ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 558

Proceedings of the Asia-Pacific Research in Social Sciences and Humanities Universitas Indonesia Conference (APRISH 2019)

ASEAN for Data Protection:
Remarks On 2016 ASEAN Framework on Personal Data Protection and The Impact Towards Regional Peer to Peer Lending

Salsabila Siliwangi Surtiwa[1*] and Christian Jeremia Gultom[1]

[1]*Faculty of Law, Universitas Indonesia, Depok, Jawa Barat, Indonesia*
**Corresponding author. Email: salsabila.siliwangi@ui.ac.id*

ABSTRACT

Technology in loan and banking has become faster and easier to access by everyone. One of the popular forms of the loaning-money method is peer-to-peer lending (P2PL), that creates a platform for lenders and borrowers to make an agreement for loaning. By this transaction through P2PL that using the digital platform, on the flow of users data through the area, including between states in the region. ASEAN remarks one of the significant of P2PL's growing users and this challenge of protection of privacy data through the transaction. The ASEAN Framework regarding the protection of the private data of the user is one of the basic need to help the guideline through the protection of data users regarding in P2PL transaction. Besides that, this framework will help the country in ASEAN to create and strengthen the policy for the protection of data privacy. But, this paper also highlights the problem of the implementation of any ASEAN legal frameworks and to compare it with the newly established European Union's General Data Protection Regulation (GDPR) and the future issues it foresees regarding cross-border crowdlending activities, especially P2PL.

Keywords: *Peer-to-Peer Lending, Data Protection, ASEAN*

1. INTRODUCTION

Ubi societas ibi ius. As part of society, humans play a role in each other's lives as a social creature. By doing so, they fulfill their own interest and their needs to survive. As each society has its own dynamics, it requires them to establish the game rules agreed upon by its own members. This self-regulating system--the law--is referred to social norms.

Technology makes up a very big part of human's everyday lives, especially in this century. Technological advancement has also allowed humans to push beyond all limits. Activities then shift into the virtual world, making limitless opportunities and networks all across the globe. Without them knowing humans have slowly become more dependent towards information and communication technology (ICT). From pre-industrial to industrial mass era, we have come a long way and may claim that 21st century the age of networks, as networks become essential in our society (van Dijk, 2006).

As mentioned before, networking today knows no boundaries with the help of internet. The dependence of humans' activities on the internet has created new empires within the virtual world, starting from casual interactions, economic activities, to integrated electronic government. It possesses trillions of information called Big Data. Big Data, which will be further explained in the next section, comprises many activities, some yet to be recognized by the existing positive law. This includes cross-border economic activities such as Peer-to-Peer Lending (P2P). It is safe to say that the era of the Internet of Things and big data has changed society tremendously over these past few decades. But one question remains: how is the existing regulation catching up with all these developments?

In accordance with several comments on the relation between law and social changes, the law itself is often unable to catch up with the dynamics. This phenomenon leaves several legal gaps. These legal gaps are indicated with an act yet to be regulated, the legal system to be outdated, and/or the law to be contradictive with the common practice. As we explore deeper the issues of personal data protection in ASEAN countries, this paper aims to discuss 2016 ASEAN Framework on Personal Data Protection that will be able to answer problems and resilient towards cross-border peer-to-peer lending issues that may occur in the next few decades.

2. DEFINITIONS

2.1. Network Society

The network society is a social structure based on networks operated by information and communication technologies based in microelectronics and digital computer networks that generate, process, and distribute information on the basis of the knowledge accumulated in the nodes of

networks. In the network society structure, the computer networks play a significant role, that information is created, processed and transmitted, buildings the knowledge in the network hubs. Members of the network society are not alienated people, but rather individuals who cultivate highly developed systems of relationships. The value of the individual is positively reappraised in the network society and make "communication space" that change the form of the media through individuals.

2.2. Big Data

Big Data is one of the trending issues and the next step of the Internet of Things (IoT). Big Data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation (Beyer & Laney, 2012). Big data shows how data become behavioral optimization and "personalized law", and as large-scale data analysis and predictive technologies are used to prescribe behavior and generate legal directives and recommendations precisely tailored to the client or regulated entity (Devins, et al, 2017).

