 'Are Ad Blocker Programs Illegal For You To Use?', Adblock Plus/WhatIsMyIPAddress, *available at* https://whatismyipaddress.com/ad-blocker-legal (last visited July 7, 2021).

[141] Act 332 of Malaysia (2010), Copyright Act 1987, §36A.

[142] *Id.*, §36(1).

[143] (Malaysian Jurisprudence), 1 LNS 32 HC (1983).

start adopting the overall secondary liability theories of the US and amend section 36(1) of the CA 1987 in order to expressly allow the courts to use such theories instead of relying on the literal approach of the word 'cause' in that provision.

When it comes to the protection of data privacy, mere reliance of Personal Data Protection Act 2010 is not sufficient to curb this issue overall as the Act only protects personal data which are used for commercial purpose and there are no provisions specifically address the issue of online privacy[144]. Another flaw which can be traced in the Personal Data Protection Act 2010 is the existing of section 3(2)[145] which expressly stated that the Act is extraneous if the personal data is processed outside Malaysia. As the cyberspace is global in nature and it is ever expanding beyond the concept of borders, such provision can provide a getaway for Malaysia to be a victim of large scale exploitation of online private data. As such, Malaysia should adopt a new set of laws and amend the already existing laws to protect their own netizens from being a victim of invasion of privacy. Inspiration to create new sets of laws in Malaysia can be taken from several developed countries such as the US, Canada and Australia where they have their own specific laws to govern online privacy. In US, there are numerous federal and state laws implemented to protect Internet privacy such as the "Children's Online Privacy Protection Act 1998" which requires several websites and ISP to obtain verifiable parental consent prior to the collection, use or disclosure of personal information given by the minors[146]. Meanwhile Canada's "Digital Privacy Act 2015" brought numerous amendments to the already existing "Personal Information Protection and Electronic Documents Act (PIPEDA)" such as the addition of what generally constitutes valid consent for the collection, use, or disclosure of personal information and the introduction of mandatory data breach notification requirements[147]. The Prime Minister of Canada had also delivered a mandate letter to the Minister of Innovation, Science and Industry recently in order to establish a new set of rights for online users including the right to data portability or privacy. Meanwhile the Privacy Act 1988 provide provisions for the protection of personal information and other form of data protection for online users in Australia[148].

When it comes to obscenity, the main concern arises from the fact that obscene materials can still be viewed using "Virtual Private Network" (VPN) despite the Malaysian Communications and Multimedia Commission (MCMC) had blocked several sites which explicitly provide obscene materials[149] such as pornography. At such, it is

[144] Naufal Fauzi, (NST Online, 2019). 'Data Privacy Laws: Malaysia Has A Long Way To Go'. Retrieved from https://www.nst.com.my/opinion/columnists/2019/02/459321/data-privacy-laws-malaysia-has-long-way-go.

[145] Act 709 of Malaysia (2010), Personal Data Protection Act 2010, §3(2).

[146] Thomson Reuters, Internet Privacy Laws Revealed - How Your Personal Information Is Protected Online, *available at* https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online (*last visited* July 7, 2021).

[147] Tariq Ahmad, Online Privacy Law: Canada, Law Library of Congress (2017) *available at* https://www.loc.gov/law/help/online-privacy-law/2017/canada.php (*last visited* July 7, 2021).

[148] Kelly Buchanan, Online Privacy Law: Australia, Law Library of Congress (2017) *available at* https://www.loc.gov/law/help/online-privacy-law/2012/australia.php (*last visited* July 7, 2021).

[149] S. Matdura, Are Vpns Illegal In Malaysia? (2019), available at https://asklegal.my/p/VPN-malaysia-legal-MCMC-restrictions-illegal (*last visited* July 7, 2021).

essential for Malaysia to follow the footsteps of China in banning the use of unauthorized VPNs to prevent the netizen from accessing obscene materials including child pornography.

In conclusion, cyberlaw is any law that applies to internet-related technologies, and is one of the legal system's newest fields. The reason is because Internet technology is evolving at such a fast pace. Cyber law provides legal protections for internet users. This includes corporations as well as people of everyday life. Thus, learning cyber law is vital to anyone who uses the internet. Although we do not have a standalone cyber security law in Malaysia, a range of sporadic laws to combat cybercrimes in this region. This includes Computer Crimes Act 1997, Communications and Multimedia Act 1998, Penal Code, Copyright Act 1987, Personal Data Protection Act 2010, Sedition Act 1948, case laws and other policies guidelines. In conclusion, by looking at technological advancement nowadays, sufficient methods and regulation to data protection and to safeguard against the essential privacy right is inevitably important without taking into account whether the status is consciously abandoned or not.

ANALYSIS OF THE PLANNED PERSONAL DATA PROTECTION LAW OF INDONESIA, ARTICLE 54 PARAGRAPH (2)

By Muhammad Ardiansyah Arifin

BACKGROUND

Indonesia has planned to promulgate the Personal Data Protection Law (*RUU PDP*) with the latest draft dated January 2020.[150] Article 54(2) stated 'Every person is prohibited from selling or buying personal data'. *RUU PDP* contains criminal sanctions for its violators. For the violation of Article 54(2) *a quo* the sanction is stated in Article 64(2) where violators could be convicted with a maximum of 5 (five) years of imprisonment or a maximum fine of Rp50.000.000.000 (fifty billion) rupiah.[151]

However, in the elucidation of Article 54(2), it is stated that buying or selling prohibition does not include 'monetization'. This implies that 'monetization' of personal data is allowed. However, the article does not elaborate on the threshold of monetization that is allowed under the elucidation of Article 54(2). As the sanction is severe, a threshold to define the allowed 'monetization' is needed. This article will try to explain the threshold of allowed monetization under *RUU PDP* with hopes that such a threshold will be taken into account in the promulgation process of *RUU PDP*. The research method used in this article is qualitative research using secondary data including primary legal sources, secondary legal sources, and other relevant online and offline sources.

ANALYSIS

The *RUU PDP* is a law under promulgation to answer society's concern about the lack of comprehensive regulation regarding personal data protection. Therefore, because the law is not yet in force, it is classified as *ius constituendum* that is a law that is hoped to be promulgated or a law that would be enacted in the future.[152] The need for *RUU PDP* is

[150] Ferdinandus Setu, Siaran Pers No. 15/HM/KOMINFO/01/2020 Tentang Presiden Serahkan Naskah RUU PDP ke DPR RI Website Resmi Kementerian Komunikasi dan Informatika RI (2020), *available at* https://kominfo.go.id/content/detail/24039/siaran-pers-no-15hmkominfo012020-tentang-presiden-serahkan-naskah-ruu-pdp-ke-dpr-ri/0/siaran_pers (*last visited* Jan 31, 2021).

[151] Wahyunanda Kusuma Pertiwi, RUU PDP, Ancaman Denda Puluhan Miliar Menanti Penjual dan Pemalsu Data Pribadi Halaman all - Kompas.com KOMPAS.com (2020), *available at* https://tekno.kompas.com/read/2020/01/30/11395917/ruu-pdp-ancaman-denda-puluhan-miliar-menanti-penjual-dan-pemalsu-data-pribadi?page=all (*last visited* Jan 31, 2021).

[152] Tri Jata Ayu Pramesti, *Ulasan lengkap : Arti Ius Constitutum dan Ius Constituendum*, Hukumonline.com (2015), *available at* https://www.hukumonline.com/klinik/detail/ulasan/lt

caused by several factors. (a) The current existing regulations are uncodified;[153] (b) provide unequal protection because of their sectoral limitation nature; (c) And obsolete because other 130 countries already have personal data protection law.[154]

There are concerns about the current draft of *RUU PDP* such as the importance of an independent oversight committee that is currently absent from the draft,[155] and the potential for the law to be a tool for state surveillance.[156] In contrast, concerns about the absence of monetization thresholds for personal data are overlooked. This is important because the definition of 'monetize' is absent from state law and the definition of 'monetize' according to Investopedia is "the process of turning a non-revenue-generating item into cash, essentially liquidating an asset or object into legal tender".[157] This could lead to an implication that all other monetization activities are allowed as long as the data is not directly bought and sold.

To answer the question upon monetization threshold, this article seeks to answer: The thresholds of monetization allowed under Article 54(2) elucidation. The analysis of this question shall include explanations. First, on the types of personal data monetization, the article will explain the varieties of personal data used for monetization by private parties in Indonesia. Second, the limits of monetization will explain personal data that could not be monetized by parties in Indonesia. Finally, real-life examples will include case studies of personal data monetization in Indonesia's private sector.

Types of Personal Data Monetization

Before we discuss the types of personal data monetization, first we shall discuss the scope of personal data in Indonesia and how personal data could be monetized. According to Government Regulation Number 71 the Year 2019 (PP no. 71/2019) Article 1(29), Personal Data is any data about a person that is identified and/or could be identified on its own or when the data is combined with other information directly or indirectly by electronic and/or non-electronic means.

The protection of personal data is guaranteed by the Indonesian Constitution 1945 post amendment 2002 (UUD 1945), and national law or *Undang-Undang* (UU) from which the Government Regulation was based. The UUD 1945 Article 28G(1) states that "Each person is entitled to the protection of self, his family, honor, dignity, the property he owns and has the right to feel secure and to be protected against threats from fear to do or not to do something that is part of basic rights". Although not explicitly mentioned in the constitution, personal data is part of basic

56777c031ec1c/arti-ius-constitutum-dan-ius-constituendum/ (*last visited* Feb 27, 2021).

[153] Glenn Wijaya, *PELINDUNGAN DATA PRIBADI DI INDONESIA: IUS CONSTITUTUM DAN IUS CONSTITUENDUM*, XIX LAW Rev. 326–361 (2020).

[154] Jawahir Gustav Rizal, *Apa Itu RUU Pelindungan Data Pribadi? Halaman all - Kompas.com*, Kompas (2020), *available at* https://www.kompas.com/tren/read/2020/11/09/184724165/apa-itu-ruu-pelindungan-data-pribadi?page=all (*last visited* Feb 1, 2021).

