Pertanika J. Soc. Sci. & Hum. 28 (3): 2295 - 2307 (2020)

PERTANIKA JOURNALS

SOCIAL SCIENCES & HUMANITIES

Journal homepage: http://www.pertanika.upm.edu.my/

Personal Data Protection in P2P Lending: What Indonesia Should Learn from Malaysia?

Russel Butarbutar

Faculty of Law, University of Indonesia, Depok, 16424, West Java, Indonesia

ABSTRACT

The question raised in this study is how personal data should be protected and can solely be used for the commercial interests of one party, which is closely related to consumer protection. Specifically, it focuses on how Indonesian laws protect the abuse of personal data exchange, especially in peer-to-peer (P2P) lending platforms and how these laws compare with Malaysia's. The results show that in Indonesia, there are no clear regulations on personal data protection in P2P lending; it is regulated by unclear protective treatments and no strict sanction regarding personal data protection. EIT Law, GR 82, MOCI Regulation 20, and FSA 77/2016 cannot guarantee the validity and reliability of personal data protection. Indonesia should learn from Malaysia, mainly from its Personal Data Protection Act (PDPA) which not only protects personal data but also imposes sanctions and has been implemented since 2013. Therefore, P2P lending platforms operating in Indonesia must be required to comply with Indonesian laws and regulations that are relevant to their activities, location, and legal structure.

Keywords: Indonesia, Malaysia, personal data protection, peer-to-peer lending

ARTICLE INFO

Article history:
Received: 17 December 2019
Accepted: 10 April 2020
Published: 25 September 2020

E-mail address:
russelbutar@gmail.com

INTRODUCTION

Legal violations of personal data are carried out by accessing, storing, and manipulating personal computers connected to the internet (Kantaatmadja et al, 2002). As a type of alternative finance, peer-to-peer (P2P) lending requires access to personal data (Mokhtarrudin et al., 2017). Loans offered through online platforms are cheaper than

ISSN: 0128-7702
e-ISSN 2231-8534

traditional financial institutions (Ghazali, 2018).

The question raised in this study is how personal data should be protected and can only be used for the commercial interests of one party, which is closely related to consumer protection (Mateescu, 2015). The public should be made aware of the importance of the regulation of personal rights protection (privacy rights). The increasing growth of P2P lending platforms in Indonesia has given importance to conduct a study regarding personal data protection.

Conceptual Approach

The Definition of Peer-to-peer Lending. P2P lending platforms provide convenience in speed, data processing, accessibility, and other appliances compared to traditional financing (Pokorná & Sponer, 2016). However, this also implies that debtors in several segments can increase their dependency on this funding source (Carney, 2017). Investors in P2P lending are faced with a big risk as they are not professionals (Lee & Lee, 2012).

Data Protection in Peer-to-peer Lending. In P2P lending, the need for data protection must be doing to reduce the risk of other people's actions accessing and sharing personal data without consent (Zarza, 2015). An example of this is the case of Facebook facing charges regarding the use of unauthorized data (Editorial Board, 2019). In contrast, social media companies regularly collect and occasionally share user data (with consent) (Carney, 2017). To create an acceptable data protection strategy, a business needs to focus holistically on proactive and reactive activities that synergize with storage strategy developments, while having an effective backup or recovery strategy (De Guise, 2017).

The Comparison Between Indonesia and Malaysia in Data Protection on Peer-to-Peer Lending. In Indonesia, P2P lending is regulated through:

1. Law Number 11 of 2008 regarding Electronic Information and Transactions, as amended by Law Number 19 of 2016 (EIT Law).
2. Government Regulation Number 82 of 2012 regarding the Implementation of Electronic Systems and Transactions (GR 82).
3. Ministry of Communication and Information Technology Regulation No. 20 of 2016 regarding Personal Data Protection in Electronic Systems (MOCI Regulation 20).
4. Financial Services Authority (FSA) Regulation Number 77/POJK.01/2016 regarding Lending Services and Information Technology-Based Loans or Peer-to-Peer Lending Financial Technology (FSA 77/2016).
5. Bank Indonesia Regulation Number 19/12/PBI/2017 regarding Financial Technology Implementation (PBI 19/12/2017).