2.3. ASEAN

On 8th of August 1967, Foreign Ministers from Indonesia, Malaysia, Singapore, Philippines, and Thailand met to agree on the ASEAN Declaration or Bangkok Declaration. The declaration consists of five articles, but the content would become the basis for the establishment of ASEAN. The objectives included economic growth, social progress, and cultural development; regional peace and security; cooperation in the economic, social, cultural, technical, scientific, and administrative fields; mutual assistance in matters of training and research; cooperation in agriculture and industry, trade, transportation and telecommunications, and in improving living standards; Southeast Asian studies promotion; and collaboration with other regional and international organizations (Severino, 2008). With the existence of various ASEAN policies, one of the missions is to form an integrated ASEAN while sticking to the values it adheres to. Today, ASEAN consists of 10 (ten) member states.

2.4. Financial Technology and Peer-to-Peer Lending

Financial Technology (Fintech) is proof of how disruptive innovation in the area of finance, including how the financial services industry structures, provisions, and captures customers demand (McWaters, 2015). One of the forms of Fintech itself was Peer-To-Peer Lending (P2PL) as one of alternative lending. P2PL is new lending platforms are transforming credit evaluation and loan origination as well as opening up consumer lending to nontraditional sources of capital (McWaters, 2015). The implication of this form are giving alternative lenders to leverage online platforms and by this method, P2PL platforms provide customer low-cost, fast, flexible, and customers-oriented rather than traditional financial institutions (McWaters, 2015).

3. ANALYSIS

3.1. Identifying P2PL in ASEAN Countries, especially cross-border issues

Society never remains the same forever. It will always be fluid to changes, either major or minor; either as the whole system or parts. These changes are parallel to time concept; as time passes, the focus and issues of society will be richer in varieties. Humans will react to these dynamics by adjusting, changing, or adding new elements to their social interactions.

One of the issues—or quests—that have been constantly encountered by humans is how to make their lives easier. In other words, humans love to challenge the concept of time and space; how do we shorten the distance between places? How do we make things go faster? How do we spend less energy to accomplish our objectives? These questions then lead to findings—new innovations. These innovations are often referred to as technology.

In this context, these changes refer to borderless nations, where information can quickly be distributed to the other side of the world as a consequence of technological advancement. The main game changer is the rapid usage of internet. On the internet, all data flows non-stop without limits. There are not enough meaningful boundaries to protect data, including personal data contained within so-called Big Data. Big Data is generally utilized in three sectors; public sector by intelligence services, the police or the tax authorities; private and semi-public sector to cater to specific objectives; and to improve economic activities (Lens, 2018).

One of the now trending economic activities lies within the Fintech category. There are many varieties of Fintech, in which one of them is P2PL. P2PL is seen as a prospective economic activity in ASEAN as it makes up eight percent of the whole Fintech market. This was motivated by the limited formal banking credit availability for Micro, Small, and Medium Enterprises (MSMEs) while the former sole alternative to keep small businesses alive was to ask credit from loan sharks. With easier terms and methods of payment, P2PL arose to its fame in the region (Young, Sim, & Leong, 2017).

The global Fintech industry gives US$24 billion of money flow in investment in 2016. For the ASEAN region, in 2016, the Fintech investment reaches US$252 million, increase US$62 million from 2015 (33 percent) (Andreasson, Aloysius, & Ross, 2018). Total investment up to September 2017 has already exceeded that of 2016 to reach US$338 million (Young, Sim, & Leong, 2017). Up to 2017, there are 1228 Fintech industries that spread over 6

ASEAN countries, with the number of distribution shows that Singapore took 39 percent of the Fintech industry, Indonesia at 20 percent, Malaysia at 15 percent, Thailand at 10 percent, the Philippines at 9 percent, and Vietnam at 6 percent (Young, Sim, & Leong, 2017). For P2PL, the growth in ASEAN countries shows increasing of P2PL transaction. P2PL growth from US$ 0.50 million (2013) to US$ 1.12 million (2014) and reach US$ 9.53 million (2015) (Zhang, et al, 2016). In Indonesia, at least 120 Fintech firm was operated with overall transactions estimated reach US$ 14.5 billion in 2020 (increasing 18.8 percent from 2019) (Wirayabi, 2017). In Singapore, P2PL growth to 14 percent from 2013 to 2015 with transaction reach US$ 9.55 million (Zhang, et al, 2016).