[155] Knowledge Sector Initiative, *Mendesaknya Regulasi Pelindungan Data Pribadi yang Kompherensif - Wawasan | Knowledge Sector Initiative (KSI)*, Knowledge Sector Initiative (2020), *available at* https://www.ksi-indonesia.org/id/insights/detail/1292-mendesaknya-regulasi-pelindungan-data-pribadi-yang-kompherensif (*last visited* Feb 1, 2021).

[156] Dani Prabowo, *RUU PDP Berpotensi Jadi Alat Negara Intai Warga*, Kompas, July 29, 2020, *available at* https://nasional.kompas.com/read/2020/07/29/13555981/ruu-pdp-berpotensi-jadi-alat-negara-intai-warga (*last visited* Feb 1, 2021).

[157] AKHILESH GANTI, *Monetize Definition*, Investopedia (2020), *available at* https://www.investopedia.com/terms/m/monetize.asp (*last visited* Feb 1, 2021).

rights. This is shown in UU No. 19/2016 on Electronic Information and Transaction Law (EIT Law) Article 26(1) which in summary states that unless provided by regulations, the use of any information through electronic media must be made with the consent of the person whose personal data is used.[158]

On how personal data is monetized, private companies use such data to cut down costs of marketing by using a large amount of personal data to find out the preferences of the public to formulate marketing strategies, by buying such data from its providers.[159] This industry has profited in millions of dollars.[160] The providers of the data could be in the form of data vendors that are an organization or individual who in some ways have the right over the data and offer it to others for a price or free in a data marketplace which is a place in a digital platform where data products are traded or closed platforms for bilateral exchange.[161]

However, not all companies bring the required data from the market, those who have the means such as Google and Facebook among others will offer digital goods and/or services for free in return for personal data.[162] It is an effective marketing strategy with Facebook managing to gather advertising revenue of USD 39.9 billion from their business model of providing free social media services to users in exchange for data collected from their users that will be licensed to third parties.[163]

From the scope of personal data, and from the example on how data could be monetized, we could narrow the types of personal data collected by private parties used for such purposes. Namely, personal data information could be used to predict customer preferences based on criteria set by each data controller such as gender, name, nationality, search preferences, profession, and/or other data that could be procured based on their needs.

For example, a shopping platform will use 'cookies' which is a tool that is stored in a visitor/customer hardware when said person is using the shopping platform. The 'cookies' will collect information about what the person did on the shopping platform, such as what are that person's search preferences, credit card, and visited webpages among others.[164] The information collected by the cookies should not personally identify the person using the platform, but given the fact that a person most likely must register into the shopping platform before being able to make a purchase, the online registration added with the stored 'cookies' would allow a person's specific digital profile to be built.[165]

Limits of Personal Data Monetization

Indonesia has limits on what data could be disclosed for monetization and what is not. We shall discuss the actions that are needed to be taken by private actors before they could disclose personal data for monetization, and the limit of such monetization. Currently,

[158] Dewa Gede Sudika Mangku et al., *THE PERSONAL DATA PROTECTION OF INTERNET USERS IN INDONESIA*, 56 J. SOUTHWEST JIAOTONG Univ. 203–209 (2021).
[159] Edmon Makarim, Pengantar Hukum Telematika Suatu Kompilasi Kajian. 185. (1 ed. 2020).
[160] *Id.*
[161] Markus Spiekermann, *Data Marketplaces: Trends and Monetisation of Data Goods*, 54 Intereconomics 208–216 (2019), 210.
[162] C.Y. LI Wendy, Makoto Nirei & Kazufumi Yamana, *Value of Data: There Is No Such Thing as a Free Lunch in Digital Economy*, *in* Research Institute of Economy, Trade and Industry (RIETI) (2018), 3, *available at* https://www.bea.gov/system/files/papers/20190220ValueofDataLiNireiYamanaforBEAworkingpaper.pdf.
[163] Op cit. C.Y. LI Wendy, Makoto Nirei & Kazufumi Yamana. P.3-4
[164] Op cit. Edmon Makarim. P. 185.
[165] Op cit. Edmon Makarim. P. 186.

several regulations in Indonesia regulates personal data which consists of UU No. 11/2008 EIT Law amended by UU No. 19/2016 EIT Law, Government Regulation No. 82/2012 on Operation of Electronic and Transaction Systems and its complementary Government Regulation No. 71/2019 on Operation of Electronic and Transaction Systems, and Ministry of Communication and Information Regulation No. 20/2016 on Personal Data Protection in Electronic System.[166]

Article 26(1) of EIT Law 2016 states that every information used from electronic media about personal data must first obtain the person's consent unless stated otherwise by law, else the owner of the personal data could file a claim against the person using his/her data according to Article 26(2) of EIT Law 2016.[167] This is echoed in Article 15(1)c of Government Regulation No. 82/2012 where consent must be given when the data is processed.[168] The activities of data 'process' are elaborated under Article 14(2) of Government Regulation No. 71/2019 which includes the collection, analysis, storage, repair, and revision, showing, announcing, transfer, publication, revelation, erasure, and/or destruction.[169]

Furthermore, aside from consent, there are additional requirements in the process of personal data. Article 14(4) states the requirements.[170] (a) The process must fulfill its contractual obligations in obtaining the data; (b) The fulfillment of obligations must be under the law; (c) The vital interest of the data owner must be fulfilled; (d) data controller must fulfill its authority following the law; (e) The data controller must comply with the public interest; (f) Data controller must fulfill other interests that could arise from the data owner.

Therefore, before a data controller could begin the process to monetize personal data, it must obtain consent from the data owner, and fulfill additional obligations stated in the articles. It is important to note that the January 2020 draft of the *RUU PDP* will differentiate between general and specific data. It is currently not clear how such differentiation will affect the public, however specific data may be more regulated compared to general data.

Examples of Personal Data Monetization Practice

There are transactions about personal data even before the *RUU PDP* promulgation. Even now, the monetization of personal data is still lacking a legal framework for countries around the globe, making trading data a risky endeavor.[171] Indonesia has cases of data monetization. This section will elaborate on legal data monetization and illegal data monetization.

[166] Ridha Aditya Nugraha, *Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era Big Data*, 30 Mimb. Huk. - Fak. Huk. Univ. Gadjah Mada 262 (2018), 273; note that the list mentioned in the journal is complemented with author knowledge over new regulations in present time.

[167] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251), art 26(1-3).

[168] Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189), art. 15(1)(c).

[169] Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185), art. 14(2).

[170] Op cit. art.14(4).

[171] Markus Spiekermann, *Data Marketplaces: Trends and Monetisation of Data Goods*, 54 Intereconomics 208–216 (2019), 214.

Legal data monetization is done in compliance with the law mentioned in the second section on the limits of personal data monetization. It is often obtained by making customers or visitors accept terms of use (also known as terms and conditions) and privacy policy. A good privacy policy contains information about what information is collected from visitors and customers, how the information collection is conducted, how the information is used, to whom the information will be shared, options for data owners to vary the collection process, security procedure for protection against loss and misuse of information under the control of the data controller, and procedure to correct inaccurate information.[172]

A case example of lawful data controllers is Tokopedia,[173] Rumah123, and Bukalapak among others.[174] This is because all of such entities have fulfilled the thresholds of the good privacy policy mentioned in the previous paragraph, from how the information is collected to the procedure to correct inaccurate information.

There are cases where data controllers did not meet the good privacy policy threshold. For example, BolehMail.com which tried to waive its responsibility for their collected data by announcing that it could not be claimed against resulting from negligence.[175] While such a waiver is inadmissible because it contradicts the law, such statements could mislead the general public. A worse case example is glodokshop.com, which did not have a privacy policy on their site despite processing their customers' data.[176]

From these examples, the practice of data monetization in Indonesia is within the framework of the law, although there are cases of non-compliance caused by either the lack of knowledge or awareness about the value of personal data. It is important to note that none of the previous examples are about direct data selling that could be outlawed when *RUU PDP* is promulgated because of the lack of data regarding this in Indonesia legally.

On the other hand, cases of direct selling of personal data that happens illegally have existed. One example is the case wherein 2019 Kompas investigated that data regarding bank clients are sold by marketing personnel for hundreds of thousand rupiahs a bulk.[177]Another example is when a hacker is selling 15 million raw data stolen from Tokopedia in an online forum in 2020.[178]

CONCLUSION

Based on the analysis, there are thresholds of personal data monetization that are allowed under Article 54(2) and its elucidation based

[172] Op cit. Edmon Makarim, 194.
[173] Tokopedia, *Term & Condition | Tokopedia*, Tokopedia (2021), *available at* https://www.tokopedia.com/privacy#pengguna-transparansi (*last visited* Feb 28, 2021).
[174] Rumah123, *Privacy Policy*, Rumah123 (2020), https://www.rumah123.com/en/privacy-policy/ (*last visited* Feb 28, 2021);
Bukalapak, *Kebijakan Privasi*, Bukalapak (2020) *available at* https://www.bukalapak.com/privacy (*last visited* Feb 28, 2021).
[175] Op Cit. Edmon Makarim, 195.
[176] *Id.*, at 194-195.
[177] Kompas, *Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial Halaman all - Kompas.com*, Kompas (2019), *available at* https://money.kompas.com/read/2019/05/13/081753626/data-pribadi-dijual-bebas-dari-gaji-hingga-info-kemampuan-finansial?page=all#page2 (*last visited* Feb 28, 2021).
[178] Sorta Tobing, *Mengenal RaidForums, Forum Hacker Tempat Jual-Beli Data yang Bocor - E-commerce Katadata.co.id*, Dkatadata.co.id (2020), *available at* https://katadata.co.id/sortatobing/digital/5eb28857e2903/mengenal-raidforums-forum-hacker-tempat-jual-beli-data-yang-bocor (*last visited* Feb 28, 2021).

on current practices by private actors which are licensing personal data while a form of monetization that is not allowed is to directly buy and/or sell the personal data. However, due care before conducting monetization is needed to avoid possible indictment of criminal sanction when *RUU PDP* comes into force, as there might be more rigid implementing regulation concerning the processing of data.