FSA 77/2016 regulates P2P loans made in Indonesian Rupiah (ABNR Counsellors at Law, 2017). The main parties involved in P2P lending are providers, debtors, and lenders, which are manifested in two types of electronically-conducted agreements, namely agreements between providers and lenders and agreements between lenders and debtors (ABNR Counsellors at Law, 2017).

Under Article 28 paragraph (3) FSA 77/2016, to ensure complete security of electronic document storage, Providers (Other Financial Services Institution) must participate in managing data security (Investasi Online, 2019).

However, to improve the quality of P2P Lending services, Providers can cooperate and exchange personal data with technology-based support service providers. The latter tends not to seek approval from data owners, which increases the risk of misuse of personal data exchange (Article 23 FSA 77/2016).

In contrast, Malaysia has established the protection of personal data through the 2010 Personal Data Protection Act (PDPA) which is successfully implemented in 2013 under the supervision of the Personal Data Protection Commission (PDPC) (Shahwahid & Miskam, 2015). To become P2P operators, companies must procure a license from the Malaysia Securities Commission (SC). SC licensed platforms are required to verify business propositions and creditworthiness to all potential publishers (iMoney.my, 2019). In May 2016, SC has regulated publisher and investment services that can participate in P2P through new guidelines in Chapter 13 (Securities Commission Malaysia, 2016b). Through this regulation, Malaysia becomes the first country in the ASEAN that regulate P2P lending (The International Comparative Legal Guides [ICLG], 2019b). In Malaysia, a fintech company must be: (1) an official or registered business as defined in the 2013 Financial Services Act and (2) an official business as defined in the 2013 Islamic Financial Services Act; or (3) a money services business as defined in the 2011 Money Services Business Act (Bank Negara Malaysia, 2016).

In Malaysia, The Central Bank of Malaysia (BNM) and SC are the main regulatory bodies that govern licensing and marketing requirements for fintech companies (Kandiah, 2019). There are two reforms to the regulation of fintech businesses in Malaysia. First, through the Financial Technology Enabler Group, BNM launched a Regulatory Sandbox in 2016. Second, it is based on the 2007 Capital Market and Services Law (Section 377 CMSA 2007) regarding digital asset guidelines. Therefore, digital currencies and tokens will be regulated by the SC so that they can eventually be used (Kandiah, 2019). The SC can conduct periodic assessments on the compliance of the IEO operator on any of its regulatory obligations and request documents and assistance (Securities Commission Malaysia, 2020). In 2016, the SC had established management responsibilities in dealing with cyber risks, including (1) maintaining the confidentiality and sensitivity of entity data; (2) protecting

information vulnerabilities and operating systems of the entity; (3) preventing existing and future cyber threats (Securities Commission Malaysia, 2016a).

Methods

This is normative legal research, a research methodology used to find legal rules, principles, or doctrines (Marzuki, 2005). This is also doctrinal research (Yaqin, 2008) with a comparative (Cruz, 1999; Soekanto, 1986), and statute approach (Marzuki, 2005) that reviews the laws and regulations related to personal data protection in both Indonesia and Malaysia in connection with P2P lending. Secondary legal resources are books or articles on P2P, data protection, and consumer protection studies written by scholars. The data gathered were then analyzed using the qualitative data analysis method.

RESULTS

Peer-to-Peer Lending Platforms

P2P lending has and will continue to exist and develop (Zhang et al., 2016), For example, Prosper.com facilitated $ 1 billion in funding and served more than 200,000 customers. The online P2P lending market can offset the risk of asymmetric information that often occurs in traditional financial institutions because it is highly decentralized without direct contact between debtors and lenders (Lin et al., 2009).

Likewise, P2P lending in Indonesia is developing at a rapid rate. There are several P2P lending platforms, including Klik ACC, Investree, Modalku, Money Friends, KoinWorks, Akselerasi, Danamas, Amartha, and DanaKita. These sites can help young entrepreneurs to obtain capital. In transactions, investors can choose prospective debtors according to their financial history and profile (Investasi Online, 2019).

