Al-Risalah
Forum Kajian Hukum dan Sosial Kemasyarakatan
Vol. 20 No. 2, December 2020 (pp. 197- 214)

p-ISSN: 1412-436X
e-ISSN: 2540-9522

FINANCIAL TECHNOLOGY AND THE LEGAL PROTECTION OF PERSONAL DATA: The Case of Malaysia and Indonesia

Nurhasanah & Indra Rahmatullah
UIN Syarif Hidayatullah Jakarta, Indonesia
Jl. Ir. H. Juanda No. 95 Ciputat, Tangerang Selatan, Indonesia
email: nurhasanah@uinjkt.ac.id; indra.rahmatullah@uinjkt.ac.id

DOI: 10.30631/al-risalah.v20i2.602
Submitted: September 16, 2020; Revised: November 11, 2020; Accepted: November 18, 2020

Abstract: The presence of digital technology brings significant changes in many aspects of human life, including the economy and financial services. The rapid development of financial technology (fintech) is being responded quickly by many countries including Indonesia and Malaysia. Not only conventional fintech, but Sharia fintech is also developing significantly in both countries. This phenomenon is caused by the efficiency and ease of fintech. However, fintech in Indonesia is not followed by a comprehensive protection of personal data. The absence of special regulation on the protection of personal data in Indonesia causes the data often be misused by certain parties such as being stolen, sold, transferred and eliminated irresponsibly causing harm to fintech users. Meanwhile, Malaysia has built a legal system of personal data protection since 2010 and becomes the first country in the ASEAN region to have a comprehensive personal data protection law system. Therefore, the article aims to overview and compare the personal data protection law in Malaysia especially in fintech. To answer the problem, this study uses a normative-empirical method with a comparative law approach. The result of this article shows that Indonesia should learn from Malaysia by doing benchmarking as an effort to establish a comprehensive regulation for protecting personal data. A comprehensive regulation and law enforcement on the protection of personal data are urgently needed in Indonesia to protect the rights of fintech users.

Keywords: Financial Technology, Personal Data, Malaysia and Indonesia

Abstrak: Kehadiran teknologi digital saat ini telah membawa perubahan signifikan dalam berbagai sendi kehidupan manusia termasuk layanan keuangan dan ekonomi digital. Pesatnya perkembangan fintech secara cepat direspon oleh banyak negara termasuk di Indonesia dan Malaysia. Tidak hanya fintech konvensional yang bertumbuh pesat, fintech syariah juga mengalami peningkatan signifikan pada dua negara tersebut. Fenomena ini disebabkan oleh efisiensi dan kemudahan fintech. Namun demikian, fintech di Indonesia tidak diikuti dengan perlindungan data pribadi yang

komprehensif. Ketiadaan regulasi khusus perlindungan data pribadi di Indonesia menyebabkan data pribadi kerap disalahgunakan oleh pihak-pihak tertentu seperti: dicuri, dijual, dialihkan dan dihilangkan dengan tidak bertanggungjawab. Sedangkan Malaysia telah membangun sistem hukum perlindungan data pribadi sejak tahun 2010 dan menjadi negara pertama di ASEAN yang memiliki sistem hukum perlindungan data pribadi yang komprehensif. Oleh karena itu, artikel ini bertujuan untuk memberikan gambaran dan perbandingan hukum perlindungan data pribadi dalam fintech di Malaysia. Metode yang digunakan dalam penelitian ini adalah normatif-empiris dengan pendekatan perbandingan hukum (comparative legal system). Kesimpulan dari artikel ini menunjukkan bahwa Indonesia melakukan benchmarking dari Malaysia dengan melakukan perbandingan sebagai salah upaya dalam membentuk regulasi khusus perlindungan data pribadi. Regulasi khusus perlindungan data pribadi sangat dibutuhkan di Indonesia untuk mengatur secara komprehensif perlindungan hak-hak pengguna fintech.

Kata Kunci: Teknologi Keuangan, Data Pribadi, Malaysia dan Indonesia

Introduction

The ease of transaction offered by fintech grows rapidly in many parts of the world, including in Indonesia. Data from the Indonesian Fintech Association (Aftech), there are 135 fintech companies dealing with five sectors currently, namely payment lending, capital markets, insurance, market provisioning, and peer-to-peer lending.[1] Based on the data mentioned, peer to peer lending is the most common types with 52 companies.[2] Currently, there are around 13 Islamic fintech providers from 161 fintech companies that registered and licensed.[3]

As a country with a majority Muslim population, Indonesia is currently developing the Islamic fintech. This is because conventional fintech implements the interest system that is prohibited as usury. The presence of islamic fintech free from usury transactions is therefore a necessity for Muslims in Indonesia. At the time of writing, 41 islamic fintech companies are now members of the Indonesian Sharia Fintech Association (AFSI).[4] In terms of organizing Islamic fintech, Indonesia is ranked third in the world after Malaysia and Great Britain.[5] To ensure the legality of islamic fintech, the Indonesian Ulama Council (MUI) issued a *fatwa* (*Islamic rulling*) on Financing Services Based on Sharia Information Technology (*Fatwa No. 117 / DSN-MUI / IX / 2018*). It regulates that islamic fintech must be clear from usury, fraud, gambling, misleading information, hazard and illicit transaction.

Behind the convenience of the fintech services, there is a legal risk such as breach of personal data of the fintech users. It occurs both in conventional and Islamic fintech in Indonesia. There are several modes of misuse of personal data in fintech services in Indonesia. The Jakarta Legal Aid (LBH Jakarta) recorded the modes of personal data misuse such as the

1 Ridwan Aji Pitoko, "Tumbuh Pesat, 135 Perusahaan Fintech Kini Ada Di Indonesia," n.d., https://ekonomi.kompas.com/read/2018/04/13/214800426/tumbuh-pesat-135-perusahaan-fintech-kini-ada-di-indonesia.

2 Ibid.

3 List of licensed and registered fintech companies per February 19, 2020 from the Financial Services Authority (OJK).

4 Safri Haliding, "Mendorong Indonesia Jadi Pusat Islamic Fintech Dunia," September 15, 2019, http://ekonomi.metrotvnews.com/analisa-ekonomi/VNnR0AXN-mendorong-indonesia-jadi-pusat-islamic-fintech-dunia.