We hope that the government takes into account the elaboration of differences between buy/sell and monetization in Article 54(2) and its elucidation in the promulgation process to avoid confusion between these terms.

IS THE RIGHTS TO BE LET ALONE PROTECTED UNDER THE PERSONAL DATA LAWS?

By Basil Rhodes Ghazali

ISSUES

The combination of computer technology with telecommunications has resulted in a revolution in the field of information systems. Data or information that in decades ago had to take days to process before being sent to the other parties can now be done in seconds. On the other hand, the rapid development of information technology creates opportunities so that people are connected to one another without national borders. For example, electronic commerce, electronic education, electronic health, and electronic government. However, these developments make it very easy for a person's personal data to be transferred to other parties without their permission. The threat of leakage of personal data is also becoming increasingly prominent with the development of the e-commerce sector in Indonesia.

[179] The 1000 Start Up movement launched by President Joko Widodo, as one of the pillars in the development of the digital economy, has at least succeeded in encouraging the growth of four Unicorn startups from Indonesia and that is Go-Jek, Tokopedia, Traveloka, and Bukalapak.[180]

The growth of this digital startup has also triggered massive collection of consumer personal data, not only personal data, but also consumer behavior data. Referring to the terms of services of a number of e-commerce in Indonesia, they collect consumer personal data. In fact, almost all applications, if a potential user wants to run, will force the user to provide access to other data, such as access to personal identity, contact list, location, SMS, photos / media / files. So, if the user really wants to run the application, he has no choice but to agree to access the data. Unfortunately, the absence of a Law on Personal Data Protection results in the absence of standardization of data protection principles, which results in minimal recognition of privacy itself. For example, in 2020 there was a leak of personal data in Indonesia related to BUMN (*Badan Usaha Milik Negara*) and start-up unicorn companies.[181]

[179] Bernadetha Aurelia Oktavira, Dasar Hukum Perlindungan Data Pribadi Pengguna Internet (2021) *available at* https://jurnal.hukumonline.com/klinik/detail/lt4f235fec78736/dasar-hukum-perlindungan-data-pribadi-pengguna-internet (*last visited* Feb. 23, 2021).

[180] Tempo, Gerakan Nasional 1000 Startup Digital, Rudiantara: Tambah Unicorn (2021) *available at* https://kominfo.go.id/content/detail/20780/gerakan-nasional-1000-startup-digital-rudiantara-tambah-unicorn/0/sorotan_media (*last visited* Feb. 23, 2021).

[181] Kasus Kebocoran Data di Indonesia dan Nasib UU Perlindungan Data Pribadi (2021) *available at* https://tekno.kompas.com/read/2020/05/05/190800

At Telkomsel, a leak of personal data happened because the customer service officer committed a violation, but at Tokopedia and Bukalapak it happened because of a server breach.[182] Another security hole in Gojek for Android and iOS, which hackers could potentially use to steal user's confidential information, such as phone numbers, e-mails, and usernames. Some of the above events show the low respect for personal data as privacy in electronic systems. This proves the digital transformation in Indonesia, which has developed rapidly in the last decade, has not been matched by the ability of the public to understand the implications of the use of personal data in information and communication technology. The neglect of privacy protection and the lack of public awareness of the protection of their privacy provides room for a number of violations and misuse of a person's personal data.[183]

In this modern era, there is a need to maintain privacy so that data becomes confidential. On the other hand, in line with the development of freedom, people often prioritize expression. This shows the controversy between privacy and expression. "Privacy and expression are oxymoronic. While privacy requires privacy and expressiveness, expression entails publicity, and this inevitably leads to friction."[184]Thus, certainty is needed in the form of regulations to maintain a balance between the two interests. The regulations must be clear and detailed. Unfortunately, until now there has been no major legal umbrella that specifically regulates personal data in Indonesia. As for today, the regulations regarding personal data in Indonesia are still separate and scattered in various regulations, namely in 32 laws and are sectoral in nature while there are around 132 countries that have regulated laws on personal data protection. This also proves that public awareness regarding personal data is still very low.

In the current scenario, the attitude of the government to form the Personal Data Protection Bill (RUU PDP) is crucial to be resolved at this time, especially with the emergence of numerous cases of public data leakage, even the PDP Bill has developed into a problem of need. The government and the DPR (*Dewan Perwakilan Rakyat)* will immediately step on the gas to complete the bill. One of the reasons is because other countries already have PDP regulations. Friendly countries require Indonesia to have a PDP law (Act) that is equivalent to that of its country. The particular reason for these circumstances is because the PDP Bill can provide a sense of security to the public in using various internet application platforms and also the PDP Bill is necessary to guarantee national interests. The increasingly massive hacking incidents, the use of data

67/kasus-kebocoran-data-di-indonesia-dan-nasib-uu-perlindungan-data-pribadi?page=all (*last visited* Feb. 23, 2021).

[182] Lazuardi Utama, Kasus Bobolnya Data Pribadi Konsumen Indonesia, Serupa tapi Tak Sama, (2021) *available at* https://www.viva.co.id/digital/digilife/1285857-3-kasus-bobolnya-data-pribadi-konsumen-indonesia-serupa-tapi-tak-sama (*last visited* Feb. 23, 2021).

[183] Wahyunanda Kusuma, Data Tokopedia, Gojek, dan Bukalapak Bocor di Tengah Absennya RUU PDP (2020) available at https://tekno.kompas.com/read/2020/05/04/20170027/data-tokopedia-gojek-dan-bukalapak-bocor-di-tengah-absennya-ruu-pdp (*last visited* Feb. 24, 2021),

[184] Althaf Marsoof, Online Social Networking and the Right to Privacy: The Conflicting Rights of Privacy and Expression, 19. Oxford I. L. J. 111, (2011).

without permission, have further strengthened the need for the PDP Law itself.

With the certainty of the PDP, it will put Indonesia on a par with countries that have previously implemented the PDP law. The government and the DPR have agreed to immediately finalize the draft law on Personal Data Protection (RUU PDP). Currently, the government and the DPR Commission did not have sharp differences in their views on the needs of the law. In this case, BPHN (*Badan Pembinaan Hukum Nasional)* has prepared an academic paper to provide an initial concept of what personal data or privacy actually is and explain that concept. The concept of privacy itself is the idea of maintaining personal integrity and dignity. The right to privacy is also an individual's ability to determine who holds information about them and how that information is used. The concept of data protection implies that individuals have the right to determine whether they will share or exchange their personal data or not. In addition, individuals also have the right to determine the conditions for carrying out the transfer of personal data. Furthermore, data protection is also related to the concept of the right to privacy.[185] The right to privacy has evolved so that it can be used to define the right to protect personal data.

Thus, the legal issue is whether privacy in the regulation of personal data for electronic systems in Indonesia has been well protected.

[185] Pamela Samuelson, Privacy As Intellectual Property? Stanford L.R. 52. 1125-1173, (2000).

REGULATIONS

The main source of regulating personal data is actually in Article 28G of the 1945 Constitution which states the right to protection, security right, right to choose to act over not doing. The provisions of the article read: "Every person has the right to protection of himself, family, honor, dignity and property under his control ...". Technically, the regulation of personal data regulation can be distinguished between those that are general (which are not examined in this paper) and those that are specific because they are in an electronic system.
General regulations are contained in:

1. Act Number 7 of 1992 on Banking as amended by Act Number 10 of 1998 concerning Amendments to Act Number 7 of 1992 on Banking;

2. Law Number 8 Year 1997 on Company Documents;

3. Law Number 36 Year 1999 on Telecommunication

4. Law Number 23 Year 2006 on Population Administration as amended by Law Number 24 Year 2013 on Amendments to Law Number 23 Year 2006 concerning Population Administration;

5. Law Number 36 Year 2009 on Health; and

6. Law Number 43 of 2009 on Archives.

While the special regulations are contained in:

1. Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 concerning

Electronic Information and Transactions (hereinafter referred to as the ITE Amendment Law);

2. Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law);

3. Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions (hereinafter referred to as PP PSTE);

4. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems (hereinafter referred to as Permenkominfo PDP).

ANALYSIS

To examine the problems in this paper, law research was conducted. This research is related to legal problems, issues, and questions, it requires theoretical, pure, or doctrinal legal research.[186] By choosing this type of research, the writer hopes to get legal principles, rules of law, or judges' decisions related to regulations regarding privacy of personal data.[187]

According to the Kamus Besar Bahasa Indonesia (KBBI), privacy is "freedom or privacy."[188] Meanwhile, according to the Cambridge Dictionary, privacy is "the state of being alone, or the right to keep one's personal matters and relationship secret."[189] The concept of privacy was first developed by Warren and Brandeis. In early times, the law gave a remedy only for physical interference with life. Right to life served only to protect the subject from battery in its various forms. Later, came recognition of man's spiritual nature, of his feelings and his intellect.[190] The scope of these legal rights broadened. The right to life has come to mean the right to enjoy life, the right to be let alone. In this regard, Judge Cooley insists on the importance of the right to be let alone.[191]

Article 12 of the Universal Declaration of Human Rights enunciates that "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attack upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks ". Based on that, many jurisdictions, including South Korea, Spain, Switzerland, Thailand, the United States, and the United Kingdom have recognized the right to privacy.[192]
Based on the provisions that are stated explicitly or implicitly regarding privacy, it is clear that the protection of the right to privacy as part of human rights has been regulated in international regulations as follows:

1. Universal Declaration of Human Rights (1948);

2. International Covenant on Civil and Political Rights (1966);

[186] Anwarul Yakin, Legal Research and Writing (2007), 10.
[187] Sutandyo Wignyosubroto, Hukum, Paradigma, Metode, dan Dinamika Masalahnya. 147-160. (2002).
[188] KBBI, Privasi, https://kbbi.web.id/privasi.
[189] Cambridge Dictionary, Privacy, https://dictionary.cambridge.org/dictionary/english/privacy.
[190] Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, 4. Harvard L.R. 193, (1890).
[191] *Id.*, 195.
[192] Althaf Marsoof, p. 111

3. European Convention on Human Rights (European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950);

4. American Convention on the Protection of Human Rights (American Convention on Human Rights, 1979); and

5. Cairo Declaration of Islamic Human Rights (Cairo Declaration of Islamic Human Rights, 1990).

In the Indonesian legal system, the right to privacy is classified as derogable rights, which means that its fulfilment can be reduced. This right is different from non-derogable rights, namely human rights that cannot be reduced under any circumstances.[193] Non-derogable rights are regulated in Article 28 G paragraph (1) of the 1945 Constitution. Thus, it can be said that reduction, limitation, or violation of privacy cannot necessarily be considered a violation of human rights.