In 2018, Lembaga Pendanaan, B2B Finpal, and Fundaztic hold the largest market shares in Malaysia. To date, Lembaga Pendanaan leads with more than RM 2.06 billion in funds raised. There are also several sharia P2P lending platforms including Nusa Kapital and microLEAP Islamic (Lim, 2019).

How Information Can be Freely Accessed by Everyone. Advances in information technology have made it possible for personal data to be accessed internationally by anyone. However, the principle of privacy must take precedence over the principles of freedom of information. In connection with the international aspect of transborder data flow (TDF (Munir, 1999), countries need international regulations on TDF (Kantaatmadja, 2002).

There are two types of privacy, namely informational privacy, and autonomous privacy. Informational privacy includes the right of individuals to determine which personal information will be conveyed to others, whether confidential or sensitive. Meanwhile, autonomy privacy guarantees individuals' rights and freedom to carry out activities without interference from other parties (Garner, 2004).

Privacy is a state or condition free from public outreach, including interference with one's decisions or actions. It is essential to protect individuals from external threats, such as harassment, ridicule, theft, manipulation, extortion, exclusion, and subordination (Petkovic & Jonker, 2007). Privacy and data protection are related articulations resulting from complex interplays of decisions, location choices, difficult to identify, and associated moments (Gutwirth et al., 2011).

In practice, privacy is a soft concept based on the public perception of risks and benefits. For example, public trust rises when using a credit card in online purchases; it provides a greater convenience compared to the potential risk of transaction data that may be misused (Schilit et al., 2003).

In the United States, personal rights can be referred to as the supervision of information dissemination on personal data, specifically the right to determine the use of personal data by the government. In Europe, personal rights is a matter of protecting personal data (Kantaatmadja, 2002).

How Personal Data Should be Protected. Article 1 GR 82 regulates the protection, storage, maintenance of personal data. Furthermore, Article 2 paragraph (1) GR 82 regulates the protection of electronic personal data consisting of the collection, acquisition, transmission, processing, and destruction of personal data.

Article 2 paragraph (2) GR 82 regulates electronic system standards, and obtaining consent for confidential personal data, treatment of personal data as personal data, relevance to the purpose of obtaining, responsibility for collecting, processing, announcing, sending and disseminating personal data, including reporting to the data owner in the event of a data protection failure.

Personal Data Protection in Peer-to-Peer Lending in Indonesia

According to Article 29 of FSA 77/2016, providers must be transparent, fair, reliable, and trustworthy in protecting users and prioritize dispute resolution methods that are cheap, fast, and affordable. Likewise, Article 26 of FSA 77/2016 states that in addition to maintaining the confidentiality, integrity, and availability of personal, transaction, and financial data, providers must also notify users in the event of a failure to protect user data and confidentiality.

Articles 27 and 28 of FSA 77/2016 require operators to protect all components of information technology, secure P2P loans, provide monthly and annual reports, and carry out audits of all their activities.

Article 43 of FSA 77/2016 regulates restrictions on providers regarding the publication of fictitious and/or misleading information, offering something to users, and asking for payment when a user issues a complaint.

Article 47 FSA 77/2016 gives FSA the right to impose administrative sanctions in the form of written warnings and license revocation to providers who violate the rules.

MOCI Regulation 20 has not been able to protect personal data, especially on social media, online market places, and financial platforms (Editorial Board, 2019). Whereas in the European Union (EU), the European Commission since 1990 has proposed a Privacy Directive to regulate the use of personal data, as well as provisions concerning the right of subjects to request the deletion of data or the "right to be forgotten" which is regulated in the EU General Data Protection Regulation (Editorial Board, 2019) and were initially supported by 12 member countries (Madsen, 1992).

Article 30 of EIT Law only regulates the criminal act of illegally accessing someone else's electronic system (Chazawi & Ferdian, 2015). The unlawful nature of the actual action lies in the lack of permission from the owner of the electronic system, rather than the owner of personal data. Furthermore, "accessing" is defined as the activity of interacting with an established electronic system.

Therefore, Indonesian law does not regulate the protection and misuse of personal data (Suwana, 2018). Many P2P lending platform behaviors have contacted, threatened, and humiliated debtors (Editorial Board, 2019).