Fintech, including P2PL, now even caters to people outside certain countries. One of Indonesia's Fintech company, Modalku's Fintech P2PL has distributed loans with a total of IDR 5.2 trillion to MSMEs in several Southeast Asia countries. The list includes Indonesia, Malaysia, and Singapore. This number makes up 40 percent of the whole loans channeled. Meanwhile, the amount has been calculated since Modalku began operating in January 2016 (Qolbi, 2019). Modalku itself is affiliated with Funding Societies, the biggest P2P online marketplace based in Malaysia, whose one of the popular services was providing unsecured term loans to MSMEs in Southeast Asia (DigFin, 2017).

With the mainstream adoption of internet users, a new technological threat to privacy appeared. Collections of personal data were stored in databases around the world and were being traded and combined to mine new insights into individuals and groups (Meessen & de Vries, 2017). In P2PL, the user's data often use for the purposes of commercial business. This data can be transferred and transform into big data and cloud computing to create a group of data to learn the behavior of the customer. Besides that, privacy data can also be used by lenders to force borrowers to pay the debt in full immediately by hiring debt collectors. On the loan's due date, some customers received intimidating text messages and phone calls from debt collectors, telling them to pay their debt in full immediately (this payment consists of interest rate and fines that are unexpectedly unfair for the customers). In some cases, the debt collectors contact the person from the contact list of borrowers and terrorized them (Rahman, 2018).

3.2. ASEAN Data Protection and Privacy: A Commitment for Better Data Protection

After the conflict between Cambodia and Vietnam (the conflict had become ASEAN's main concern at that time) was over, the political atmosphere in ASEAN gave the impression that ASEAN's raison d'etre was increasingly blurred (Nesadurai, 2009). Failure to initiate AFTA (which finally returned to the surface in 2015) was due to dynamics. So, it takes a form of reaffirmation of ASEAN's position. In 2003, through the Declaration of the ASEAN Concord II, ASEAN also initiated a new organ which each represented the three pillars (Gonzalez-Manalo, 2009). The initiation is called the ASEAN Community, which consists of the ASEAN Security Community, ASEAN Economic Community, and the ASEAN Socio-cultural Community (ESCAP, 2009). This initiative was carried out to enhance regional cooperation in the fields of politics and security and in the social and cultural fields. ASC aims to maintain peace between member countries and the world through a just, democratic and harmonious environment (Supancana, 2008). AEC functions to formulate market standardization and harmonization of policies to accommodate economic transactions across boundaries between members (Saputro, 2017). ASCC was formed with the aim of realizing an ASEAN community that is inclusive and has a social spirit through a common identity or family (ESCAP, 2009).

The integration then comes to a certain extent, including in the field of data privacy and its protection. Over the past decade, international data flows have increased global GDP by 10.1 percent. Besides that, data flows accounted for US$2.8 trillion of global GDP in 2014 (McKinsey, 2016). As a response towards this rapid increase of data flow related to regional peace and security, ASEAN Telecommunications and Information Technology Ministers initiated a framework to strengthen the region's data ecosystem. In 2016, the ASEAN Minister adopted the ASEAN Framework on Personal Data Protection that set the principles and basic rules of implement the protection of data privacy both national and regional level. This includes achieving legal and regulatory alignment of data regulations and governance frameworks in the region and fostering data-driven innovation to boost the growth of the digital economy through regional integration (GSMA, 2018).

It should be noted that 2016 ASEAN Framework on Personal Data Protection does not create any legally binding obligations, neither on national level nor international level, as it only reflected the state members' commitment to protecting personal data from being misused without any meaningful consequences. The Philippines would co-lead one of the four initiatives called the ASEAN Data Protection and Privacy Forum. Its two objectives are to harmonize the legal landscape between Southeast Asian countries; and the development and adoption of best practices. To date, the Philippines is one of only three Southeast Asian countries with comprehensive data protection law and fully-established functioning data privacy authority regulator.