The basic concept of protecting personal data first appeared around 1960. In 1970 the German state of Hesse became the first state to enact data protection regulations. This was followed by national law in Sweden in 1973, West Germany in 1977, the United States in 1974, and France in 1978, and the UK in 1984.[194]

[193] The meaning of "under any circumstances" includes a state of war, armed dispute, and / or a state of emergency, in accordance with Law No. 39 of the Republic of Indonesia (1999), concerning Human Rights, art. 4.

[194] Andrew Murray, Information Technology Law, (2010), 466.

Data protection is often seen as part of privacy protection. Basically, data protection can specifically relate to privacy as stated by Allan Westin: "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." He was the first to define privacy as the right of individuals, groups or institutions to determine whether or not information about them is communicated to others. This understanding of privacy is called information privacy because it involves personal information.[195]

Therefore, in order to respond to today's challenges, including the global trend in personal data protection, as part of protecting the right to privacy of every citizen, it is important for Indonesia to have a comprehensive Personal Data Protection Act immediately. Protecting privacy also means protecting one's dignity, which is part of the individual's sovereignty in cyberspace, because with that sovereignty one can exercise freedom of expression in a democratic system.

In order to find out whether protection of privacy has been included in the existing regulations, the author uses the parameters compiled by Althaf Marsoof, to examine the following four aspects.

a. Breach of Confidence

Privacy can be protected in numerous ways as the law stands today. In most common law jurisdictions, breach of confidence is sanctioned seriously. Therefore, breach of

[195] Alan F. Westin, Privacy and Freedom (1967), 7.

confidence can be resorted to as a suitable cause of action in fighting the threat to privacy. Traditionally, in order to form a breach of confidence action, the plaintiff was required to establish, inter alia, that the information was capable of being protected. It is clear that only information that was intended to be kept confidential satisfies the criteria.[196]

According to Article 32 (1) of the ITE Law, any changes to electronic information are prohibited. According to Article 48 (1) of the ITE Law, offenders can be subject to a maximum imprisonment of 8 years or a maximum fine of Rp. 2 billion. Moreover, actions that result in electronic information becoming no longer confidential because it can be accessed by the public, in accordance with Article 32 paragraph (3) of the ITE Law. This action is punishable by imprisonment for a maximum of 10 years or a maximum fine of Rp. 5 billion, in accordance with Article 48 paragraph (3) of the ITE Law.

Meanwhile, Article 9 paragraph (1) PP PSTE states that electronic system operators are required to guarantee the confidentiality of the software source code used. Article 2 paragraph (2) Permenkominfo PDP states that privacy is a form of respect for personal data. This is the owner's freedom to declare a secret or not, as determined by Article 2 paragraph (3) Permenkominfo PDP. Therefore, the owner of the data has the right to keep confidential, complain for dispute resolution, amend, obtain history, and destroy personal data that has been submitted to electronic system administrators, in accordance with Article 26 Permenkominfo PDP. If there is a party who without permission violates the privacy of the owner of personal data, then according to Article 36 paragraph (1) Permenkominfo PDP, it will be given administrative sanctions such as oral, written warnings, cessation of activities, or announcements on the website.

b. Copyright in Confidence Material

Certain personal information may include copyright as literary or artistic work. For example, a digital diary or a blog or wall post maintained in a website and shared between limited contacts would undoubtedly attract the website-user's copyright. It provided that the material is "original" and involved "sufficient skill, labor and judgment" to warrant copyright protection.[197] Elucidation of Article 25 paragraph (1) of the ITE Law states that electronic information is protected as intellectual property rights, including copyright, must be protected by this regulation.

This provision applies to databases or data compilations, in a format that can be read by computer programs or other media, as stipulated in Article 10 paragraph (1) of Law Number 28 of 2014 concerning Copyright. Based on Article 3 (2) a of PDP Ministry Decree, in obtaining and collecting personal databases, electronic system operators must respect the owners of the database for their privacy. So that it can be concluded that the database is a confidential document whose privacy must be respected.

c. Personality in Merchandising

[196] Althaf Marsoof, 116.

[197] *Supra,* note 18, at 117.

The question is "Can the law of personal data protect the unauthorized commercial use of celebrity photographs in websites?". This specifically relates to the possibility of creating false profiles in the name of well-known individuals and the ability to liberally tag photographs. Given the possibility of creating groups and interactive applications in websites, such as Facebook, websites are a promising tool for advertising and promoting one's businesses.[198] According to Article 26 paragraph (1) of the ITE Law, the use of electronic information related to personal data must be subject to the consent of the owner. Although violations of this provision are not subject to criminal sanctions, the injured party can file a claim for compensation, in accordance with Article 26 paragraph (2) of the ITE Law.

The Electronic System Operator is obliged to guarantee that the processing of personal data is based on the approval of the owner, based on Article 15 paragraph (1) b PP PSTE. As in Indonesia, everyone is prohibited from making commercial use, that he has made for commercial purposes of advertising or advertising without written consent. So the use of personal data by other parties must obtain the owner's permission, even in written documents, according to the Article 6 Permenkominfo PDP.

d. Defamation, Slander, and Libel

From the above observation, it is manifest that a remedy against a breach of individual privacy exists in the realm of the law of defamation. However, it must be noted that the remedy has its limitations. Firstly, the plaintiff must establish a defamatory statement (oral or written) injurious to the plaintiff's reputation. Second, it must be established that the statement had been publicized. Third, the defendant must have known or should have known that the statement was false. Given these limitations, privacy breaches lacking defamatory characteristics cannot be prevented or redressed through the law of defamation.[199]

There is a prohibition on insulting or defamation when transmitting, distributing and accessing electronic information, in Article 27 paragraph (3) of the ITE Law. This violation is punishable by imprisonment for a maximum of 6 years or a maximum fine of Rp. 1 billion, as regulated in Article 45 paragraph (1). Regarding this matter, PP PSTE and Permenkominfo PDP do not regulate it at all.

CONCLUSION

Based on the discussion on the four aspects of regulations related to personal data, it can be argued that the regulations in the existing electronic systems are adequate. Indeed, there are opinions that the regulation of personal data protection in Indonesia is still weak. Looking back on the analysis that has been written above, the question of whether the Personal Data Protection Law should be legalized or not is no longer a question, because the answer is affirmative, legalized. After knowing the information about the high potential of crimes committed by data keepers against data collectors, it is clear that there is

[198] *Id.*, at 118.

[199] *Supra,* note 18, at 122.

an urgency to pass a law as soon as possible which includes clear provisions protecting the personal data and privacy of Indonesian citizens. The regulation regarding the right to privacy over personal data is a manifestation of recognition and protection of basic human rights and also a necessity that cannot be underestimated. In fact, there are many aspects that should be assessed from the existing regulations. But partially, it can be considered that the PDP law has touched on the essential thing.

This proves that we no longer rely on fragmented laws and regulations that have no legal certainty. If the ITE Law is passed on the basis of awareness of rampant crimes in the cyber world, the Personal Data Protection Law must also be passed as soon as possible with the same awareness or even more urgently. Basically personal data is personal identity, whose existence is a constitutional right of citizens to be left alone. The irregularity regarding this matter causes losses for citizens whose rights to privacy are bypassed by those who kept their personal data. Seeing how many countries have implemented similar laws, Indonesia as one of the largest cyber citizens in the world, should as soon as possible enact a similar draft law, into binding legislation.[200]

From the author point of view, the weakness may occur due to the protection of personal data for conventional activities, not in the field of electronic systems. In this case, a legal umbrella is needed that can be held by the perpetrators, whether they have personal data, process personal data, or who control personal data.[201] Personal data management is related to privacy, which is part of human rights. Therefore, the author suggests that a special law be established that comprehensively regulates personal data, whether related to electronic systems or conventional means. Given the low level and limited scope of the ministry of decree, it is necessary to establish a more robust, dependable and also persistent regulation which is summarized in one personal data protection law. Seeing how many countries have implemented similar laws, Indonesia as one of the largest cyber citizens in the world, should as soon as possible enact a similar draft law, into binding legislation

[200] The Conversation, RUU PDP masih memiliki banyak kekurangan dibandingkan standar internasional dalam melindungi data pribadi, (Feb. 25, 2021, 5.50 PM) https://theconversation.com/ruu-pdp-masih-memiliki-banyak-kekurangan-dibandingkan-standar-internasional-dalam-melindungi-data-pribadi-151212.

[201] Merdeka.com, Indonesia Butuh Aturan Khusus Perlindungan Data Pribadi, 9 November 2020, (last visited Feb. 23, 2021, 7. 47 PM) https://www.merdeka.com/uang/indonesia-butuh-aturan-khusus-perlindungan-data-pribadi.html.