5 Tim Cooper, "The Race to Become the World's Leading Islamic Fintech Hub," September 15, 2018, https://www.raconteur.net/finance/race-become-worlds-leading-leading-islamic-fintech-hub.

retrieval of personal data (suctioning) in the form of contact numbers, texting, calls, sim cards, etc on consumers cellular phones so that if consumers are late in paying their debts or defaulting the payment, fintech companies will contact people in the debtor's contact numbers to inform them about the late payment or default, and then to ask them to remind or caution the debtor.[6]

Until September 2019, the Jakarta Legal Aid (LBH) Indonesia has received around 4500 complaints from the victims of online loans from the registered and unregistered fintech platforms both conventional and islamic online loans. The most reported type of fintech was Peer to Peer lending but there were also several other types such as crowdfunding. 4,500 complaints came from 79 applications. From 79 fintech applications, 29 of them were registered applications and the rest have not been registered. This means that fintech violations are not only committed by those which have not yet registered, but also those which have registered at Financial Service Authority (OJK).[7]

LBH Jakarta found several types of violations committed by fintech companies:

1. Retrieval of personal data in the form of contact numbers, SMS, calls, memory cards in the consumers phone. This condition will occur if the consumer is late in paying the debt or if he defaults the debt, then the fintech provider would use all the numbers of the consumer contact directly through the system.
2. The bill is conducted by contacting all the names on the contact who know the consumers. The provider will contact all relatives, parents, close friends and others who know the consumer whether they know or dont know exactly what the consumer doing.
3. The bill is done by humiliating, cursing, threatening, slandering, and sometimes sexual harassment.
4. The bill is done before the due date and anytime.
5. The loan interest is very high and unlimited.
6. Contact numbers for customer complaint numbers are not always available.
7. The fintech company address is not clear.
8. Fintech application change names without adequate notice to consumers while interests on loans during the name changing process continue.[8]

The mode of fintech personal data violation in Indonesia occurs because of public ignorance. For example, the personal data will move to other people without consent while downloading. It happens when fintech application requests personal photos, access to all telephone numbers, location, and files stored on mobile phones from the people who download the application. Ironically, the violation of personal data is not only done by the private sector but also by the government in providing services to the public.[9]

Based on data from the Directorate of Criminal Investigation of Police, from January to 17 April 2020, there were 4,008 (1,322 through the Regional Police and 2,686 through the cyber portal reports related to cybercrime with estimated total loss of IDR 10.74 billion. The reports consist of 2,157 online frauds from fintech platforms and the rest are reports of threats, extortion, data/identity theft, electronic system hacking, illegal interception, system interruption, data manipulation, and related illegal content/access. Compared to January until April last year, this phenomenon has

6 Jeany Sirait, Public Lawyer at Jakarta Legal Aid (LBH Jakarta), October 8, 2019.

7 Ibid.

8 LBH Jakarta, "Korban Pinjaman Online," n.d., https://www.bantuanhukum.or.id/web/banyak-masalah-lbh-jakarta-buka-posko-pengaduan-korban-pinjaman-online/.

9 David Tobing, "Berpotensikah Anda Menjadi Korban? Bersama Satgas Waspada Investasi: Jauhi Jerat Utang Fintech Illegal" (Seminar, Indosterling Forum, Jakarta, October 16, 2019).

raised significantly from a total of 2,029 reports (1,862 through the Regional Police and 167 through the portal cyber) with an estimated total loss of 134.03 million IDR.[10] One of the root causes of this is because there is no comprehensive law protecting personal data in Indonesia. Indonesia has actually had some personal data regulation in some sectors found in scattered laws. The laws are not only sectoral in nature, but they often overlap or contradict against each other.

Besides Indonesia, violation of personal data also occurs in Malaysia, although not specific violations in fintech services. For example, in 2016, violation of personal data in Malaysia was dominated by the financial sector to be around 19%. Other fields are services 20%, education 12%, direct marketing 10%, insurance 7% and the rest are other sectors.[11] There was also a violation of personal data with the leaking of 46.7 million cell phone user data at the end of 2017.[12]

The same story was repeated in 2019, where customer data from Malindo Air was leaked to the public. From the result of the investigation conducted by an independent team, there were around 7.8 million passengers related to cases of failure of personal data protection consisting of several nationalities including 66 percent from Malaysia, 4 percent from India and 2 percent from Indonesia.[13]

Personal data violations occur in many sectors, such as the case of telco user data sabotage in November 2019[14], 17000 patient data were exposed to the national neurology registry website in October 2019.[15] Even the case of data violations reached students at the University of Malaya[16] and Universiti Malaysia Sabah at the end of 2019.[17]

Malaysia and Indonesia face cases of personal data violation. However, the situation in Malaysia is better and more controlled as Malaysia already has a comprehensive legal instrument that regulates the protection of personal data in the form of the Personal Data Protection Act 2010 (PDPA). PDPA is the legal basis for the regulation and law enforcement of personal data violation in Malaysia. While Indonesia still does not have a specific and comprehensive law because personal data protection regulations are still scattered in many laws and regulations. Ironically, the laws and regulations overlap substantially with each other causing legal uncertainty.

Several previous studies have analyzed and discussed related to the problem mentioned above. First, Nurhasanah and Indra

10 Ira Aprilianti, "Personal Data Protection in Pandemi COVID-19," n.d., https://referensi.elsam.or.id/wp-content/uploads/2020/04/Hari-Konsumen-Nasional-Perlindungan-Data-Pribadi-di-Tengah-Pandemi-COVID-19.pdf.

11 Abu Bakar Munir, "Personal Data Protection Act in Research," *Malaysia and Beyond, K&K Advocates - Expert Panel Discussion on Data Protection*, March 28, 2018, 38.

12 "Puluhan Data Pengguna Ponsoel Bocor Di Malaysia," n.d., https://www.cnnindonesia.com/internasional/20171102100434-106-252917/puluhan-juta-data-pengguna-ponsel-bocor-di-malaysia.

13 "Kasus Bocor Data Malindo 2 Persen Milik WNI," n.d., https://bisnis.tempo.co/read/1253036/kominfo-kasus-bocor-data-malindo-air-2-persen-milik-wni/full&view=ok.

14 "Deputy Minister Probe to Determine," n.d., https://www.malaymail.com/news/malaysia/2019/11/26/deputy-minister-probe-to-determine-if-2018s-telco-data-leak-due-to-sabotage/1813616.

15 "Patients Personal Data Exposed on National Neurology Registry Website," n.d., https://www. - thestar.com. my/news/nation/2019/10/23/over-17000-patients039-personal-data-exposed-on-national-neurology-registry-website.

16 "University Malaya PDPD Looking Into Report of Massive Data Breach Affecting the University," n.d., https://www.thestar.com.my/news/nation/2019/10/19/university-malaya-pdpd-looking-into-report-of-massive-data-breach-affecting-the-university.

17 "Hacker Claims to Have Stolen Personal Data of Universiti Malaysia Sabah Students," n.d., https://www.thestar.com.my/tech/tech-news/2019/11/05/hacker-claims-to-have-stolen-personal-data-of-universiti-malaysia-sabah-students.