Personal Data Protection in Peer-to-Peer Lending in Malaysia

Fintech, such as equity crowdfunding (ECF) and P2P lending, provides technology convenience and benefits to the business world and provides cost-effective and efficient solutions to debtors (Kunhibava & Muneeza, 2020). In Malaysia, the SC functions to regulate fintech as an intermediary between business investors to provide investment and financing alternatives.

Meanwhile, personal data protection is regulated by the PDPA, passed by the Malaysian Parliament in 2010 (Hassan, 2012). According to section 5, PDPA regulates the principles of personal data protection in data processing, including general, notification and choice, disclosure, security, retention, data integrity, and access principles. Furthermore, data processing by third parties including data users, data processors, or people who are authorized in writing to process personal data under the direct supervision of data users is regulated in section 47.

In Malaysia, 97% of the total businesses consist of small and medium enterprises (SMEs) (ICLG, 2019c). SMEs in Malaysia, apart from getting financing from getting support from conventional and sharia banks. They are also supported by the Malaysian Security Berhad; and the Malaysian Government with the Malaysian SME Corporation through the 2012-2020 SME Master Plan (ICLG, 2019c).

All data users in Malaysia must comply with PDPA, including data users not established in Malaysia who process personal data using Malaysian equipment except for those that transit through Malaysia. Data users who transfer personal data outside Malaysia must understand and comply with the terms of data transfer

between the subject and the user for contract implementation, transfers for the summary performance of contracts between users and third parties, and data transfer agreements based on subjects (ICLG, 2019c). Section 4 of the PDPA regulates credit reporting based on the 2010 Credit Reporting Agent Act regarding commercial, investment, banking, financing, insurance, service, and agency transactions.

DISCUSSIONS

The protection of personal data in Indonesia is regulated separately in different laws and regulations, making it difficult to understand the scope of legal protections for personal data. Currently, data protection regulations overlap with one another. Providers can exchange data and cooperate with information technology-based support service providers to improve the quality of P2P lending, without any restrictions regarding the parties involved and the types of data being exchanged. Meanwhile, Article 47, FSA 77/2016 only applies to violations of obligations and restrictions but not to the protection of personal data as regulated in Article 23. Therefore, operators must take responsibility when P2P lending platforms want to announce and disseminate failed customer data through the use of certain applications to access and retrieve contact numbers, which is a legal violation of personal data protection.

Although the FSA is authorized to impose administrative sanctions on the operator, it may be imposed with or without prior administrative sanctions in the form of a written warning. Article 84 GR 82 does not apply sanctions for moral or civil violations, but only provides sanctions to those who commit administrative violations.

Criminal sanctions in Article 30 of the EIT Law are limited to the actions of anyone intentionally and without rights or unlawfully accessing computers and/or electronic systems in any way by violating, breaking through, surpassing, or breaking into security systems, being convicted with a maximum of 8 (eight) years of imprisonment and/or a maximum fine of IDR 800,000,000.00 (eight hundred million rupiahs).

To date, Indonesia does not have a legal rule concerning personal data protection. There are many cases of customer data misuse that occur in P2P lending. To conduct an assessment of prospective debtors, companies require thorough access to consumer phones, including telephone contacts. However, in some cases, contact access is used for billing (CNBC Indonesia, 2019). P2P lending providers collect crucial customer data, including sensitive personal information and financial records. They track online shopping and social media patterns for digital trace tracking. The data is then analyzed for marketing, sales, and data retrieval purposes such as creating a scoring system to determine customer profiles (Ng, 2018).

In contrast, the personal data protection laws in Malaysia are comprehensive and orderly that sanctions are quickly determined for violators through PDPA, including those that violate sensitive personal data

(Cieh, 2013) and cases related to fintech (Bromberg et al., 2017). PDPA adheres to the principles of the e-government security legal framework which includes general principles, disclosure, notification and choice, data integrity, security, retention, and data access (Sonny, 2012).