INDONESIA'S VIRTUAL POLICE AND TOKOPEDIA DATA BREACH: URGENCY FOR DATA PROTECTION LAW

By Aulia Shifa Hamida

INDONESIA'S VIRTUAL POLICE AGENDA

In the aftermath of the appointment of the new Chief of Indonesian National Police, Listyo Sigit Prabowo, and later of his inauguration by President Joko Widodo on 27 January 2021, several of his proposed policies with regard to the reform of Indonesian National Police have since come to prominence and gained national critical acclaim, among which is the initiative of Virtual Police which has been very much on his high agenda.[202][203][204] It has been taking effect as of 25 February 2021 and there have been different moral judgments pertaining to the initiative. What makes it critically acclaimed has been its possession of values of compromise and mediation, which Mr. Listyo regards as a manifestation of restorative justice system, which on the other side makes it critically condemned and people have been questioning its legitimacy, whether it is contrary to the basic principles of democracy; freedom speech, press and expression. Nevertheless, in a utilitarian point of view, by virtue of its restorative justice values, this initiative is said to be, substantively and procedurally, based on the ground that the approach of restorative justice in law enforcement can and will decrease criminalisation, hence convictions, and otherwise resort to that of cyber, social media ethics and etiquette education, remedy the prolonged public opinion towards police and prevent the tendency of police prejudice towards conviction by means of partially and in a prejudiced manner interpreting laws that are in fact, subject to multi-interpretation.

[202] BPMI Setpres, "Presiden Jokowi Lantik Listyo Sigit Prabowo sebagai Kapolri", Presiden RI, (2021), *available at* https://www.presidenri.go.id/siaran-pers/presiden-jokowi-lantik-listyo-sigit-prabowo-sebagai-kapolri/ (*last visited* July 7, 2021).

[203] Merlion Gusti, "Kapolri Baru, Momentum Reformasi Polri", Kompas TV (2021), *available at* https://www.kompas.tv/article/141889/kapolri-baru-momentum-reformasi-polri

[204] Syailendra Persada, "Kompolnas Sebut Reformasi Polri Jadi Salah Satu PR Kapolri Terpilih", Tempo, (2021), *available at* https://nasional.tempo.co/read/1424033/kompolnas-sebut-reformasi-polri-jadi-salah-satu-pr-kapolri-terpilih/full?view=ok (*last visited* July 7, 2021).

VIRTUAL POLICE PROCEDURE, CRITICAL ACCLAMATIONS AND CONDEMNATIONS

The procedure itself begins with people, who are thought to be violating the law especially Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 on Electronic Information and Transactions (EIT) will be receiving digital warning through their direct messages and they will be obliged to delete their post, whatever the form it may take.[205] It is worth noting that how the judgment is being made and the law is being interpreted to finally convict and summon a person, will not be carried out solely by subjective judgment of the police personnel. Instead, this phase in advance of giving people virtual warning to delete whatever they share on social media which is thought to be unlawful will be preceded by deliberation among several professional experts, that are to say, language experts, criminal law experts and experts in information and transactions law.[206] If the person were to refuse to undo their post, they will be given a second warning. If one insists on not complying with what they are obliged to, they will be granted a fair audience at the police agency's earliest convenience for the purpose of thorough clarification. Notwithstanding, a conviction is said to be the last resort. This procedure applies to cases such as libel, slander and humiliation. Its critical acclamations have been the foreseeable decline in criminalisation, prevention of police prejudice in interpreting law, cyber, social media ethics and etiquette education and police reform which is said to deal with the current public opinion towards police.[207] Its critical condemnations have been the people taking stance on the matter saying that it possesses a big tendency to restrict people from remaining vocal about their voice and critics of government, and is contrary to the basic principles of democracy; freedom of speech, expression and press.

THE LEGITIMACY OF VIRTUAL POLICE

Speaking of the legitimacy, the government and national legislature, People's Representative Council of Indonesia, must second guess its legitimacy as to whether it is compatible with the country's legal system of Civil Law along with its positivist and rigid nature, and as well as the rule of law; and that this Virtual Police agenda can not simply exist without data protection law. First and foremost, the law *per se* is not supposed to be compromising, at least not in Civil Law countries, especially Indonesia, due to its positivist nature of its Civil Law system, along with its written and codified laws, that are not, substantively and procedurally, easily interpreted. And if legal uncertainty or legal vacuum were to exist or if certain laws were to be subject to multiple interpretations, the legal measures must be carried out by the national

[205] CNN Indonesia, Cara Kerja Virtual Police: Peringatan Polisi Dikirim via DM, CNN Indonesia (2021), *available at* https://m.cnnindonesia.com/nasional/20210225093152-12-610643/cara-kerja-virtual-police-peringatan-polisi-dikirim-via-dm (*last visited* July 7, 2021).

[206] Tim Detikcom, "Ini Langkah-langkah Virtual Police Sesuai Pedoman Baru UU ITE", Detik News (2021), *available at* https://news.detik.com/berita/d-5407271/ini-langkah-langkah-virtual-police-sesuai-pedoman-baru-uu-ite (*last visited* July 7, 2021).

[207] *Id.*

legislature, either by making, amending or repealing any particular laws.

The presence of the restorative justice system may educate the community and decrease criminalisation, but its manner in mediation and its compromising nature unequivocally reflect the need for change in our law, especially the EIT Law and the lack of thorough personal data protection law. Nevertheless, the legitimate role needed to deal with the gap in law, which may take the form of legal uncertainty or clauses that are subject to multiple interpretations, must not be carried out by a police agency and an offender meeting each other halfway. There are four tendencies which can be inflicted by the Virtual Police initiative. First, people will be on their best behaviour, and being followed suit by decline in law-breaking behaviour, convictions and imprisonments. That being said, some people will only behave after being virtually warned or summoned to undo whatever they share on social media and being proven that the scheme is not a smoke and mirror; which means that some people are going to take law less seriously. Third, the law is now open to compromises and legal positivism in Indonesia is likely to start wearing off, which is relatively good and relatively bad. Fourth, the emergence of this restorative justice system with police agencies and offenders trying to meet each other halfway, this can lead to more policy bribery.

Apart from that, this Virtual Police agenda aimed at preventing criminalisation and conviction in consequence of violating Electronic Information and Transactions Law unequivocally reflects the need for change in our laws and the existing loophole, which is the absence of data protection law in Indonesia. By preventing criminalisation and conviction of offenders, it is concrete that the current law, that is to say EIT Law is no longer compatible with the modern day. So, there is urgency for the coexistence between Virtual Police and the amendment of the EIT Law, thus people can still be educated on how to behave on social media legitimately without having to diminish the legitimacy of the current law.

POLICY RECOMMENDATIONS

The legal measures to deal with this illegitimacy must be carried out by the national legislature, not police agencies, resorting to amend or repeal the current law, or make new law. Notwithstanding, to be forward-thinking, if this Police Virtual agenda were to continue to exist and not to be rescinded at a later time, the solution will be to pass the *ius constituendum* on Personal Data Protection, which will set guidance and standards in the execution of Virtual Police, with the aim of protecting social media users and technology companies, not only nationally but also those who fall under another country's jurisdiction. The bill will define rights and obligations of parties involved, that is to say, police agencies who have legitimate authority, social media users and technology companies nationally and internationally. This is a matter of great importance because police, owing to their legitimacy, have authority to gain access to personal data of social media users if they are thought to be violating the law. We know that law does not only regulate citizens, markets and corporations. Politicians, legislators, administrators and public servants are also being defined by their rights and obligations and thus are subject to administrative law.

DATA PROTECTION LAW AS A NECESSITY

The continuing absence of data protection law can result in the abuse of power. In the midst of globalisation where science and technology have become the two most powerful determinants in bringing forth favourable opportunities to those who remain vocal about their interest, social and political activism and are critical of government in getting their voices publicly disseminated in just one glance, it is also of increasing competition following suit among those of different, if not irreconcilable voices and interests. And as more social and political activities are taking place online, data privacy is a matter of great importance. Nevertheless, what is more concerning than that of the need for personal data protection law is that many Indonesian citizens are yet to be aware of the damage that can be inflicted by the absence of such legislation protecting personal data privacy. *Pro tempore*, there are a considerable number of individuals who *hitherto* are not even aware of what actual data protection law is. The casualties inflicted due to this ignorance is thus the unfamiliarity of harms inflicted by the likely data breach and the absence of public participation as stakeholders to call their government out pertaining to the urgency for personal data protection law.

TOKOPEDIA DATA BREACH

There are currently 128 out of 194 countries and independent territories, including nearly every country in Europe, Latin America and the Caribbean, Asia and Africa that have adopted data protection laws.[208] The European Union even has their General Data Protection Regulation (GDPR) which has been taking into force since May 2018.[209] However, Indonesia still has yet to pass its *ius constituendum*, to wit, Bill on Personal Data Protection among the emerging breaches of personal data and privacy committed by perpetrators, one of which is data breach of both consumers and merchants of one of the biggest technology companies specializing in e- commerce, Tokopedia.[210][211]

The data breach inflicted by third party not only harms those of consumers data comprising both general and specific information which can lead to fraught, racketeering and identity theft, this unfortunate event can and will hold back the prospective investors in investing in Indonesia's technology companies due to the legal uncertainty on personal data protection. In the absence of personal data protection law which to a great extent has inflicted legal vacuum, by no means do we have a party to be held accountable if data breaches are to

[208] United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide (2021) *available at* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[209] GDPR EU, What is GDPR, the EU's New Data Protection Law?, GDPR EU (2021) https://gdpr.eu/what-is-gdpr/(*last accessed* March 19, 2021).

[210] Paulina Herasmaranindar, "RI Butuh RUU Perlindungan Data Pribadi, Singapura hingga Malaysia Sudah Atur", Kumparan News (2021) *available at* https://m.kumparan.com/kumparannews/ri-butuh-ruu-perlindungan-data-pribadi-singapura-hingga-malaysia-sudah-atur-1v2usbz47hN

[211] Eisya Eloksari, Tokopedia Data Breach Exposes Vulnerability of Personal Data, The Jakarta Post (2020), *available at* https://www.thejakartapost.com/news/2020/05/04/tokopedia-data-breach-exposes-vulnerability-of-personal-data.html?utm_campaign=os&utm_source=mobile&utm_medium=ios (*last accessed* March 19, 2021).

continue to take place. In the case of Tokopedia, not only has its users been put at a great disadvantage, Tokopedia will also most likely forfeit their prospective investors.