Some countries in ASEAN have not regulated the specific data privacy related to P2PL, but they regulate the data flow across the territory related to P2PL activities. The paper will mention three countries, which are Indonesia, Malaysia, and the Philippines. In Indonesia, the data protection is derived under three principal regulations; Law No. 11 of 2008 on Electronic Information and Transaction, later amended by Law No. 19 of 2016 (EIT Law). The EIT law regulates activities about the use of electronic information and legal conducts involving the use of computers or any other form of electronic media. Article 26 of Law No 11 of 2008 mandated that the "use of any information through electronic media that involves personal

data of a Person must be made with the consent of the person concerned" and by the amended law, a right of individuals to request the deletion of his personal data, as well as to request the deletion of personal data where they are no longer relevant (the so-called Indonesian "right to be forgotten") (ABLI, 2018). Second, the Government Regulation No. 82 of 2012 on the Implementation of the Electronic Information and Transaction Law that further detailed regulation of the EIT Law requires that any electronic system provider (i.e, "any Person, state agency, Business Entity, and community that provide, manage, and/or operate Electronic System individually or jointly to Electronic System User for its interest or other party's interest" (Article 1(4)) must ensure that the collection, use, and disclosure of personal data is based on consent from the "owner of personal data" (ie, the data subject), unless otherwise provided by regulations. Data may be disclosed to a third party only if that disclosure is in line with the original purpose for which the data had been originally collected from the data owner (ABLI, 2018). The third relevant regulation is Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (MCI 20/2016). By that specific regulation, on Article 21(1) requires that any display, announcement, transfer, dissemination or provision of access to personal data in an electronic system can take place only with the individual's consent unless otherwise regulated by other applicable laws and regulations, after the verification of the accuracy of the personal data and that it is in line with the purposes of gathering and collecting the personal data. On Article 22(1) mandates that any cross-border transfer of personal data outside of Indonesia is to be coordinated with MCI or an authorized entity, as well as comply with applicable laws and regulations on cross-border transfer of personal data. These provisions will be further elaborated on below (ABLI, 2018).

In Malaysia, the data privacy regulation stipulates under the Personal Data Protection Act 2010. The PDPA will apply to data users in three circumstances: (a) Firstly, where the data user is established in Malaysia and the data user processes data, whether or not in the context of the establishment. (b) Secondly, when the processing is done by any person employed or engaged by the data user established in Malaysia. (c) Thirdly, when the data user is not established in Malaysia but uses equipment in Malaysia to process personal data (ABLI, 2018). The general principles of the data user to process specify that consent has to be "recorded" and "maintained", which implies that express consent is needed. It seems "implied consent" can be adequate, provided that the person/individual has been made completely aware of the goal regarding the processing of his personal data (ABLI, 2018). Besides that, using the data privacy must doing notice and choice principle (section 7), disclosure principle (section 8), security principle (section 9), retention principle (section 10), data integrity principle (section 11), access principle (section 12), rights of data subject (part II, division 4), registration of data users, offences and liability, enforcement mechanism, and international data transfers. Section 129(1) of the PDPA is the provision of the Act which regulates the transfer of personal data outside of Malaysia. As a rule, this section provides that a data user shall not transfer any personal data to a place outside Malaysia, unless such place has been specified by the Minister, upon the recommendation of the Commissioner, by notification published in the Gazette. In the absence of a published white list, data users in Malaysia must rely on one of the exemptions provided by section 129(3) of the PDPA in order to transfer personal data outside Malaysia. These exemptions include (among others): (a) where the data subject has consented to the transfer; (b) where the transfer is necessary for the performance of a contract between the data subject and the data user; (c) where the transfer is necessary to protect the vital interests of the data subject; and (d) where the data user has "taken all reasonable precautions and exercised all due diligence" to ensure that the personal data will not be processed in the recipient country in a way that would be a contravention of the PDPA (ABLI, 2018).

In the Philippines, there were Republic Act No 10173, otherwise known as the Data Privacy Act of 2012 ("DPA"), with respect to enforcing this legal framework, it is the National Privacy Commission ("NPC") that primarily handles this, including the application of the rules on international data transfers and the NPC is helmed by the Hon Raymund E Liboro as Commissioner. The Philippines' approach to liability regarding cross-border transfers is fairly simple: it is the personal information controller who is responsible for ensuring the protection of personal information under its control or custody – even when such personal information has been transferred to a third party outside of the country for processing. Personal information controllers are required to use contractual or other means to ensure that the third-party entity to whom the personal information is to be transferred for processing provides a comparable level of protection as that of the Philippines (ABLI, 2018). Republic Act No 10175, otherwise known as the Cybercrime Prevention Act ("CPA"), serves to complement the DPA in terms of protecting data within the Philippine legal framework (ABLI, 2018).