Rahmatullah with the title "The Legal Protection of Sharia Financial Technology in Indonesia (Analysis of Regulation, Structure and Law Enforcement)." This article discussed the importance of legal protection both in terms of legal material, legal structure and legal culture. In conclusion, legal protection on islamic fintech in Indonesia is inadequate because the state does not provide the legal protection and also because islamic fintech has not been clearly regulated in state law. Furthermore, there is an absence of clear regulation on the position of the sharia supervisory board to supervise sharia product in fintech and there is no protection of personal data. The focus of this article emphasizes the uncertainty of Islamic fintech law in Indonesia. However, this article does not analyze deeply on the importance of personal data protection law in fintech.[18]

Second, Muhammad Saiful Rizal, with the title "Comparison of Protection of Personal Data between Indonesia and Malaysia." The article discussed the comparison of personal data protection regulation in Indonesia and Malaysia. Although discussing personal data protection, this article does not specifically analyze which sectors or industries to be protected by personal data law. He only discussed the protection of personal data generally.[19]

Third, Farah Mohd Shahwahid and Surianom Miskam, with the title "Personal Data Protection Act 2010: Taking the First Steps Towards Compliance." This article only discussed the background of the presence of PDPA in 2010, its urgency and the concept of protecting personal data generally. According to them, there are 7 important principles in the PDPA in 2010, namely: General Principles, Notice and Choice Principle, Disclosure Principle, Security Principle, Retention Principle, Data Integrity Principle, and Access Principle.[20]

Fourth, Santhi Kandiah, with the tittle "The Privacy, Data Protection and Cybersecurity." This book is a collection of articles from some experts who reviewed the law of personal data in the world. Santhi Kandiah reviewed the protection of personal data in Malaysia. She revealed the background of regulation in Malaysia, general concept and law enforcement.[21]

Based on literature review, this article has novelty issue and significant analysis that differs from the existing discussions. This article tries to overview the legal system of personal data in Malaysia such as regulation, structure and law enforcement comparing with situation in Indonesia where it still does not have specific and comprehensive law because personal data protection regulations are still scattered throughout many laws, causing overlaps and legal uncertainties.

The Phenomenon of Financial Technology (Fintech)

Globalization has changed the established legal order in every country. Even as the result of globalization, law in certain countries lag behind others. Ohmae believes that technology is a factor that drives and determines the direction of social change, including changes that occur in the field of law. In other words, when technology develops in the society, it becomes as a determinant factor for the change in community. While social change-including changes in the field of law-is a reaction from change and development of technology. It

[18] Nur Hasanah and Indra Rahmatullah, "The Legal Protection of Sharia Financial Technology In Indonesia (Analysis of Regulation, Structure and Law Enforcement)," *International Journal of Advanced Science and Technology* 29, no. 3 (2020): 3086–97.

[19] Muhammad Saiful Rizal, "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia," *Jurnal Cakrawala Hukum* 10, No. 2 (December 9, 2019).

[20] Farah Mohd Shahwahid and Surianom Miskam, "Personal Data Protection Act 2010: Taking The First Steps Towards Comliance," *E-Proceedings of the Conference on Management and Muamalah*, May 26-27, 2014.

[21] Shanti Kandiyah, Alan Charles Raul Ed., *The Privacy, Data Protection and Cybersecurity Law Review* (London: Law Business Research Ltd, 2019), p. 251.

means, the changes that occur in the field of law always follow the development of technology.[22]

The law and information technology are a phenomenon that cannot be avoided in the era of the third wave of society.[23] The third civilization phase clearly has begun. The civilization is marked by advance in communication and information technology (data processing). The impact of the civilization is that the flow of information in modern human life can no longer be limited. Marshall MacLuhan called it the Global Village.[24] the Latin phrase says "tempora mutantur, nos et mutamur in Illis (the times changed and we also changed with it)" feels very relevant in the era of global information technology.[25]

The law and technology are revealed by the Organization for Economic and Cooperative Development (OECD) which believes that information technology has huge implication on economic, social, economic and the law.[26] Related to various implications of information technology, the law must be responsive to non-legal factors. For example, technological development. The law and technology cause the shift of traditional legal paradigm to the new era.

Edmon Makarim explains that the shift in the paradigm of traditional law, including which has not been accommodated by traditional law, happened in 3 ways:1. The shift from written characters to unwritten; 2. the shift from document to non-document, and 3. the shift from conventional characters to electronic-based.[27]

However, technological development causes a crime loophole known as cybercrime (Cybercrime). Cybercrime is a crime that arises as a result of the existence of cyberspace community on the internet and has its own characteristics that is different from conventional crime. The targets of cybercrime are:[28]

1. Cybercrime affects/brings harm to person. The target of the attack is directed to person who has certain characteristics or criteria according to the purpose of the attack. Some examples of these crimes include:
   a. Pornography, the activity is conducted by making, installing, and distributing material of pornography, obscene, and exposing inappropriate things.
   b. Cyberstalking, the activity is to disrupt or harass someone by using a computer, for example by using e-mail that is done repeatedly like terror in the cyber space. It can be sexual, religious, etc.
   c. Cyber-Trespass, the activity is to violate other people privacy area such as Web

---

22 M. Arsyad Sanusi, *Konvergensi hukum dan teknologi informasi: sebuah torehan empiris-yuridis* (Jakarta: Indonesian Rearch, 2007), p.58.

23 Alftin Toffler divided the social changes in three phases:as follows, The first social changes phase due to agrarian revolution (8000 SM – 1700 SM). The second phase is industrial revolution with the invention of the steam engine and called etra industrialization (1700 M- 1970 M). The third phase is information and communication era (1970 M- 2000 M). The third phase is the society with the presence of information technology changed very significant in 3 dimensions, as follows: human behavior, human interaction, and human relations. In later development, the change of interaction and human inter-relation practiced in the relation of business and commerce. Business is not always doing by face to face but it can use technology. Cited in Syahrial Syarbaini, *Sosiologi dan politik* (Jakarta: Ghalia Indonesia, 2002), p. 41.

24 Marshal Macluhan in Dimitri Mahanaya, *Menjemput Masa Depan: Futuristik dan Rekayasa Masyarakat Menuju Era Global* (Bandung: Remaja Rosda Karya, 1999), p. 49.

25 Barita Saragih, "Tantangan Hukum Atas Aktivitas Internet," Kompas, July 9, 2000. p. 8.

26 OECD, The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda (OECD, 1999), https://doi.org/10.1787/9789264172081-en.

27 Sanusi, *Konvergensi Hukum dan Teknologi Informasi*, p. 113.

28 Ari Dermawan, "Pengaruh Kemudahan Teknologi Informasi Terhadap Pelanggaran Atau Kejahatan Hukum" *Jurnal Manajemen Informatika dan Teknik Komputer* 2 (2017): 17.

Hacking. Breaking to PC, Probing, Port Scanning and others.

2. Cybercrime brings harm to property rights, Cybercrime is conducted to interfere with or attack the property of others. Some examples of this crime include accessing computer through the cyberspace illegally, possessing electronic information/information theft illegally, carding, cybersquatting, hijacking, data forgery and all activities that are detrimental to other properties.
3. Cybercrime bring harms to the government, it is conducted with the specific purpose of attacking the government. For example, cyber terrorism as an act that threatens the government including cracking into official government sites or military sites.

The struggle between law and technology has also penetrated the financial services in the world. In 2014, the term Financial Technology (Fintech) began to be widely used as a reference for the entry of technology tools, platform and ecosystem that made financial service or product more accessible, efficient, and affordable. Although the use of the term Fintech is relatively new, in the financial industry such as bank has been using technology such as Automatic Teller Machines (ATMs) since 1967. ATM also includes financial services based on information technology (digitization) as in today's Fintech phenomenon where all services use the internet network.