POLICY RECOMMENDATIONS

It has always been a matter of great importance and Indonesia must have a consistent and committed stance towards such an issue. Government and the national legislature must put a greater concern on data protection by putting the Bill on Personal Data Protection into the National Legislation Program. And in transition process, the government will have to ensure that all companies within the legal jurisdiction of Indonesia comply with the existing regulations concerning the use and management of electronic data, which are *hitherto* being regulated in Law No. 11 of 2008 regarding Electronic Information and Transactions (EIT Law) as amended by Law No. 19 of 2016 (EIT Law Amendment); Government Regulation No. 71 of 2019 regarding Provisions of Electronic Systems and Transactions (Reg. 71); Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation); Article 40 & 42 of Law No. 36 of 1999 regarding Telecommunications as partially amended by Law No. 11 of 2020 on Job Creation or generally referred to as the Omnibus Law; Article 6 & 17 of Law No. 14 of 2008 regarding Disclosure of Public Information; Law 7 of 1992 as amended by Law 10 of 1998 on Banking and as partially amended by Law No. 11 on Job Creation ("Banking Law") and Law 8 of 1995 on Capital Markets ("Capital Markets Law") respectively; and Article 21 of Financial Services Authority Regulation No. 38/POJK.03/2016 as partially amended by Financial Services Authority Regulation No. 13/POJK.03/2020 on the Implementation of Risk Management in the Utilization of Information Technology by the Bank.[212]

CONCLUSION

As more social and economic activities are taking place online, data privacy is a matter of great importance. We are constantly being asked to grant general and specific information such as our ID, credit card number, driving licence, health insurance, criminal record, so on and so forth as a key provision in exchange for the products and services we use. And what is currently being concerned with is the absence of data protection law in Indonesia which is to define and regulate the rights and obligations of the parties involved, that are to say, personal data owner; personal data controller; personal data processor; personal data protection officer; and the events occurring within such a system, such as personal data transfer inside and outside Indonesia's jurisdiction, end-to-end encryption, third party regulation, up to compliance with the regulation and administrative and criminal sanctions imposed for data breach. The absence of such regulation has inflicted a state of legal vacuum. The casualties inflicted due to legal vacuum is very much detrimental since there will be no party to be called to account when data breaches are to occur. This is why the national legislature should unanimously pass the bill, because the bill will not only protect

[212] DLA Piper, Data Protection Laws of the World: Indonesia (2021), *available at* https://www.dlapiperdataprotection.com/index.html?t=law&c=ID (*last accessed* March 19, 2021).

citizens, it will protect everyone. Citizens, politicians, activists and companies. It is to protect all of us. And it should not be politicised. It should be humane.

PROTECTING PERSONAL DATA IN THE ERA OF PLATFORM ECOSYSTEMS

By Tran Ngoc Minh; Nguyen Van Thu; Tran Duc Long

Industry 4.0 was born with the explosion of high technologies such as cloud computing, the Internet of Things, and Big Data analytics, among others. Together, it is blurring the boundaries of three realms: the physical, the digital and the biological. This creates a digital economy platform called a platform ecosystem. Within this ecosystem, consumers have enjoyed the full package of fast and modern products and services that enable them to just sit at home and enjoy all conveniences such as online learning, therapy products, ordering, catering services, relaxation services, online medical assistance, among many others. In recent years, digital platforms and ecosystems are quickly advancing as the business model that flourishes the most in the digital economy. However, in contrast to the fast, low-cost utilities, data scandals like the Facebook-Cambridge Analytica incident involving the illegal collection and sale of consumers' personal information have shocked the world. More importantly, it sparked a series of legislative debates in the United States and Europe, as well as a shift in consumer perceptions of privacy and in the protection of personal information of consumers. This raises two questions of data protection in the use of platforms and platform ecosystems: "Do users freely make a choice in sharing data in an ecosystem?" and "What are the coping mechanisms enacted by lawmakers to protect users' information from leaking from one platform to another in an ecosystem?" To address these questions, this article will cover restrictions from a legal perspective and thereafter give an analysis on protecting user information in the ecosystem platform.

INTRODUCTION

"Ecosystem" is not a new word, especially in the field of technology. In 2003, Apple fired the first shot when it released iLife, a bundled package that included iPhoto, iTunes, iMovie and iDVD. Not long after the first iPhone, Android was presented by Google as a counterweight to iOS. Since then, the world witnessed the rapid change in user experience, and the fall of giants in the mobile phone industry, Nokia and Blackberry. Those two companies had wrongly predicted the course that the modern citizen would take in using phone and smartphones—that people would still only pay attention to performance, security, or celebrity endorsement—and thereby capitalized on their advantages, but iOS and Android instead created a place for content creators and game developers to meet users, called a platform. In fact, digital platforms and ecosystems are quickly advancing as the business model that flourishes the most in the digital economy.

Users have always had various options in apps and games, while for operating systems, they had only two or three to choose from. But in those two or three systems, users could fulfill every need such as studying, working, entertainment, and even security from smartphone viruses. While the basic platform ecosystem model alone has disrupted industries like retail, travel, and mobility, some companies that aren't digitally native are shaping their platform and ecosystem strategies to create value and stay competitive. More and more companies present users' IDs so that they can receive gifts and vouchers in their "ecosystem," mostly in fintech and retail. Through their dominant position in a particular market, they can attract users, sell more and make higher profits. For example, one corporation in the real estate industry invested in retail and created a platform to promote offers to customers in other branches, then successfully converted the data they collected into outstanding sales. While this success was made possible by many factors, still, a platform strategy grounded on understanding customers and creating products that target customer segments is not the least among them. This situation is similar to what Lundqvist (2020) mentioned on firms that pool business data and may use the same, not to advance their services or products, but to collude, to exclude competitors or to abuse their market position.

To clarify the risks of consumer rights violations respecting personal information in a platform ecosystem, the authors proceed in the following order:

1. Consumer data protection concepts in platform ecosystems; and
2. Cross-country legal analysis on consumer data protection on platform ecosystems.

CONSUMER DATA PROTECTION CONCEPTS ACROSS PLATFORM ECOSYSTEMS

In defining *consumers*, there are many different concepts and perspectives to consider. From an economic perspective, "The consumer is any economic unit that has the need to end up consuming goods and services … Normally, the consumer is considered an individual but in reality, consumers can be agencies, individuals and groups of individuals."[213] From a legal perspective, *consumer* means a person who buys goods or services for personal, family or household use without the purpose of reselling."[214] This definition once again affirms that consumers are characterized by an individual or organization directly using goods or services. Such a definition makes it easier and more reasonable to solve problems directly related to products and services because here, consumers are the ones directly using and experiencing them.

As for the definition of *personal data*, the 1980 OECD Guidelines[215] defines it as any information relating to an identified or identifiable individual, called the data subject. Similarly, Article 4.1 of the EU's General Data Protection Regulation (GDPR) defines it as

[213] David W. Pearce, The Dictionary of Modern Economics, Aberdeen Economic Consultants, Palgrave Macmillan, London (1983), *available at* https://doi.org/10.1007/978-1-349-17125-5 (*last visited* July 7, 2021).
[214] Bryan A. Garner, & Black, Henry C. Black, Black's Law Dictionary (9th ed. St. Paul, MN: West, 2009).
[215] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

"any information relating to an identified or identifiable natural person."[216]

The right of consumers to protect their personal information is accessed through the angle of human privacy. Privacy is a fundamental human right. Privacy has two main functions: freedom from physical access and promoting liberty of action. When infringements of this right are prevented, the individual is separated from distractions and hindering factors resulting from contact with others. Protecting individual privacy is essential for a democratic society because it promotes the autonomy of every citizen.[217]

To understand the concept of a cross-platform ecosystem, we first need to analyze the fundamental concept. In general, platforms are connected by a network of nodes. In the past, the network was often envisioned in tangible terms, such as the transportation network, the electricity and water networks. Nowadays, under the development of information technology, invisible networks like the internet develop and become popular. Since then, the definition of *multi-platform ecosystem* has been developed as follows: "A multi-platform ecosystem is a system of digital platforms with separate functions but links to create a variety of types of goods and services to serve the needs of consumers under an integrated experience."

Developing business models towards building a multi-platform ecosystem has become a trend because it helps businesses in the ecosystem to maximize profits, and at the same time help consumers to have more access to goods and services on the market. It entails the need to protect consumers' data on multi-platform ecosystems for two (2) reasons: inequality in the position of consumers in the platform ecosystem and consumer data protection being the driving force behind a platform ecosystem.

Inequality in the position of consumers in the platform ecosystem

It must be emphasized that consumers have always been identified as the weak side in the relationship of transactions with suppliers of goods and services, especially in view of identifying consumers as individuals, due to the typical consumer's lack of information or understanding. Set in a cross-platform ecosystem, where consumers are mostly single individuals with Internet-enabled devices, where it is virtually impossible to stay anonymous, the digital platform requires that consumer rights be extended. According to the European Consumer Organisation (BEUC), on digital platforms, many services do not require payment in money, but are often served based on data in the form of remuneration. In this sense, services are not free. Consumers actively provide personal and non-personal data in exchange for services, products, or content or to allow service providers to track them and collect data about their habits and preferences passively. This data is then typically sold to advertising networks, and in return, the service provider pays a fee.[218]

[216] General Data Protection Regulation (GDPR), art. 41, available at https://gdpr-info.eu (last visited July 7, 2021).
[217] Ruth Gavision, Privacy and the Limit of the Law, 444–445 (2012).
[218] The European Consumer Organisation, Ensuring consumer protection in the platform economy, 8 (2018).

According to the above theory, users voluntarily share their personal information, purchase and search behavior for platforms in exchange for a "free" service. But consumers are often unaware of what information they voluntarily and actively provide and how it is used; moreover, with the expansion of platforms, consumers are forced to choose between sharing information in exchange for convenience and connection with a seller on one hand and being outside and not enjoying the benefits offered by the platform on the other. And as consumers step into these online platforms, the platforms also use a number of techniques to keep users in their own ecosystems. One of these techniques is to push users towards the so-called "filter bubble."[219] While platforms may represent these functions as "personalizing the user experience," the filter bubble is designed to maximize the amount of platform-specific user attention and to keep giving them as much time as possible on the platform itself, generating as much advertising revenue as possible. Real users are not aware of this, and these actions have been referred to by the European Data Protection Supervisor as a form of online manipulation.[220]

[219] A filter bubble is a term coined by the Internet activist Eli Pariser to refer to a state of intellectual isolation that can result from personalized searches when a website algorithm selectively guesses what information a user would like to see based on information about the user, such as location, past click-behavior and search history.
Engin Bozdag, *Bias in algorithmic filtering and personalization*, Ethics and Information Technology. 15 (3): 209–227 (September 2013).