In a P2P application, the data distribution system is designed to provide control over data access and is shared with the participating community. Participants can share data bilaterally or multilaterally, using sophisticated platforms governed by the system. The decentralized data sharing model will create a new mechanism for exchanging trusted data among participants without requiring a single third party to handle the data. The main obstacle faced in this system is ensuring that participants actually share data (PDPC Singapore, 2019). In P2P lending, the operator is held responsible for the collection, assignment, and use of debtor data (Crowdfund talks, 2019).

To protect personal data, PDPA regulates the collection, use, and disclosure of personal data to recognize and balance the protection of individual rights with the need to collect, use or disclose personal data for purposes deemed appropriate by authorized individuals. This obligation is addressed to everyone who processes personal data and anyone who has control over or authorizes the processing of any personal data relating to commercial transactions conducted by Malaysian citizens using equipment in Malaysia, except for those that transit through Malaysia (Leong & Bakar, 2010).

Section 9 of the PDPA (Security Principles) states that data users must consciously protect their data, including taking practical steps. If processing is carried out by a data processor, the user is required to ensure the data processor must (1) provide adequate guarantees regarding technical security measures and the organization that govern the process, and (2) take reasonable action to ensure compliance with these steps (ICLG, 2019a).

The Personal Data Protection Commissioner ('Commissioner') is the main regulator that oversees data protection issues, appointed by the minister to carry out the functions and authorities granted under the PDPA on terms and conditions deemed appropriate. Commissioners are appointed by the Personal Data Protection Advisory Committee (Chambers & Partners, 2019).

P2P lending in Malaysia must comply with Malaysian laws and regulations that are relevant to its activities, location, and legal structure. The provisions of the Electronic Commerce Act 2006 govern the validity of electronic communications and transactions (ICLG, 2019b). Likewise, the 1998 Malaysian Communications and Multimedia Law must also be complied with by financial institutions, insurance companies, aviation service providers, and licensees (Chambers & Partners, 2019). On December 23, 2016, the commissioners completed and registered the Personal Data Protection Practice Code for the Insurance/ Takaful Industry. Then, on January 19, 2017, the commissioners completed the Personal Data Protection for the Banking

and Financial Sector. Furthermore, on November 21, 2017, the Commissioners completed the Code of Practice for the Transportation (Aviation) Sector (Chambers & Partners, 2019).

There are many decisions issued by commissioners regarding violations of personal data protection (Chambers & Partners, 2019):

- In November 2016, the PDPC requested the Malaysian Communications and Multimedia Commission (MCMC) to block websites under Section 130 of PDPA for the collection of unlawful personal data.
- In May 2017, the commissioners reported that they had sued and fined private tertiary institutions, hotels, and employment agencies. The fines imposed reached MYR 20,000 (around USD 5,000).
- In November 2017, the MCMC also blocked the microsite sayakenahack.com due to data privacy issues following an application from PDPC.
- In 2018, the PDPC imposed a fine of MYR 10,000 on employment agencies for processing personal data without obtaining a registration certificate from the Commissioner.
- Since January 25, 2019, the PDPC has investigated massive data breaches resulting in the leakage of 1,164,540 students' data and alumni records from leading Malaysian universities. This includes MyKad numbers, student names, email addresses, home addresses, campus codes, campus names, program codes, course levels, student IDs, and mobile numbers (Chambers & Partners, 2019).

Under Section 104 of the PDPA, after the commissioner receives a complaint, they will conduct an investigation related to the relevant data used to determine whether the actions specified in the complaint are contrary to the PDPA. If the complainant is not satisfied (disadvantaged), he can submit an appeal. Furthermore, if data users are not satisfied with the decision of the Personal Data Protection Advisory Committee, they can submit a review of the decision in the Malaysian High Court (Chambers & Partners, 2019).

Financial institutions (P2P lending platforms) are bound by their license terms and conditions, which will usually involve strict requirements relating to customer data processing, which often require customer data to be stored in Malaysia. This will depend on the category of approval obtained by the relevant financial institution (Chambers & Partners, 2019). Of course, any electronic processing of personal data in Malaysia will be subject to PDPA, and the commissioner can issue further guidance on this issue in the future (DLA PIPER, 2020).