Financial technology is an innovation from financial services that most or even all of its activities rely on the advancement of information technology, especially the internet of things where innovation has an impact in connecting financial technology (fintech service providers) with corporate or business consumers (business to business) and individual consumers (business to customer).[29] The National Digital Research Center (NDRC) in Dublin, Ireland, defines fintech as innovation in financial services based on modern information technology.[30]

Catradiningrat defines fintech as an entity that combines technology with financial service features so that it becomes a creative disruption in the financial market because it changes the prevailing order.[31] McKinsey defines fintech or digital finance as financial services delivered through digital infrastructure from cash and conventional bank. Cell phones, computers, or cards used through point of sale (POS) devices connecting individual and business to the digital national payment infrastructure to enable unlimited transaction between all parties.[32] Oxford Dictionary defines fintech as computer program and other technologies used to support or enable banking and financial services (computer program and other technologies used to support or activate banking and financial services).

From some of the definitions, it can be understood that financial technology is a digitalisation-based financial service (information technology) that enables it to be used by economic subjects such as: individual, business entities, banks, and other financial institutions. Fintech today refers to not just one, but a number of technologies that broadly impact the financial payment, funding, loan, investment, financial service, and currency.

Indonesia and Malaysia are equally concerned in the development of the Islamic eco-

[29] Ernama Santi and Hendro Saptono, "Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016)," *Dipenegoro Law Journal,* 6, no. 3 (2017): 1–2.

[30] Titik Wijayanti, "Pelaksanaan Pemberian Kredit Berbasis Tehnologi Informasi oleh Fintech kepada Pelaku UKM," *Fakultas Hukum, University Muhammadiyah Surakarta*, 2018, 1.

[31] Catradiningrat RM and M Yusuf, "Towards Financial Inclusiveness Through Financial Technology" (Research and Development of Academics HMPSEP 2016/2017.).

[32] Mckinsey Indonesia Office. "Unlocking Indonesia's Digital Opportunity" (McKinsey & Company, 2016).

nomic system. Based on statistical data from the State of the Global Islamic Economy 2018/2019. There are 10 countries that have the largest Islamic economic market assets in the world; 1. Iran (US $ 578M), 2. Saudi Arabia (US% 509), 3. Malaysia (US $ 491M), 4. UAE (US $ 222M), 5. Qatar (US $ 129M), 6. Kuwait (US $ 109M), 7. Bahrain (US $ 84M), 8. Indonesia (US $ 82M), 9. Turkey (US $ 54M) and 10. Bangladesh (US $ 34M). Malaysia and Indonesia are the two countries in the ASEAN region that are included in the 10 countries with the largest Islamic economic market assets in the world. Malaysia is ranked third, while Indonesia is ranked eight. This means that Malaysia is 5 levels above Indonesia in terms of Islamic economic market assets.[33]

Even though Malaysia's total market asset is still above Indonesia, in the field of fintech, Indonesia and Malaysia have significant differences. The majority of fintech services in Indonesia are dominated by the Peer to Peer (P2P) or a loan 31%, payment 38% and others.[34] While in Malaysia the majority of fintech services are dominated by payments 36%, Cryptocurrency 12%, Crowdfunding 6%. Interestingly in Malaysia, there is no peer to peer (P2P) category that uses fintech.[35] Suprisingly, in Indonesia peer to peer (P2P) occupies a very large portion. The following is a table of comparison:

Malaysia		Indonesia	
Payments	19%	Payment	38%
Wallets	17%	Lending	31%
Cryptocurrency	12%	Personal finance & wealth management	8%
Crowdfunding	6%	Comparison	7%
Wealth/investment	4%	Insurtech	6%
Blockchain	4%	Crowdfunding	4%
Lending	6%	Pos System	3%
Insurtech	6%	Cryptocurrency and blockchain	2%
Comparison	7%	Accounting	1%
Remittance	6%		
KYC/Regtech	6%		
Currency Exchange	2%		
Marketplace	2%		
Islamic Fintech	2%		
AI	2%		

In addition, the trend of fintech in Indonesia is still dominated by start-up companies, while Malaysian Islamic fintech is dominated by banks. It can be seen that Indonesia has 31 fintech Islamic fintech start-up companies. This is the world's highest number in one country followed by the United States (12 companies), UAE (11 Companies), United Kingdom (10 companies), Malaysia (7 companies) and others (ranked 22).[36]

The Urgency of Personal Data Protection

Oftentimes, we conduct transactional activities such as buying product online, registering email, paying tax, playing games and transaction using fintech (including Islamic fintech) every day and all of them require our data. The data contains personal information that will be received by the private sector and the government. Therefore, the data must be protected by law in order not to be misused.

There are at least several reasons why personal data is important and need to be protected. Firstly, personal data is part of the privacy right that is recognized as one of the instruments in the Universal Declaration of Human Rights (UDHR). Article 12 states that: No one shall be subjected to arbitrary interference

[33] "An Inclusive Ethical Economy State of the Global Islamic Economy Report 2018/19" (Dubai The Capital of Islamic Economy, Thomson Reuters and Dinar Standard, n.d.).

[34] "Fintech News Singapore," Percentage Distribution of Indonesian Fintech Ecosystem 2018, n.d., http://fintechnews.sg/20712/indonesia/fintech-indonesia-report-2018/.

[35] Vincent Fong, "Breakdown of Fintech Players in Malaysia," July 29, 2019, https://fintechnews.my/17922/editors-pick/fintech-malaysia-report-2018/.

[36] "An Inclusive Ethical Economy State of the Global Islamic Economy Report 2018/19."

with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

The UDHR is revealed in the International Convention on Civil and Political Rights (ICCPR) Article 17. In General Comment Number 16 to Article 17 of the ICCPR, it is stated that:

> The gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. ... [E]very individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files ... have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.

Secondly, protecting personal data is part of a commitment to protect consumers. Personal data is very closely related to consumer protection law. Data is one of the consumer rights that must be protected by law. In the consumer protection law, consumers are given rights that must be guaranteed by the state. One of them is the right to secure from the product and service. Therefore, consumer personal data may not be used, modified, and distributed without the consent from consumer.

Thirdly, business reputation. Data is one of the valuable assets for the company. The importance of data is potentially to be stolen and traded by certain individual for any purposes. Data leaks for companies cause financial losses, distrust and bad reputation from the public.

In the development of technology, personal data must be protected by the law. It can be seen that many countries respond with several international law, as follows: The Council of Europe Convention for the Protection of Individual regard to Automatic Processing of Personal Data (No. 108) on 1981. The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) as amended in 2013, The Guidelines for the regulation of computerized personal data files, (General Assembly resolution 45/95 and E/CN.4/1990/72) dan Other regional frameworks also exist including the APEC Privacy Framework-Asia Pacific Economic Cooperation.

Currently, the latest comprehensive regulation is in the EU General Data Protection Regulation (GDPR). It was adopted on 14 April 2016, and became enforceable since 25th May 2018. The GDPR is a comprehensive regulation because it covers almost all personal data aspects.[37] According to GDPR, personal data is:

> Personal data means any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, such as a name, an identification number, location data, physical, economic, physiological, genetic, mental, cultural or social identity of that natural person.