[220] European Data Protection Supervisor, EDPS Opinion on online manipulation and personal data (March 2018), *available at* https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf (last visited July 7, 2021).

Consumer data protection being the driving force behind a platform ecosystem

Consumers are a very important factor for the development of commercial activities, and are the target of most businesses. Consumers' needs and preferences are the driving force behind competition among businesses. The success or failure of a business depends on consumer confidence in that business. Platform ecosystems activities are not an exception: the larger the number of individuals participating in platform ecosystems, the higher the level of socialization. This creates a large market for businesses, prompting them to choose platform ecosystems as their product distribution channel.

In platform ecosystem activities, a feature of the collection and use of consumer personal data is the intervention of technological factors in the process. Platform ecosystems serve as a vehicle for transactions associated with electronic data transmission. Personal data of consumers are stored electronically. Therefore, customer's personal data are regularly collected and used not only for the present transaction but also for future transactions. For example, today's businesses often focus on building and exploiting customer data through what is called "customer relationship management" (CRM). Through CRM, businesses approach and communicate with customers in a systematic and effective way to better serve customers, to maintain relationships with customers, to bring back old customers, and to reduce spending, marketing fees and customer service extensions. By detecting and analyzing

data, businesses can identify a list of potential and long-term customers to come up with a reasonable customer care strategy. With the support of the new technological trends brought about by the Industrial Revolution 4.0, modern data-processing and analysis chips have been designed to extract every piece of data of the consumer and even information that consumers provide to entirely separate channels (causing information externalities).

CROSS-COUNTRY LEGAL ANALYSIS ON CONSUMER DATA PROTECTION ON PLATFORM ECOSYSTEMS

The first country to enact a complete personal data protection law was Sweden in 1973. In 2020, about 120 countries around the world have issued laws related to the protection of personal data under different forms. Some countries enact their own laws on data protection that are specified in other specialized laws; others also note general provisions in their constitutions and civil laws. The law on protection of personal data in the world can be divided into 3 main models:

The European model with a central ideology of individualism and protection of privacy for personal data. The EU GDPR is considered to be one of the world's strictest laws on personal data protection. The GDPR is a privacy law that gives individuals much control over data collection, use, and protection. This act sets out strict rules about the data security that organizations collect, including the use of technical protections such as encryption and stricter accountability when collecting data.

The US model approaches personal data protection at a level of more harmony between the rights and interests of sensitive security information owners and other entities. At the federal level, the US Federal Trade Commission (FTC) has broad authority in enforcing data protection regulations. However, the US does not have a comprehensive federal law regulating the protection and use of personal data. Personal data protection is regulated by state laws and guidelines developed by government agencies, such as:

1. The US Privacy Act of 1974;

2. The Gramm-Leach-Bliley Act 1999 (GLBA);

3. The Children's Online Privacy Protection Act 2000 (COPPA); and

4. The Guide to Protecting the Confidentiality of Personally Identifiable Information 2010 by the National Institute of Standards and Technology (NIST).

The US model is a minimalist approach in which lawyers play an important role in enforcement. However, there is growing public concern about the amount of private data that businesses collect. In fact, the protection of consumers' privacy and data in e-commerce in the US is mainly done through self-regulation methods within the e-commerce industry. Self-regulation measures are divided into four groups: (i) self-building guidance; (ii) e-commerce privacy authentication program, where businesses commit to protecting the privacy of e-commerce; (iii) technology protection

methods, focusing on protecting the privacy of consumers by using software technology to automatically warn what information web pages will be collected, allowing consumers to both decide in advance what data will be collected, and pre-select what data is allowed; (iv) the "safe harbor" method, a new method combining self-regulation with legislative rules. This method is used to update privacy protection guidelines in e-commerce, issued by specific online service providers.

The mixed model is a combination of the two above models applied in some Asian countries such as Japan and South Korea. Countries following this model often enact a separate privacy law or protection law to centrally and comprehensively regulate relevant issues. In combining features of the European and American models, this adjustment becomes more reasonable and harmonious. A notable example of this model is Japan's Act on Protection of Personal Information (APPI) of 2003, as amended. The core principles in APPI are based on a combination of the OECD Guidelines and the EU Directives. Japan is also a member of Asia-Pacific Economic Cooperation (APEC), so the APPI was made in compliance with the APEC Code of Conduct. The APPI does not establish a central privacy protection enforcement and governance body. Instead, with the enforcement of industry-governed privacy regulations, each industry regulator is responsible for regulating privacy in that area. The amendment to the APPI established a Personal Information Protection Commission (PIPC). The PIPC has substantial powers including audit rights, auditing rights, and requiring companies to submit reports on privacy compliance.[221] However, the degree of harmonization is most reflected in the fact that the 2017 amendment to the APPI allows companies to purchase and sell personal data that have been anonymized or aggregated to enable and encourage the use of big data Analysis in Japan. The APPI has a series of EU-style guidelines that apply to data flows to be transferred to domestic and international third-party service providers, including requirements for data monitoring transferred to a third party. However, there is still a large difference between the APPI and GDPR. For example, the purpose of the APPI is to protect the legitimate rights and interests of individuals while ensuring proper consideration of the usefulness of personal data according to the general principles of personal data privacy. Meanwhile, the GDPR prioritizes protecting the privacy of individuals when moving data within the EU.

The APPI only applies to personal data use by enterprises, and personal data will not be considered infringed if the purpose of use is promptly made known to data subjects or publicly announced after the enterprise acquires personal data, unless the intended use has been made public. Meanwhile, the GDPR requires that personal data be collected for specific, explicit purposes and not further processed in a manner incompatible with those purposes.

It can be seen that each country has a tendency to adjust their own data privacy laws

[221] Robert Healey, How the Japan APPI compares to GDPR Are you Compliant? (2021) *available at* https://relentlessdataprivacy.com/how-the-japan-appi-compares-to-gdpr-are-youcompliant/?fbclid=IwAR008P7P6bRjdy3zvmxg1ZY3MH5OGJtCDGq7l-EK-glk3udiHfVfbd7h28U, (*last visited* July 7, 2021)

depending on their own economic, political, social, cultural, and geographical conditions, situation and needs. However, in the context of strongly developed information technology and increasing concerns about the privacy rights of personal data, countries around the world have been tending toward legislating tighter privacy regulations.

CONCLUSION

The first prerequisite for building a cross-platform ecosystem as well as implementing digital transformation is to win the trust of its users, creating a legal corridor for protecting data. In the current context, ensuring security in the digital space is the key to building trust in consumers. Because they are vulnerable, cross-platform ecosystems need fitting protection measures. And by looking at models of personal information protection in different countries, we find laws that regulate personal data privacy in different ways—whether tightly, minimally, or somewhere in between—depending on their unique considerations. However, we can see the trend of increasingly stricter regulations on the protection of personal information of countries around the world in the context of strong information technology and privacy concerns with increasing amounts of personal information.

FINTECH'S RISE IN THE TIME OF PANDEMIC: DATA PRIVACY REQUIREMENTS

By Gisela Tracy Gracia King

"Data is the most valuable commodity on earth today."

As the COVID-19 virus pandemic continues to be highly transmissible, responses by different governments to these health emergencies differ but point toward the same disruption of the normal occurrence in people's lives. This ongoing outbreak has posed various problems that immensely affect our daily lives, as the implementation of Governor Regulation No.79 of 2020 compels people to adhere to large-scale social restrictions and to stay at home. One by one, countries began to enact regulations that established lockdowns to maintain discipline and order, as well as to decrease the number of infected cases. This led to schools, universities, offices, and businesses being shut down, spreading economic suffering worldwide. Hence, people are left with no option but to utilize technology in their daily lives.

There has been a strong uptake in digital solutions, as people are turning into online options, making Financial Technology (**"Fintech"**) businesses largely resilient in spite of the pandemic. A joint study by the World Bank, the Cambridge Center for Alternative Finance at the University of Cambridge's Judge Business School, and World Economic Forum shows that the fintech market has continued to help expand access to financial services during the COVID-19 pandemic—particularly in emerging markets—with strong growth in all types of digital financial services.[222] Fintechs based in Indonesia, such as Investree and Tunaikita, have helped small and medium enterprises (**"SMEs"**) to get loans at a lower cost with digital-friendly services that outstrip conventional banks, as only 12% out of 60 million SMEs in Indonesia can get financing or bank loans.[223] In smaller aspects, fintech has helped self-isolation much easier, since online services that are practically covering every industry imaginable can be paid through fintechs. It is safe to say that fintech has

[222] The World Bank, https://www.worldbank.org/en/news/press-release/2020/12/03/fintech-market-reports-rapid-growth-during-covid-19-pandemic (last visited on Mar. 3, 2021)

[223] Nurhastuty K. Wardhani and Marc Bohmann, How fintech can help Indonesia's small and medium enterprises survive the COVID-19 pandemic, The Conversation (Nov. 5, 2020, 09:30 A.M.), https://theconversation.com/how-fintech-can-help-indonesias-small-and-medium-enterprises-survive-the-covid-19-pandemic-148528.

played a role in helping people battling the COVID-19 pandemic.

However, recent advances in information technology threaten privacy and have reduced the number of control over personal data, and open up the threats as a result of access to personal data.[224] According to The Jakarta Post, data on almost 3 million users from fintech aggregator platform Cermati.com was leaked and sold online for US$2,200 on Oct. 28. The leaked data includes names, addresses, bank accounts, emails, mother's maiden names, tax numbers, and passwords.[225] Similar case happened at US fintech giant– Dave–as it has admitted to a breach of customer's personal data via a third-party supplier after researchers found a database containing millions of records for sale online.[226] Fintech may be bringing opportunities in the banking and financial industry, but it also comes with challenges. To address this challenge, many countries are adopting policies similar to General Data Protection Regulation (**"GDPR"**) as well as data sovereignty regulations.[227] This highlights the vulnerability of user data in digital platforms and therefore the urgency to ratify Indonesia's Personal Data Protection bill (**"PDP Bill"**).