3.3. Analyzing the problem of ASEAN Framework: ASEAN Law?

It should be noted that all policies carried out by ASEAN are using a mechanism known in foreign relations, namely "ASEAN Way". This, in its application, even raises questions about the enactment of ASEAN policies on the problems it encounters as it often lacks compliance of the head of state to follow the consensus and consultation given by ASEAN. With so much pressure from foreign parties and their influence on the decision, it can be said that "ASEAN Way" is a myth in its implementation. The existence of policies made by ASEAN should maintain the fundamental principles, in which its one of the most important pillars is the existence of cooperation among countries. On the other hand, it should be noted that the community with such

security awareness can still unite despite different backgrounds (Nischalke, 2000).

Reflecting on past experience, especially conflicts that occur between member states, the discourse arises regarding the mechanism of decision making and its implementation in ASEAN. It cannot be denied that each country needs to reduce its ego in terms of resolving disputes and seeking regional integration. In addition, regional anatomy is needed to solve regional problems. The octagonal interpretation and main principles in the application of The ASEAN Way, namely non-interference, need to be reviewed, especially regarding security. Security is often perceived as an internal problem, not an external one. So that intervention from other member states is often a trigger for conflict (Wiwasukh, 2017). It can be seen in the example of the Rohingya crisis, especially with the refugee problem, the principle of cooperation and non-interference carried out simultaneously. The Rohingya crisis as a global problem can be taken with the application of the principle of non-interference if member countries can cooperate so that they do not depend on foreign assistance. For example, there is an increase in the acceptance of refugees from ASEAN member countries (Hasan & Yudarsan, 2017).

This situation can be contextualized with the establishment of 2016 ASEAN Framework on Personal Data Protection. To ensure the enactment of this framework, it is necessary to measure the willingness of member states to be committed. Personal data protection is a matter of human rights, but one of the very delicate ones. The high rate of sensitivity on this case causes difficulty to put a light on a unanimously agreed framework even though most member states see it essential to be regulated.

By that framework, there are several numbers of personal data flow cross border through the ASEAN region. As opposed to local data storage and forced localization which are currently only enforced in a small number of countries, laws regulating personal data are more common (Greenleaf, 2014). The large volume of personal data that is obtained, used and transported to other countries, including that of third parties, raise concerns and region focus about how personal data and control over one's own data. As the volume of personal data processed increases, so does the concern from individuals regarding how their personal data are being used. Some sort of privacy legislation and data protection which limits the application and transfer of either personal or any sensitive data had been adopted by more than a hundred countries (Haufler, 2013). This kind of regulation is meant to rein in risks of abuse of personal information and to preserve individuals' right to information privacy. Companies across different industries are obliged to comply with the aforementioned laws, which create difficulties arising from restrictive or burdensome laws as well as differing legal frameworks between countries, which in turn generate higher compliance costs and unpredictability for firms. By this occasion, the role of government across the ASEAN to protect and ensure the privacy data protection through this online and P2PL transaction is an urge. By establishing the rule of protection across the border in ASEAN, the country provides the protection and how the third parties using this credential data for restricted purposes.

3.4. Comparisons to the European Union's General Data Protection Regulation (GDPR)

In order to understand better the impact of a regional regulation regarding personal data protection towards cross-border P2PL activities, this paper will compare the already existing system from other regionals, specifically the European Union. European Union has established regional personal data protection regulation which is applied to any virtual activities, including financial technology such as P2PL. P2PL makes up 75% of the total crowdfunding market in the United Kingdom, and more than 50% of other European markets. This significant growth is displayed by 2015 number that shows €4.4 billion in volume for P2PL market in the UK, and €1 billion in other European markets outside the United Kingdom (Zhang, et al, 2016).

P2PL utilizes big data analytics to combine and examine large economic data, including personal information of users. This includes the personal information generated from the internet, such as social media activities, personal background information, and other digital footprints. All this data is taken to analyze the borrower's probability of default as an alternative to assess the historical relationship with the conventional banking system (Lenz, 2016).

P2PL activities among European Union countries have been regulated in the respective countries. In the UK, the Financial Conduct Authority established rules for P2PL in 2014. Platforms became subject to the principal elements of regulation that other financial intermediaries were subject to. With this, the P2PL industry in the UK is a subject to the authority and supervision of a single entity and is regulated comprehensively. There is also an established organization that caters to P2PL companies, the Peer to Peer Finance Association (P2PFA) which is self-regulatory to control the market with respect. Portugal has also adopted a law regulating crowdfunding (Law no. 102/2015 of 25 of August) whose regulation imposes to P2PL and other crowdfunding activities. According to the law, P2PL platforms are subject to the authority and supervision of the Comissão de Mercado de Valores Mobiliários (the entity in charge of the supervision of the securities market) (Pacheco, 2018).