The importance of protection in personal data, all regulations managed by the government and the private sector related to personal data must adopt international regulations on the protection of personal data. All sectors must adopt international law on personal data such as communication services, IT, law enforcement, trade, education, e-government, health services, financial and banking institution, consumer service, cyber security and product responsibility. Therefore, in financial and banking services including islamic fintech

[37] Alan Charles Raul, *The Privacy, Data Protection and Cybersecurity Law Review*, 2019, p. 17.

the protection of personal data is a must because the development of fintech is vulnerable to any legal risks such as transaction security, and data breach in the financial system.[38]

The regulation of personal data protection is very important because we are in the era of the industrial revolution 4.0 which brings about the fintech.[39] The main problem in this digital age is the misuse of personal data such as geolocation data, phone books and data recycling.[40] At least 4 parties will always look for our data: a. Big brothers; government authority b. Big data aggregator; someone who hunts data for commercial purposes, c. Big Fans; fans and haters and d. Malice: someone aims to do something for a specific subject.[41]

Therefore, the need of personal data regulation in fintech becomes something very urgent so that personal data can be stored and used legally according to the law in accordance with the principles of data protection, as follows:[42]

1. The purposes the data and information should be specified at the time of collection, and should only be used for those agreed purposes. Personal data can only be used, retained or disclosed for the legal purposes except with the consent of the individual or under law: accordingly, it must be deleted when no longer needed.
2. Personal data, as generated and processed, should be relevant, limited, and adequate to necessity of the purposes of original purposes.
3. The data should be measured, complete, accurate and up to date whenever to be used.
4. The personal data must be secured and safe from disclosure, modification, use, loss, unauthorized access, and destruction.
5. There are no secret processors of data, processing, or sources. The data owner must be aware of the collection and processing of their data, as well as the purpose of its use, who is controlling it, and who is processing it
6. Individuals have rights to control their personal data and any processing
7. The use of personal data must be responsible and demonstrate compliance with the mentioned principles, and facilitate and fulfil the exercise of these rights, abiding by applicable laws that are enshrined in those principles

Personal Data Protection in Malaysia and Indonesia

1. Malaysia

For Malaysia, the data is a valuable commodity and therefore it is important to be protected. Malaysia has a Personal Data Protection Act (Act 709 Personal Data Protection Act 2010 (PDPA) which is effective since 2013. This is the first personal data protection law in ASEAN at that time. The PDPA draft began in 2001 and the process at that time was influenced by the Hong Kong Personal Data (privacy) 1995 and the Data Protection Act 1998 United Kingdom.

PDPA is a comprehensive guideline for all sectors using electronic transaction to provide security protection for consumers from credit card fraud, identity or data and the sale or spread of personal data without the consent of

---

38 Sonny Zulhuda, "Financial Technology, Regulated System and Its Benefit for The Maslahat Ummah," National Seminar Universitas Al-Azhar Indonesia, October 8, 2019.

39 The latest development is Internet of Things. Sidi Mohamed Sidi Ahmed and Sonny Zulhuda, "Data Protection Challenges in The Internet of Things Era: an Assesment of Protection Offered by PDPA 2010," *International Journal of Law, Government and Communication* 4, no. 17 (2019): 3.

40 Sonny Zulhuda, IIUM Research, September 1, 2019.

41 Sonny Zulhuda, "Perlindungan Data Dalam Konteks Hukum Siber Di Era Disrupsi" (Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, October 7, 2019).

42 Raul, *The Privacy, Data Protection and Cybersecurity Law Review*, p. 15.

consumers. The presence of PDPA is to response the spread of personal data regulations in various fields.[43] The scope of PDPA is very broad so that it includes many fields including: banking and finance, insurance, telecommunications, health, hospitals and tourism, education, real estate and property, direct sales, services (law, accounting, business consultants, engineering, architecture, employment) agents, transportation and retail.

The definion of data according to PDPA is any information in respect of commercial transactions:

1. It is being processed wholly or partly for equipment operating automatically in response to instructions given for that purpose;
2. It is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
3. It is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Sonny Zulhuda explains more specifically about personal data as follows:[44]

In respect of commercial Transaction;	Any transaction of a commercial purposes based on contract or non-contract (includes goods, services, agency, employment, etc)
Relating directly or indirectly To a data subject	The person who is the subject of the personal data (regardless nationality/residence)
Where the data subject is Identified or identifiable	Single information or from other information in data user's possession
Including any sensitive personal Data	Physical/mental health /condition, political preferences, religious beliefs, social life.
Including expression of opinion	E.g. Data user's opinion related to his former employee
Processed by automated means OR is recorded as part of relevant Filing system	It applies to both paper-based document and electronically processed data

Personal Data must at least consist of 3 criterias: a. The data must be related to commercial transaction, b. Information must be processed or recorded electronically as part of the filling system and c. data information must be directly or indirectly related to a personal data identified from information or others in the possession of data users. In addition, there are also sensitive personal data consisting of physical data or mental health of a person, political view, religion or belief, alleged violation of the law.[45]

There are 7 principles in PDPA which the contents have been adapted to several international law for the protection of personal data. The seven principles are:[46]

43 Ibid., p.237.

44 Sonny Zulhuda, "Data Protection in Malaysia," Desember 2019, https://sonnyzulhuda.files.wordpress.com/2019/12/pdp-law-for-it-law-class--131219.pdf.

45 Raul, *The Privacy, Data Protection and Cybersecurity Law Review*, p. 240

46 Several experts had discussed personal data protection principles, among them are: Khaw Lake Tee "Towards a personal data protection regime in Malaysia" (2002) JMCL 11, Abu Bakar Munir "Data Protection Law: Too little, too late?" (Public Lecture, Universiti Malaya, 4 August 2009), Ida Madieha Azmi "E-Commerce and privacy issues: An analysis of the Personal Data Protection Bill" (17th BILETA Annual Conference, Free University, Amsterdam, 5–6 April 2002) and Graham Greenleaf "Limitations of Malaysia's data protection Bill" (2010) 104 Privacy Laws and Business International Newsletter 1. Zuryati Mohamed Yussof, "The Malaysian Personal Data Protection Act 2010: A Legislative Note," *New Zealand Journal Public and Intenational Law* 1, no. 1 (2011): 125-126. N. A. Mohamed Yusofa, N. A. Ahmad and Z. Mohamed, "A Study on Collection of Personal Data by Banking Industry in Malaysia," *Journal of Advanced Research in Business and Management Studies* 2, no. 1 (2016): 42-45.

1. General Principle
   Data user must not process personal data about an individual unless the data owner grants the permission. Without the permission of the data owner, the personal data must not be disclosed.
2. Notice and Choice Principle
   A data user is obliged to give a written notice informing to data owner that his/her personal data is being processed.
3. Disclosure Principle
   Without the permission of the data owner, personal data must not be disclosed for any purpose other than the purpose which was initially disclosed at the time of collection or to any party other than third parties for whom the data owner has given permission.
4. Security Principle
   Data users must take technical steps to ensure the integrity, reliability and security of the personal data. It is the obligation of the data user to take all the necessary efforts to protect any loss, accidental access or disclosure, modification, misuse, unauthorized, alteration and destruction of personal data.
5. Retention Principle
   The personal data processed cannot be kept longer than is necessary and the data user must take all reasonable steps to delete personal data whenever is no longer required except the life span of personal data.
6. Data Integrity Principle
   A data user must ensure that personal data is complete, not misleading, accurate, up to date, and related to the purpose for which it was collected. It is the obligation of data user to guarantee completeness, the accuracy and correctness of the data collected.
7. Access Principle
   A data owner must be given access to, and be able to amend, correct, or destroy personal data whenever it is invalid. However, access or correction must be regulated under the Act. Thus, in any processing and handling of personal data it is mandatory for the data user to observe all data protection principles and any contravention of the principles results in an offence committed by the data use.