If there is a failure in compliance, depending on which part/regulation is violated, a fine of RM 10,000-500,000 and/or imprisonment for up to three years is imposed. Then, if a legal entity commits

a crime, anyone who at the time of the violation was a director, chief executive, manager, secretary, similar official, and acted in the capacity as a legal entity, or the person responsible for all company affairs may be held liable under Article 133 of the PDPA (ICLG, 2019b).

Therefore, personal data protection systems that adhere to the principles of privacy, autonomy, transparency, and non-discrimination must be regulated in the personal data protection law in Indonesia (McDermott, 2017). This is particularly important in P2P lending which involves sensitive personal data (Liu & Kuhn, 2010) which is limited in commercial affairs (Cohen, 2018). To protect personal data in P2P lending, Indonesia should adopt Malaysian laws related to PDPA data protection and form a PDPC.

CONCLUSION

In Indonesia, there are no clear regulations on personal data protection in P2P lending; it is regulated by unclear protective treatments and strict sanctions regarding personal data protection. Moreover, the complexity of the P2P lending system makes it difficult to protect such data, to determine who is most responsible for personal data leaks, and to pinpoint users of illegal personal data. EIT Law, GR 82 regarding The Implementation of Electronic Systems and Transactions, MOCI Regulation 20, and FSA 77/2016 cannot guarantee the validity and reliability of personal data protection. Indonesia should learn from Malaysia, a neighboring country with a PDPA that has been protecting personal data, including the compliance system since 2013. Furthermore, in case of a failure in compliance, depending on which parts/regulations are violated, a fine of RM 10,000-500,000 and/or imprisonment of up to three years will be imposed. P2P lending in Malaysia must also comply with Malaysian laws and regulations that are relevant to its activities, location, and legal structure.

ACKNOWLEDGEMENT

Thanks to my primary supervisor, Prof. Hikmahanto Juwana, SH., LLM., Ph.D., and my colleagues in Ph.D. programme and academic staff at the Faculty of Law, University of Indonesia.

REFERENCES

ABNR Counsellors at Law. (2017). *OJK's regulation on financial technology-based lending services.* Retrieved October 25, 2019, from https://www.lexology.com/library/detail.aspx?g=0b387cf6-5564-4f5c-a9cd-8c202e26936e

Bank Negara Malaysia. (2016). *Financial technology regulatory sandbox framework.* Retrieved February 10, 2020, from https://www.bnm.gov.my/index.php?ch=57&pg=137&ac=533&bb=file

Bromberg, L., Godwin, A., & Ramsay, I. (2017). Fintech sandboxes: Achieving a balance between regulation and innovation. *Journal of Banking and Finance Law and Practice*, *28*(4), 314-336. Retrieved from http://www.fsa.gov.uk/pubs/other/turner_review.pdf

Carney, M. (2017, January 25). *The promise of Fintech–something new under the sun*. In Speech at Deutsche Bundesbank G20 Conference. https://doi.org/10.3386/w22476

Chambers & Partners. (2019). *Data protection & cybersecurity 2019.* Retrieved February 10, 2020, from https://practiceguides.chambers.com/practice-guides/data-protection-cybersecurity-2019/malaysia

Chazawi, A., & Ferdian, A. (2015). *Tindak pidana informasi & transaksi elektronik* [Information & electronic transactions crime]. Malang, Indonesia: Media Nusa Creative.

Cieh, E. L. Y. (2013). Personal data protection and privacy law in Malaysia. *In Beyond Data Protection*. Heidelberg, Germany: Springer.

CNBC Indonesia. (2019). *Fintech salahgunakan data konsumen, siap-siap kena denda* [Fintech misuses consumer data, get ready to get fines]. Retrieved February 10, 2020, from https://www.cnbcindonesia.com/tech/20190705141712-37-82978/fintech-salahgunakan-data-konsumen-siap-siap-kena-denda

Cohen, M. C. (2018). Big data and service operations. *Production and Operations Management*, *27*(9), 1709-1723.

Crowdfund talks. (2019). *Privacy policy.* Retrieved October 20, 2019, from https://crowdfundtalks.com/privacypolicy

Cruz, P. (1999). *Comparative law in a changing world* (2nd ed.). London, England: Cavendish Publishing Limited.