In what regards data protection regulation, both the UK and Portugal are now subject to the GDPR, despite UK's Brexit, which regulates companies that require personal data processes despite the size or kind industry, that process personal data when performing their activities. This regulation not only applies to companies based in the territory of the EU Member States, but also to companies that process EU citizens personal data. This regulation will limit P2P platforms' ability to process data when performing their activities (Pacheco, 2018).

The single most important innovation of the GDPR is the operationalization of accountability requirements that make organizations liable not just to comply with the law but to be able to demonstrate how they comply. This shifts the burden onorganizations to step up and take responsibility. In return, organizations are allowed a certain degree of flexibility and the regulatory approach shifts from ex-ante to ex-post. It also further adapts the EU's longstanding rights-based approach to privacy (GSMA, 2018).

One of the issues that may arise regarding data protection in P2PL is P2PL platforms collect a large amount of personal and credit data, which leaves borrowers vulnerable in case the platform suffers, for example, a cyber-attack or misuse of the information by the employees. Plus, borrowers share personal information on the platform website making it available to everyone who accesses the platform and, although platforms censor personally identifying information from loan listings and borrowers' profiles, sometimes the information displayed is enough to discover the identity of the borrower (Pacheco, 2018).

Although there has been little to no evident of issues regarding cross-border P2PL arisen in European Union, the rising number of P2PL activities in the national level of countries shown before opens a great possibility for MSMEs in Europe to demand people to conduct P2PL activities cross-border. With that being said, the regarded and established GDPR has helped to connect and bridge gaps between the future possibility of Fintech and the importance of personal data protection.

4. CONCLUSION

As the future sets with financial technology development as the center of the market, it is important to foresee future possibilities of digital businesses and the issues that come along with it, including and especially the issues of data protection. The breaching of data privacy, identity theft, and blackmails are some of the potential issues that will be faced as MSMEs grow and spread, especially in P2PL activities in which personal data plays an essential role in the process. The problems do not also harness within the territory, but also beyond boundaries. Although recent situations have yet to show concrete issues nor court cases regarding cross-border P2PL, it is not impossible for Southeast Asian countries to popularize P2PL in the region with the growing economy.

One of the main problems that have to be tackled is how ASEAN legal framework can be implemented effectively. Regional policy has been recently initiated with the establishment of ASEAN Data Privacy and Protection. One question arises: how will the ASEAN countries apply the policy to future cross-border issues. This is reflected by the history of policies designed in which they often face compliance issues among ASEAN countries. With this being said, ASEAN countries should make sure that the regulation meets the interests of the state members see fits.

REFERENCES

[1] Jan A.G.M. van Dijk, The Network Society: Social Aspects of New Media, (London: Sage Publications, 2006), p. 2.

[2] Mark Beyer, Douglas Laney, The Importance of 'Big Data': A Definition, in https://www.gartner.com/en/documents/2057415/the-importance-of-big-data-a-definition access on 21 June 2019.

[3] Caryn Devins, et.al., "The Law and Big Data", in Facial Analytics: From Big Data to Law Enforcement, Vol. 45 No. 9, p. 358.

[4] Rodolfo C. Severino, Southeast Asia Background Series No.10: ASEAN, (Singapore: Institute of Southeast Asian Studies, 2008), p. 1-2.

[5] World Economic Forum, The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned, and consumed, in http://www3.weforum.org/docs/WEF_The_future__of_financial_servisssces.pdf, p. 13.

[6] Margot Lens, "GDPR & Convention 108: Adequate Protection in a Big Data Era?" (Paper presented at Tilburg University on 8 June 2018), p. 7.

[7] Janet Young, Pauline Sim, & Arthur Leong, "State of FinTech in ASEAN," United Overseas Bank Report (2017), p. 17.

[8] Kim Andreasson, Scott Aloysius, Charles Ross, "Fintech in ASEAN: Unlock the Opportunity," The Economist Intelligence Unit (2018) p. 5

[9] Bryan Zhang, et.al., Harnessing Potential: The Asia-Pacific Alternative Finance Benchmarking Report, Cambridge: Cambridge Centre for Alternative Finance, 2016), p. 83.