In general, the PDPA regulates the following: a. The processing of PII in commercial transaction. It is related to the rule of the process of storing, using and closing data. The process of storing data is intended in what way public data is stored securely, not leaked to other parties and guarantee its confidentiality. The process of using data is to ensure that public personal data is not misused and not used other than the previous purpose. While the closure of data is related to when all transaction activities have been completed, then the personal data of the community must be removed,[47] b. New rules of obligations for data users, c. New offences relating to data abuses etc. d. Rights for data owner, e. Information governance and data due diligence, and f. Promotes selfregulatory Codes of Practices.[48]

PDPA prescribes several types of breach of personal data including: a. breaching data protection principles, b. failure to register as Data user (when applicable), c. Unlawful collection of personal data, d. Unlawful sale of personal data and e. Breach of data security system. The breach of personal data in certain sectors, will be subject to legal sanctions, ie:[49]

No	Sector	Offence (s)	Sanction
1	Tourisme (Hotelier)	Processing personal data without the permission of Commissioner's Certificate Processing	MYR10,000 fine or 8 months imprisonment for each of the offence
2	Education (Private university)	Processing without Certificate	MYR 10.000 or 3 months imprisonment
3	Service sector (em-	Processing without Certif-	MYR 10.000 fine

47 Zulhuda, IIUM Research.
48 Zulhuda, "Data Protection in Malaysia."
49 Zulhuda.

	ployment agency)	icate	
4	Education (Private university)	Processing without Certif-icate	Com-pound RM 10.000
5	Service (job agency)	Processing without Certif-icate	MYR 10.000 fine

The table shows some cases that had been litigated and prosecuted in Malaysian courts between 2017-2018. Therefore, the use of personal data must fulfill the following: a. Personal data obtained legally and not against the law, b. Data collected is accurate, correct and complete, c. The data owner is notified the use of data and what his rights, d. The data owner is given the choice in doing his rights, e. Personal data is not accessed/shared with third parties without permission, f. Personal data is secured by data users, g. Personal data that is no longer used may not be stored and h. The data owner has the right to access and correct the data.[50]

Beside the legislation, the Malaysian government also provides the blue print to ensure the public and country's safety with issued national blueprint on security concern in information management. Ministry of Science, Technology and Innovation (MOSTI) endorsed National Cyber Security Policy (NCSP) as a blueprint in handling cyber security in Malaysia. This institution is designed to facilitate Malaysia's move towards a knowledge-based economy (K-economy) and addressed the risks to the Critical National Information Infrastructure (CNII) in which comprises the networked information systems of ten critical sectors: National Defence and Security, Banking and Finance, Information and Communications, Energy, Transportation, Water, Health Services, Government, Emergency services, Food and Agriculture. This national level security policy governs all moves taken by the government in their facility to ensure the government data and information are safe in this connected world.[51]

2. *Indonesia*

During Covid-19, data from Analytics Data Advertising (ADA) shows a trend in online shopping transaction up to 300%. ADA also notes in the use of productivity application which is more than 400%. Changes in consumer behavior also occurs in the consumption of financial products. One example is the volume of transaction in DANA digital wallet is increasing up to 15% since the introduction of social distancing policy. In addition, OJK data also shows a trend in the accumulation of online lending up to 17.05% in February 2020 compared to December 2019.[52]

However, regulation of fintech in Indonesia generally still leaves very crucial problem on the protection of personal data for consumers or users both in conventional and islamic fintech as a result of technological development. Cyberspace now becomes a virtual battleground due to the development of technology that is prone to be misused by any interest groups, individual, business entities, or the state. The deviation from technological development is the issue of cybersecurity.

IT Governance noted that in the first quarter of 2019 there had been at least 1,769,185,063 cases of personal data leakage and cyberattacks worldwide with an average loss of at least US $ 3.86 million for each lost or stolen data contained sensitive and confidential information according to the IBM study in 2018. While in Indonesia, according to the Siber and Sandi Negara (BSSN) from January to June 2018, there were at least 143.4 million cyberat-

[50] Zulhuda, "Perlindungan Data Dalam Konteks Hukum Siber Di Era Disrupsi."

[51] Mohd Amiruddin Hamzah, Abdul Rahman Ahmad, Norhayati Hussin, Zaharuddin Ibrahim, "Personal Data Privacy Protection: A Review on Malaysia's Cyber Security Policies," *International Journal of Academic Research in Business and Social Science* 8, no. 12 (2018): 1480.

[52] Aprilianti, "Personal Data Protection in Pandemi COVID-19."

tacks where 1,355 cases were the reports from the public.[53]

Ironically, Indonesia does not have a special and comprehensive law on the protection of personal data, allowing many violations of the law to occur. The legal draft on Personal Data Protection has been discussed in the House of Representatives of the Republic of Indonesia (DPR RI) since 2012. However, the draft has not been finished until now. It causes massive violations of personal data protection in Indonesia because personal data protection regulations are still scattered in various laws and regulations. Indonesia still do not have a special and comprehensive personal data protection law to provide legal protection for the public.

According to study from ELSAM and the Ministry of Communication and Information, there are about 32 laws and regulations of state institutions which in substance overlap on the matters of personal data processing. The overlap among the regulations are related to the purpose of data processing, notification, the purpose to open the data, the duration to open and collect data, destruction of data, to allow permission for open the data, sanction, and recovery.[54]

Regulations that overlap among other are Criminal Law (KUHP), the Criminal Procedure Law (KUHAP), Law Number 39 of 1999 on Human Rights, Law Number 21 of 2007 on Trafficking in Person, Law number 36 of 1999 on Telecommunication, Law Number 11 of 2008 on Information and Transaction Electronic, Law Number 14 of 2008 on Open Public Information, Law Number 5 of 2018 on Anti-Terrorism, Law Number 17 of 2011 on State Intelligence, Law Number 9 of 2013 on Terrorism Funding, Law Number 30 of 2002 on Corruption Crime, Law Number 19 of 2019 on Corruption Eradication Commission, Law Number 18 of 2011 on Judicial Commission, Law Number 18 of 2003 on Advocate, Law Number 23 of 2006 on Population Administration, Law Number 43 of 2009 on Filing Law, Law Number 29 of 2004 on Medical Practice, Law Number 35 of 2009 on Narcotics, Law Number 26 of 2009 on Health, Law Number 44 of 2009 on Hospital, Law Number 36 of 2014 on Manpower Health, Law Number 10 of 1998 on Banking, Law Number 21 of 2008 on Sharia Banking, Law Number 3 of 2004 on Bank Indonesia, Law Number 21 of 2011 on Financial Services Authority, Law Number 8 of 2010 on Money Laundering, Law Number 8 of 1997 on Company Document, Law Number 8 of 1999 on Consumer Protection, Law Number 7 of 2014 on Trade Law, Minister of Communication and Information Regulation No. 20 of 2016 on Personal Data Protection, POJK Number 77 / POJK.01 / 2016 on Information Technology Lending and Borrowing Services.