First and foremost, **Indonesia is yet to have a specific and comprehensive law about personal data protection**. Article 28G Paragraph 1 of the 1945 Constitution states that every person shall be entitled to protection of his/her own person, family, honor, dignity, and property under his/her control, as well as be entitled to feel secure and be entitled to protection against threat of fear to do or omit to do something being his/her fundamental right–implicitly mentioning the right to protect personal data. In addition, there is a minimum of 30 regulations that contain clauses on personal data protection, such as Law No.11 of 2008 on Electronic Information and Transactions, Law No.24 of 2013 on Amendment to Law No.23 of 2006, Law No.8 of 1999 on Consumer Protection, Law No.36 of 1999 on Telecommunications, Ministerial Regulations No. 20 of 2016 on Protection of Personal Data in Electronic Systems, etc. Despite this, the existing regulations remain sporadic and siloed. In addition, Indonesia's progress on data protection is slow in comparison to other ASEAN countries, such as Singapore, Malaysia, Thailand, and Philippines.[228] This is

[224] Van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, *Privacy and Information Technology*, The Stanford Encyclopedia of Philosophy (2020), https://plato.stanford.edu/archives/sum2020/entries/it-privacy/.

[225] Eisya A. Eloksari, Fintech Cermati data breach points to urgency for data protection law: Experts, The Jakarta Post (Nov. 5, 2020, 03:13 P.M.), https://www.thejakartapost.com/news/2020/11/05/fintech-cermati-data-breach-points-to-urgency-for-data-protection-law-experts.html.

[226] Phil Muncaster, US Digital Bank Dave Admits Customer Data Breach, Info Security (Jul. 27, 2020), https://www.infosecurity-magazine.com/news/us-bank-dave-admits-customer-data/.

[227] Subianto and Ravi Ivaturi, Personal data protection key as fintech grows, The Jakarta Post (Dec. 26, 2019, 10:58 A.M.), https://www.thejakartapost.com/academia/2019/12/26/personal-data-protection-key-as-fintech-grows.html.

[228] Agus Tri Haryanto, Bukti Indonesia Terlambat Punya UU Perlindungan Data Pribadi, Detik (Jan. 28, 2020, 09:10 P.M.), https://inet.detik.com/law-and-policy/d-4877050/bukti

where the PDP Bill came into the picture. Once the PDP Bill is ratified, Indonesia will be the 127th country in the world to implement regulations aiming at data protection.[229]

On 24th January 2020, the Indonesian President, Mr. Joko Widodo, signed the PDP Bill that is now being finalized by the House of Representatives.[230] Although the PDP Bill will not be the first personal data protection law in Indonesia, it sure will be the most important one yet since it has a greater scope of protection and insurance, acknowledging the rights and obligations of the stakeholders involved. The PDP Bill aims to protect the privacy of individuals with respect to their personal data and governs the relationship between individuals and entities processing their personal data. It simultaneously strives to create a robust digital economy by ensuring innovation through digital governance.[231]Nonetheless, the House of Representatives plans to conclude deliberations on the PDP Bill in the first quarter of 2021, a delay from its initial target of finishing it in October 2020.[232]

The PDP Bill adopted several principles and aspects of the European Union's GDPR, which focuses on five main areas: data collection, data processing, data security, data breach, and the right for individuals to have their personal data erased.[233] However, the PDP Bill, in contrast to the GDPR, does not refer to data owners as "identified or identifiable natural persons or data subjects"; rather, it uses the term "persons or corporations", which thus calls for specifications for applicable protections.[234] The final draft law has 72 articles in 15 Chapters discussing the following topics:[235]

1. The definition and types of personal data;
2. The rights of data owners;
3. The processing of personal data;
4. The obligations of data controllers and processors when processing personal data;
5. Transferring personal data;
6. Administrative sanctions;
7. Prohibitions against certain uses of personal data;
8. The establishment of behaviour guidelines for personal data controllers;

-indonesia-terlambat-punya-uu-perlindungan-data-pribadi.

[229] *Ibid.*

[230] PwC Digital Services, https://www.pwc.com/id/en/publications/digital/digital-trust-newsflash-2020-02.pdf. (last visited on Jan. 15, 2021)

[231] Trilegal, https://www.trilegal.com/index.php/publications/analysis/the-personal-data-protection-bill-2019. (last visited on Mar. 3, 2021)

[232] Imantoko Kurniadi, RUU PDP Ditargetkan Rampung Maret 2021 Mendatang, Selular Id (Dec. 29, 2020, 16:00 P.M.), https://selular.id/2020/12/ruu-pdp-ditargetkan-rampung-maret-2021-mendatang/.

[233] News Desk, Indonesia to conclude data protection bill in November, The Jakarta Post (Sep. 2, 2020, 07:38 P.M.), https://www.thejakartapost.com/news/2020/09/02/indonesia-to-conclude-data-protection-bill-in-november.html.

[234] Indonesia's Personal Data Protection Bill. H.R., (2021).

[235] Indonesia's Personal Data Protection Bill. H.R., (2021).

9. The dispute resolution over the use of personal data;
10. International cooperation; and
11. The roles of the government and the public.

The current finalization of the bill begs the question, **is the PDP Bill comprehensive enough?** A preliminary study at Tifa Foundation comparing the PDP Bill with two leading international personal data protection instruments, the Convention 108+ from Council of Europe (**"CoE 108+"**) and GDPR, found two major shortfalls of the PDP Bill.[236]

The first problem is **the lack of detail in the PDP provisions**.[237] This can be found in Article 9, where it specifies the conditions of consent and the right of data subjects to withdraw consent without mentioning any provision that necessitates that withdrawing consent should be as easy as providing consent.[238] It also fails to include the fundamental principles of data protection, such as privacy by design, privacy impact assessment, and privacy by default.[239] It is crucial to point out that there is the creation of a Personal Data Controller (**"PDC"**), which can be a person, a business, or even a corporation that is responsible for controlling and processing personal data that is collected, and a Personal Data Processor (**"PDPr"**) that process personal data on behalf of the PDC.[240] However, the PDP Bill is not specific enough with regard to the obligations of PDC and PDPr in today's digital age. The second problem is **the absence of arrangements of the supervisory authority to enforce the law when enacted**.[241] Article 58 paragraph 2 of the PDP Bill only stipulates that the implementation of PDP will be executed by the Ministry of Communications and Information Technology, showing the lack of clarity on the powers and roles of the data protection authority.[242] Due to the absence of such authority, one can only assume that when the data subject claims for his or her rights, the communication will be direct between the data subject and the PDC and/or PDPr. However, this procedure has no guarantees from the supervisory authority to ensure the implementation of a request from the data subject by the PDC or PDPr, making the future fulfillment of the law rely excessively on the knowledge of individuals to protect their personal data.[243] Although the PDP Bill to a large extent mimics the data protection principles in current international standards, those two major gaps might obstruct the enforcement of the law once it is enacted.[244]

---

[236] Sherly Haristya and Shita Laksmi, How comprehensive is personal data protection bill?, The Jakarta Post (Nov. 18, 2020, 01:00 A.M.), https://www.thejakartapost.com/paper/2020/11/17/how-comprehensive-is-personal-data-protection-bill.html.

[237] *Ibid.*

[238] Indonesia's Personal Data Protection Bill. H.R., (2021).

[239] *Ibid.*

[240] *Ibid.*

[241] *Ibid.*

[242] *Ibid.*

[243] Sherly Haristya, Shita Laksmi, An Nisa Tri Astuti, and Intan Fatma Dewi, *Preliminary Study: A Comparison of Indonesia's Personal Data Protection Bill with Europe's Convention 108+ and General Data Protection Regulation,* Tifa Foundation (2020), https://www.tifafoundation.id/yayasan-tifa-preliminary-study-a-comparison-of-indonesias-pdp-bill-with-coe-108-and-gdpr/.

[244] *Ibid.*

To address the problem raised, researchers at Tifa Foundation propose a way forward. First, authorities must **add more clarity on the data protection rules and fill in the gaps of the roles and responsibilities of the data protection authority**.[245] There is still a need for the government to identify the regulations needed to complement the PDP Bill and act in the principle of "*lex superior derogat legi inferiori*" whereby a statutory provision lower in hierarchy shall act in accordance with the higher ones, hence the local government can be repealed if it is contradictory with the higher regulation. Another way to address the problem is **for the government to establish a dedicated data protection authority that could lead the enforcement efforts,** not only of private sector actors, but also all the ministries and government institutions.[246] Lastly, the government needs **to acknowledge the different types and capacities of actors to comply with the law when it is enacted**.[247] The bill has to recognize that the role of supervisory authority must be able to educate different actors on the importance of personal data protection for the sustainability of their businesses and empower them to comply with the law.[248]

Indonesia is at the forefront of digital transformation. In order for this to continue, Indonesia must have effective ICT-related regulations, such as the proposed PDP Bill. Once the PDP Bill is ratified, it will be the first Indonesian law to provide comprehensive regulations aiming at data protection, not only via an electronic system but also via analog systems, while also playing a critical part for people to have a sense of security in the digital world. The PDP Bill will enable Indonesia to build an environment that is conducive for economic growth. However, challenges in formulating comprehensive regulations cannot be avoided, which is why Indonesia needs to regulate meticulously by assuring that the bill accommodates all of the fundamental principles and enforcement mechanisms to implement the law effectively.

[245] *Ibid.*
[246] *Ibid.*
[247] *Ibid.*
[248] *Ibid.*

ASIAN LAW STUDENTS' ASSOCIATION

ALSA Law Review Magazine
Volume 9 . Issue No. 1
July 2021