[10] Prima Wirayabi, "Fintech to further grow with the new rule," https://www.thejakartapost.com/news/2017/01/05/Fintech-to-further-grow-with-new-rule.html, accessed on June 23, 2019

[11] Nur Qolbi, "Fintech Modalku telah salurkan pinjaman Rp5,2 trillion ke Tiga Negara di ASEAN," https://keuangan.kontan.co.id/news/Fintech-modalku-telah-salurkan-pinjaman-rp-52-triliun-ke-tiga-negara-di-asean accessed on June 22, 2019.

[12] DigFin, "Capital Match Taking on Funding Societies in Regional P2P arena," https://www.digfingroup.com/capital-match/ accessed on June 22, 2019.

[13] Paulus Nicolas Meessen, Arjen de Vries, Long Term Data Storage Using Peer-to-Peer Technology, Radbound University (2017), p. 11.

[14] Riska Rahman, "They terrorized me every day: Fintech debtors tell of abuse," https://www.thejakartapost.com/news/2018/11/06/they-terrorized-me-every-day-Fintech-debtors-tell-of-abuse.html accessed on July 02, 2019.

[15] Helen E.S. Nesadurai, "ASEAN and regional governance after the Cold War: from regional order to regional community?" The Pacific Review, Vol. 22 No. 1 (Maret 2009), p. 92.

[16] Rosario Gonzalez-Manalo, "Drafting ASEAN's Tomorrow: The Eminent Persons Group and the ASEAN Charter" dalam Tommy Koh, Rosario G. Manalo, & Walter Woon, eds., The Making of the ASEAN Charter, (Singapore: World Scientific Publishing, 2009), p. 39-40.

[17] The United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), Striving Together: ASEAN & The UN, Cet. 2, (Bangkok: United Nations Publication, 2009), p. 1-2.

[18] I.B.R. Supancana, "The Roadmap toward the Creation of ASEAN Security Community in 2015: Legal Perspectives," Journal of East Asia & International Law, Vol. 1 (2008), p. 325.

[19] Eko Saputro, Indonesia and ASEAN Plus Three Financial Cooperation, (Singapura: Palgrave Macmillan, 2017), p. 219.

[20] The United Nations Economic and Social Commission for Asia and the Pacific (ESCAP), Striving Together: ASEAN & The UN, p. 30.

[21] McKinsey Global Institute, Digital Globalization: The New Era of Global Flows, (New York: McKinsey&Company, 2016), p. 10.

[22] GSMA, "Regional Privacy Frameworks and Cross-Border Data Flows," GSMA Reports (September 2018), p.13.

[23] ABLI Legal Convergence Series, "Regulation of Cross-Border Transfer of Personal Data in Asia", (Singapore: Asian Business Law Institute, 2018), p. 142.

[24] Tobias Ingo Nischalke, "Insights from ASEAN's Foreign Policy Co-operation: The "ASEAN Way", a Real Spirit or a Phantom?" Contemporary Southeast Asia, Vol. 22, No. 1 (April 2000), p. 112

[25] Montree Wiwasukh, "ASEAN Response to Politics of New Regionalism", p. 73-74.

[26] Muh. Hidayat Hasan dan Muh. Akbar Yudarsan, The Relevance of Non-Interference in ASEAN, Proceedings of ISER International Conference, Tokyo, Japan, January 29-30 2017, -. 23-24

[27] Graham Greenleaf, "Asian Data Privacy Laws: Trade and Human Rights Perspectives", (Oxford: Oxford University Press, 2014), p. 457.

[28] V Haufler, "A Public Role for the Private Sector: Industry Self-regulation in a Global Economy", (Carnegie Endowment, 2013), p. 135.

[29] Bryan Zhang, Peter Baeck, Tania Ziegler, Jonathan Bone, and Kieran Garvey, Pushing Boundaries: The 2015 UK Alternative Finance Industry Report, Cambridge: Cambridge Centre for Alternative Finance, 2016, p. 39.

[30] Rainer Lenz, "Peer to Peer Lending: Opportunities and Risks," European Journal of RIsk Regulation, Vol. 4 (2016), p. 690.

[31] Ines Tomaz da Costa Pacheco, "Regulating the Online Peer-to-Peer Lending Industry: A proposal for a regulatory approach in the US," (In partial fulfillment of the requirement for the degree of Master of International Business Law Tilburg University, June 6, 2018), p. 51-54.