De Guise, P. (2017). *Data protection: Ensuring data availability*. New York, USA: CRC Press.

DLA PIPER. (2020). *Data protection laws of the world.* Retrieved February 10, 2020, from https://www.dlapiperdataprotection.com/index.html?c=MY&c2=&go-button=GO&t=law.

Garner, B. A. (2004). *Black's law dictionary.* St. Paul, USA: West Thomson.

Ghazali, N. H. (2018). Awareness and perception analysis of small medium enterprise and start-up towards fintech instruments: Crowdfunding and peer-to-peer lending in Malaysia. *International Journal of Finance and Banking Research*, *4*(1), 13-24.

Gutwirth, S., Poullet, Y., De Hert, P., & Leenes, R. (Eds.). (2011). *Computers, privacy and data protection: An element of choice*. Heidelberg, Germany: Springer Science & Business Media.

Hassan, K. H. (2012). Personal data protection in employment: New legal challenges for Malaysia. *Computer Law and Security Review*, *28*(6), 696-703. https://doi.org/10.1016/j.clsr.2012.07.006

The International Comparative Legal Guides. (2019a). *Malaysia: Data protection 2019.* Retrieved February 10, 2020, from https://iclg.com/practice-areas/data-protection-laws-and-regulations/malaysia

The International Comparative Legal Guides. (2019b). *Malaysia: Fintech 2019.* Retrieved November 11, 2019, from https://iclg.com/practice-areas/fintech-laws-and-regulations/malaysia

The International Comparative Legal Guides. (2019c). *Malaysia: Fintech 2019.* Retrieved November 11, 2019, from https://iclg.com/practice-areas/fintech-laws-and-regulations/malaysia

iMoney.my. (2019). *All you need to know about P2P lending in Malaysia.* Retrieved February 10, 2020, from https://www.imoney.my/articles/p2p-lending-guide

Investasi Online. (2019). *9 situs P2P lending indonesia terbaik dan terpercaya yang terdaftar OJK* [9 best and most trusted P2P lending sites in Indonesia registered by OJK]. Retrieved October 25, 2019, from https://investasi.online/peer-to-peer-lending-indonesia-terbaik/

Kandiah, S. (2019). *The financial technology law review.* Retrieved February 10, 2020, from https://thelawreviews.co.uk/edition/the-financial-technology-law-review-edition-2/1192796/malaysia

Kantaatmadja, M. K. (2002). *Cyberlaw: Suatu pengantar* [Cyber law: An introduction]. Bandung, Indonesia: ELIPS.

Kunhibava, S. B., & Muneeza, A. (2020). Regulating FinTech businesses: The Malaysian experience. In *Impact of Financial technology (FinTech) on Islamic finance and financial stability*. Pennsylvania, USA: IGI Global.

Lee, E., & Lee, B. (2012). Herding behavior in online P2P lending: An empirical investigation. *Electronic Commerce Research and Applications*, *11*(5), 495-503.

Leong, F., & Bakar, H. (2010). *Personal data protection act 2010.* Retrieved December 15, 2019, from http://static1.1.sqspcdn.com/static/f/419448/8974173/1287135355977/LH+Jul-Sept.pdf?token=A4mINOPhvtSauf3SN6hMPcaJv3g%3D

Lim, J.-L. (2019). *All you need to know about P2P lending in Malaysia.* Retrieved November 8, 2019, from https://www.imoney.my/articles/p2p-lending-guide

Lin, M., Prabhala, N. R., & Viswanathan, S. (2009). *Social networks as signaling mechanisms: Evidence from online peer-to-peer lending.* WISE 2009. Retrieved December 21, 2019, from http://people.stern.nyu.edu/bakos/wise/papers/wise2009-p09_paper.pdf

Liu, S., & Kuhn, R. (2010). Data loss prevention. *IT Professional*, *12*(2), 10-13.

Madsen, W. (1992). *Handbook of personal data protection*. Heidelberg, Germany: Springer.

Marzuki, P. M. (2005). *Penelitian hukum* [Legal research]. Jakarta, Indonesia: Prenata Medya.