Therefore, Indonesia must have a comprehensive law on the protection of personal data and covering fields sector for the unification of personal data protection. Indonesia must adapt quickly with the rapid development of technology. Law becomes the dependent variable on technological development in the case of financial technology.

Law Enforcement on Personal Data Protection in Malaysia and Indonesia

1. Malaysia

Malaysia already has a personal data protection law since 2010 to support and facilitate the process of law enforcement on personal data violations directly and indirectly. It confirms that Malaysia is able to capture the phenomenon of legal and technology quickly.

---

53 Wahyudi Djafar, Lintang Setianti, and Alia Yofira Karunian, *Mengembangkan Pendekatan Berbasis HAM Dalam Kebijakan Keamanan Siber* (Jakarta: Elsam, 2019), p. 5.

54 Denico Doly, "Politik Hukum Pengaturan Pelindungan Data Pribadi," Info Singkat Pusat Penelitian Badan Keahlian DPR Vol. X, No. 08/II/Puslit/April/2018. p. 6.

Law enforcement on personal data violation is an important matter because law without enforcement is futile. Law enforcement on personal data violation in Malaysia in all sectors (including fintech) is conducted in two ways: First, Maximizing the Industrial Code of Practice (COP). COP is implemented in all sectors such as the Utility (Electricity), Banking and Financial Institution, Insurance and Transportation sectors. Other sectors that the COP is still drafting includes Utility (Water), Telco, Services (legal), Pawnbroker, Health, Direct Selling and Tourism and Hospitalities. Second, the law enforcement conducted by The Department of Personal Data Protection (JPDP) under the Ministry of Communications and Multi Media (KKMM). The main task of JPDP is to conduct law enforcement of PDPA in Malaysia.

JPDP commissioners are mandated by PDPA to inspect company data protection system. If the company does not meet the requirements set by JPDP, the company may be subject to criminal sanction. The instrument used by JPDP in inspecting companies include: personal data collection form and privacy notice, internal standard operating procedures for personal data management within the organization, person in charge of personal data management within the organization and his or her awareness of the legal requirements and compliance with the seven data protection principles in the PDPA.[55] The commissioner's decision is not final and can be appealed to the appellate court. The appeal court decision is final and binding for the parties.[56]

In the JPDP, there is an important division to monitor the protection of personal data. It has the duty to conduct monitoring and law enforcement as stated in PDPA which includes: evaluation, investigation and monitoring. The role and function of the monitoring division are:

1. To ensure the integrity and accountability of data users to protect personal data which is the most important asset in the company.
2. To ensure the implementation of all of programs and activities in the context of personal protection based on independent audit, analysis and objective assessment.
3. To help the organization improve on the operation of personal data users and convince stakeholders and the public in the use and management of personal data protection.
4. To evaluate the risk of the system and the process of protecting personal data. If there are deficiencies, it can be corrected.
5. To process and hold public disputes settlement related to the use of personal data.

2. *Indonesia*

Because of the absence of a comprehensive personal data protection law in Indonesia the law enforcement is not optimal and there is a lack of coordination between legal enforcer. Therefore, the supervision and law enforcement on personal data protection is still weak. Coordination between institutions is not going well enough because the concept is unclear on what institution becomes the front guard in conducting supervision and law enforcement.

Currently, the law enforcement is still based on the initiative and depends on responsibilities (responsible business conduct) and independent (self-regulatory) business entities. For example, the signing of joint code of ethic by three Indonesian fintech associations (Aftech, AFPI, and AFSI) in September 2019 related to consumer protection, privacy protection and personal data, cyber risk mitigation,

[55] Raul, *The Privacy, Data Protection and Cybersecurity Law Review*, p. 252-253.

[56] Zuryati Mohamed Yusoff, "The Malaysian Personal Data Protection Aact 2010: a Legislation Note," *New Zealand Journal of Public and International Law* 1, no. 9 (2014): 127.

and the minimum mechanism for handling consumer complaints.[57]

However, Indonesia cannot rely on the initiative of business entities because the initiative is not legally binding. This causes business entities to freely choose wether or not they wish conduct the initiative. Indonesia still needs specific, comprehensive, and mandatory regulation related to the protection of personal data so it can provide legal protection and certainty for users of fintech including Islamic fintech. Therefore, based on the weaknesses in Indonesia on protecting personal data, benchmarking towards Malaysia is one of the solutions to imitate and apply a comprehensive legal system of personal data protection.

Conclusion

The existence of personal data in fintech is very important because it is inherent with personal data that tends to be misused. This condition pushed Malaysia to design personal data protection framework and policies. In 2010, Malaysia has issued a Personal Data Protection Act (PDPA). PDPA regulates all the personal data protection from many sectors such banking, insurance, digital payment etc. It consists of principles, provisions, sanctions and law enforcement. It also becomes the material and formal law. Although Malaysia has also been exposed to cases of personal data protection, they have a clear, comprehensive, and coordinative legal instruments that guides all parties such as the State, and business actors. This shows that the state has demonstrated the commitment to provide legal protection and legal certainty for the citizen.

Meanwhile, the situation is different in Indonesia. The regulation of personal data in Indonesia is still scattered in various laws and regulations depending on the sector. Each sector has its own personal data regulation that is different with other personal data sectors. Therefore, it causes legal uncertainty because the substances overlap among other regulations (conflict of norms). It makes the law enforcement to not be effective because there is no coordination between state institutions related to the coordinator or front guard for conducting law enforcement personal data cases. State institutions work individually without coordination and communication in accordance with their authorities. It proves that the country has failed to provide legal protection and legal certainty for its citizens. The Government and The House of Representatives of The Republic of Indonesia must sign the draft of Personal Data Protection that is listed in National Legislation Program (Prolegnas) 2019-2024 of the House of Representatives of The Republic of Indonesia as soon as possible.

[57] Aprilianti, "Personal Data Protection in Pandemi COVID-19."

Bibliography

Journals

Ahmed, Sidi Mohamed Sidi and Sonny Zulhuda. "Data Protection Challenges in The Internet of Things Era: an Assesment of Protection Offered by PDPA 2010." *International Journal of Law, Government and Communication* 4, no. 17 (2019).

Dermawan, Ari. "Pengaruh Kemudahan Teknologi Informasi Terhadap Pelanggaran atau Kejahatan Hukum." *Jurnal Manajemen Informatika dan Teknik Komputer* 2, no. 1 (2017).

Doly, Denico. "Politik Hukum Pengaturan Perlindungan Data Pribadi," Info Singkat Pusat Penelitian Badan Keahlian DPR Vol. X, No. 08/II/Puslit/April/2018.

Hasanah, Nur, and Indra Rahmatullah. "The Legal Protection of Sharia Financial Technology in Indonesia (Analysis of Regulation, Structure and Law Enforcement)." *International Journal of Advanced Science and Technology* 29, no. 3 (2020): 3086–97.