Mateescu, A. (2015). *Peer-to-peer lending survey*. Data & Society Research Institute. Retrieved December 22, 2019, from https://www.datasociety.net/pubs/dcr/PeertoPeerLending.pdf

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, *4*(1), 1-7. Retrieved January 12, 2020, from https://doi.org/10.1177/2053951716686994.

Mokhtarrudin, A., Masrurah, I. M. K., & Muhamad, S. C. R. (2017). Crowdfunding as a funding opportunity for youth start-ups in Malaysia. *Pertanika Journal of Social Sciences and Humanities*, *25*(S), 139-153.

Munir, A. B. (1999). *Cyber law: Policies and challenges*. Kuala Lumpur, Malaysia: Butterworth Asia.

Ng, C. (2018). *Regulating Fintech: Addressing challenges in cybersecurity and data privacy.* Retrieved February 9, 2020, from https://www.innovations.harvard.edu/blog/regulating-fintech-addressing-challenges-cybersecurity-and-data-privacy

PDPC Singapore. (2019). *Purpose of trusted data sharing framework.* Retrieved February 9, 2020, from https://www.imda.gov.sg/-/media/Imda/Files/Programme/AI-Data-Innovation/Trusted-Data-Sharing-Framework.pdf

Petkovic, M., & Jonker, W. (Eds.). (2007). *Security, privacy, and trust in modern data management*. Heidelberg, Germany: Springer Science & Business Media.

Pokorná, M., & Sponer, M. (2016). Social lending and its risks. *Procedia - Social and Behavioral Sciences*, *220*(March), 330-337. https://doi.org/10.1016/j.sbspro.2016.05.506

Schilit, B., Hong, J., & Gruteser, M. (2003). Wireless location privacy protection. *Computer*, *36*(12), 135-137.

Securities Commission Malaysia. (2016a). *Guidelines on management of cyber risk.* Retrieved February 10, 2020, from https://www.sc.com.my/api/documentms/download.ashx?id=9aaddb2e-aa13-409a-a47f-8d0124afd229

Securities Commission Malaysia. (2016b). *SC Introduces regulatory framework to facilitate peer-to-peer financing.* Retrieved February 10, 2020, from https://www.sc.com.my/resources/media-releases-and-announcements/sc-introduces-regulatory-framework-to-facilitate-peer-to-peer-financing

Securities Commission Malaysia. (2020). *Guidelines on digital assets.* Retrieved February 10, 2020, from https://www.sc.com.my/api/documentms/download.ashx?id=dabaa83c-c2e8-40c3-9d8f-1ce3cabe598a

Shahwahid, F. M., & Miskam, S. (2015). Personal Data Protection Act 2010: Taking the first steps towards compliance. *Journal of Management & Muamalah, 5*(2), 64-75.

Soekanto, S. (1986). *Pengantar penelitian hukum* [Introduction of legal research]. Jakarta, Indonesia: UI-Press.

Sonny, Z. (2012). The state of e-government security in Malaysia: Reassessing the legal and regulatory framework on the threat of information theft. *1st Taibah University International Conference on Computing and Information Technology* (pp. 812-817). Retrieved December 23, 2013, from http://irep.iium.edu.my/id/eprint/27226

Suwana, F. (2018). *Indonesia urgently needs personal data protection law.* Retrieved August 22, 2019, from https://theconversation.com/indonesia-urgently-needs-personal-data-protection-law-91929

Editorial Board. (2019, January 4). Protecting personal data. *The Jakarta Post.* Retrieved August 22, 2019, from https://www.thejakartapost.com/academia/2019/01/04/protecting-personal-data.html

Yaqin, A. (2008). *Legal research and writing methods*. Nagpur, India: Lexis Nexis Butterworth Wadhwa.

Zarza, Á. G. (2015). *Exchange of information and data protection in cross-border criminal proceedings in Europe*. Heidelberg, Germany: Springer.

Zhang, B., Baeck, P., Ziegler, T., Bone, J., & Garvey, K. (2016). *Pushing boundaries.* Retrieved January 22, 2020, from https://jbs.cam.ac.uk/wp-content/uploads/2020/08/2015-uk-alternative-finance-industry-report.pdf