Hamzah, Mohd Amiruddin, Abdul Rahman Ahmad, Norhayati Hussin, Zaharuddin Ibrahim. "Personal Data Privacy Protection: A Review on Malaysia's Cyber Security Policies". *International Journal of Academic Research in Business and Social Science* 8. no. 12 (2018).

Munir, Abu Bakar. "Personal Data Protection Act in Research." *Malaysia and Beyond, K&K Advocates - Expert Panel Discussion on Data Protection*, March 28, 2018.

Rizal, Muhammad Saiful. "Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia." *Jurnal Cakrawala Hukum* 10, no. 2 (2019).

Shahwahid, Farah Mohd, and Surianom Miskam. "Personal Data Protection Act 2010: Taking The First Steps Towards Compliance," *E-proceedings of the Conference on Management and Muamalah (CoMM 2014-),* 26-27 May 2014

Santi, Ernama, and Hendro Saptono. "Pengawasan Ootoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016)." *Dipenegoro Law Journal* 6, no. 3 (2017).

Yusoff, Zuryati Mohamed. "The Malaysian Personal Data Protection Aact 2010: a Legislation Note." *New Zealand Journal of Public and International Law* 1, no. 9 (2014).

Yusofa, Mohamed N. A. Ahmad and Z. Mohamed. "A Study on Collection of Personal Data by Banking Industry in Malaysia." *Journal of Advanced Research in Business and Management Studies* 2, no. 1 (2016).

Zulhuda, Sonny. "Data Protection in Malaysia," *International Islamic University Malaysia (IIUM)* (2019).

Books

Dubai The Capital of Islamic Economy. *An Inclusive Ethical Economy State of the Global Islamic Economy Report 2018/19*. Thomson Reuters and Dinar Standard.

Djafar, Wahyudi, Lintang Setianti, and Alia Yofira Karunian. *Mengembangkan Pendekatan Berbasis HAM Dalam Kebijakan Keamanan Siber*. Jakarta: Elsam, 2019.

Mahanaya, Marshal Macluhan in Dimitri. *Menjemput Masa Depan (Futuristik Dan Rekayasa Masyarakat Menuju Era Global)*. Bandung: Remaja Rosda Karya, 1999.

Mckinsey Indonesia Office. *Unlocking Indonesia's Digital Opportunity*. McKinsey & Company, 2016.

OECD. *The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda*. OECD, 1999.

Raul, Alan Charles. *The Privacy, Data Protection and Cybersecurity Law Review*. London: Law Business Research Ltd, 2019.

RM, Catradiningrat, and M Yusuf. "Towards Financial Inclusiveness Through Financial Technology." Research and Development of Academics HMPSEP 2016/2017.

Sanusi, M. Arsyad. *Konvergensi hukum dan teknologi informasi: sebuah torehan empirisyuridis*. Jakarta: Indonesian Rearch, 2007.

Syarbaini, Syahrial. *Sosiologi dan politik*. Jakarta: Ghalia Indonesia, 2002.

Wijayanti, Titik. "Pelaksanaan Pemberian Kredit Berbasis Tehnologi Informasi oleh Fintech kepada Pelaku UKM." *Fakultas Hukum, University Muhammadiyah Surakarta*, 2018.

Seminars

Tobing, David. "Berpotensikah Anda Menjadi Korban? Bersama Satgas Waspada Investasi: Jauhi Jerat Utang Fintech Illegal." Seminar presented at the Indosterling Forum, Jakarta, October 16, 2019.

Zulhuda, Sonny. "Perlindungan Data Dalam Konteks Hukum Siber Di Era Disrupsi." Fakultas Syariah dan Hukum UIN Syarif Hidayatullah Jakarta, October 7, 2019.

———. "Financial Technology, Regulated System and Its Benefit for The Maslahat Ummah," National Seminar Universitas Al-Azhar Indonesia, October 8, 2019.

Websites

Aprilianti, Ira. "Personal Data Protection in Pandemi COVID-19," n.d. https://referensi.elsam.or.id/wp-content/uploads/2020/04/Hari-Konsumen-Nasional-Perlindungan-Data-Pribadi-di-Tengah-Pandemi-COVID-19.pdf

Cooper, Tim. "The Race to Become the World's Leading Islamic Fintech Hub," September 15, 2018. https://www.raconteur.net/finance/race-become-worlds-leading-leading-islamic-fintech-hub.

"Deputy Minister Probe to Determine," n.d. https://www.malaymail.com/news/malaysia/2019/11/26/deputy-minister-probe-to-determine-if-2018s-telco-data-leak-due-to-sabotage/1813616.

Fong, Vincent. "Breakdown of Fintech Players in Malaysia," July 29, 2019. https://fintechnews.my/17922/editors-pick/fintech-malaysia-report-2018/.

"Hacker Claims to Have Stolen Personal Data of Universiti Malaysia Sabah Students," n.d. https://www.thestar.com.my/tech/tech-news/2019/11/05/hacker-claims-to-have-stolen-personal-data-of-universiti-malaysia-sabah-students

Haliding, Safri. "Mendorong Indonesia Jadi Pusat Islamic Fintech Dunia," September 15, 2019. http://ekonomi.metrotvnews.com/analisa-ekonomi/VNnR0AXN-mendorong-indonesia-jadi-pusat-islamic-fintech-dunia.

Jakarta, LBH. "Korban Pinjaman Online," n.d. https://www.bantuanhukum.or.id/web/banyak-masalah-lbh-jakarta-buka-posko-pengaduan-korban-pinjaman-online/.

"Kasus Bocor Data Malindo 2 Persen Milik WNI," n.d. https://bisnis.tempo.co/read/1253036/kominfo-kasus-bocor-data-malindo-air-2-persen-milik-wni/full&view=ok

"University Malaya PDPD Looking Into Report of Massive Data Breach Affecting the University," n.d. https://www.thestar.com.my/news/nation/2019/10/19/university-malaya-pdpd-looking-into-report-of-massive-data-breach-affecting-the-university.

"Puluhan Data Pengguna Ponsoel Bocor Di Malaysia," n.d. https://www.cnnindonesia.com/internasional/20171102100434-106-252917/puluhan-juta-data-pengguna-ponsel-bocor-di-malaysia.

"Patients Personal Data Exposed on National Neurology Registry Website," n.d. https://www.thestar.com.my/news/nation/2019/10/23/over-17000-patients039-personal--data-exposed-on-national-neurology-registry-website.

Percentage Distribution of Indonesian Fintech Ecosystem 2018. "Fintech News Singapore," n.d. http://fintechnews.sg/20712/indonesia/fintech-indonesia-report-2018/

Pitoko, Ridwan Aji. "Tumbuh Pesat, 135 Perusahaan Fintech Kini Ada Di Indonesia," n.d. https://ekonomi.kompas.com/read/2018/04/13/214800426/tumbuh-pesat-135-perusahaan-fintech-kini-ada-di-indonesia.

Saragih, Barita. "Tantangan Hukum Atas Aktivitas Internet." *Kompas*, July 9, 2000.

Interviews

Sirait, Jeany. Public Lawyer at Jakarta Legal Aid (LBH Jakarta), October 8, 2019.

Zulhuda, Sonny. IIUM Research, September 1, 2019.