Journal of Infrastructure, Policy and Development 2024, 8(7), 4158.
https://doi.org/10.24294/jipd.v8i7.4158

Article

Personal data protection in fintech: A case study from Indonesia

Acep Rohendi[1,*], Dona Budi Kharisma[2]

[1] Universitas Adhirajasa Reswara Sanjaya (ARS University), Bandung 40283, Indonesia
[2] Faculty of Law, Universitas Sebelas Maret, Surakarta 57126, Indonesia
*** Corresponding author:** Acep Rohendi, arohendi@ars.ac.id

CITATION

Rohendi A, Kharisma DB. (2024). Personal data protection in fintech: A case study from Indonesia. Journal of Infrastructure, Policy and Development. 8(7): 4158. https://doi.org/10.24294/jipd.v8i7.4158

ARTICLE INFO

Received: 10 January 2024
Accepted: 6 April 2024
Available online: 26 July 2024

Abstract: Personal data privacy regulation and mitigation are critical in implementing financial technology (fintech). Problems with fintech users' data might result from data breaches, improper usage, and trade. Issues with personal data will result in financial losses, crimes, and violations of personal information. This legal research used three approaches: conceptual, comparative, and statute-based. In order to implement the statutory method, all laws and regulations pertaining to the legal concerns of information technology, fintech, personal data security, and protection are reviewed. Due to the nature of the sources of data, this study mainly used literature study and document observation to collect the data. Then, legal interpretation, legal reasoning, and legal argumentation are all included in the qualitative juridical analysis. This article recommends two strategies that Indonesia should take to provide personal data protection, including: 1) establishing the Personal Data Protection Commission (PDPC); and 2) improving the financial literacy of consumers.

Keywords: personal data; protection; regulation; fintech

1. Introduction

Financial service innovation that has been influenced by technological developments is called financial technology (fintech). Fintech can be defined as the use of technology in innovating financial services via the internet network (Wiwoho and Kharisma, 2021). In Indonesia, fintech to access financial services is increasing along with the rapidly massive digital transformation. The statistics of Bank Indonesia show that in 2024, the digital payment transaction in Indonesia shows a positive trend. The value of digital banking transactions will continue to grow 23.2% in 2024 to reach IDR 71,584 trillion, and grow 18.8% in 2025 to IDR 85,044 trillion. E-commerce transactions will also continue to grow 2.8% to IDR 487 trillion in 2024 and 3.3% to IDR 503 trillion in 2025 (Bank Indonesia, 2023).

In the fintech lending sector, until September 2023 the performance of the fintech peer to peer (P2P) lending industry showed good growth performance. Outstanding financing distributed by fintech P2P lending grew by 14.28 percent yoy, with nominal financing of IDR 55.70 trillion. This growth was also accompanied by maintained financing risk quality with a Default Rate (TWP 90) of 2.82 percent (OJK, 2023).

As Wiwoho and Kharisma (2021) found, the rising middle class and widespread internet use in Indonesia are the two main drivers of the country's digital economy. Fintech in Indonesia will also continue to grow to accommodate consumer needs and community lifestyle. For developing countries like Indonesia, fintech can encourage increased financial literacy because it increases access to financial services and sources of capital (Wiwoho and Kharisma, 2021). In addition, the improving financial landscape and the degree of literacy and knowledge regarding financial services and

products will hasten the fintech industry's expansion in Indonesia (Rohendi et al, 2023). In fact, the COVID-19 pandemic has also contributed to using fintech in Indonesia (Kharisma, 2020; Muryanto et al., 2021).

By 2025, President Joko Widodo projects that Indonesia's digital economy will be the biggest in Southeast Asia, valued at an estimated $133 million. However, the President reminded that the development of fintech can also pose potential risks such as cyber-crime, money laundering, terrorism financing, and the misuse of personal data (Secretariat of President of the Republic of Indonesia, 2020).

However, there are still issues with this positive trend, one of which is the theft and misuse of personal information (Wiwoho et al., 2022). From January to June 2020, the Indonesian Consumers Foundation (YLKI) documented 277 occurrences of e-commerce data theft, of which 54 were reported to them. At least 27 instances of P2P lending data leaks and five cases involving electronic money were reported in the fintech industry (Lokadata.id, 2020; YLKI, 2020). Earlier in May 2020, a large case of personal data leak occurred. The data of 91 million users of Tokopedia e-commerce platform were allegedly leaked (CNN Indonesia, 2020). The Indonesian Consumers Community (KKI) then filed a lawsuit against Tokopedia for IDR100 billion (CNBC Indonesia, 2020).

The latest cases of data leaks happened in the early 2022. First, the data of 6 million patients from the Ministry of Health was allegedly leaked and sold on the Raid Forums, an online discussion forum. This reminds us of the leak of population data from the government servers that happened earlier. Second, 160 thousand data of job applicants at Pertamina were also allegedly leaked and shared for free in Raid Forums (CNN Indonesia, 2022; Compass, 2022).

Problems of such data leak will potentially lead to crimes (Rohendi, 2020). Applications used in fintech generally use personal databases. Therefore, if consumers' personal data is leaked or stolen, it is vulnerable to misuse for fraud, bank account break-ins, or even illegal online loan applications. In many cases, P2P lending service providers even threaten the customers that they will spread their personal data if they do not pay the installment on time (Kharisma and Hunaifa, 2022).

Some scholars have investigated the issues of personal data and fintech. Stewart and Jürjens (2018) found that consumer confidence and data security are crucial to the usage of fintech in Germany. Meanwhile, Addae et al. (2017) found that the attitude toward personal data (privacy concerns, cost-benefit analysis, protective behavior, awareness, accountability, and security) plays a big part in data security (Addae et al., 2017).

A few studies also contrast the laws and practices around the protection of personal data across several nations (Da Veiga et al., 2019; Gibbs, 2020;) and the impact of data breaches (Gwebu and Barrows, 2020; Holtfreter and Harrington, 2015; Juma'h and Alnsour, 2020). Some studies have concluded that regulations governing the protection of personal data have an essential role in data security in the e-commerce sector, including cyber-crime prevention (Bechara and Schuch, 2020; Belwal et al., 2020; Kharisma and Hunaifa, 2022; Ng and Kwok, 2017; Younies and Al-Tawil, 2020; Zhu et al., 2020). Some studies recommend that fintechs must diligently assess cybersecurity risks and stay updated on evolving data regulations and compliance demands (Sudarwanto and Kharisma, 2021; Wiwoho et al, 2024).

However, more research needs to be done to determine how urgent it is to create laws protecting personal data in Indonesia's fintech industry. This article, therefore, explores the problems and legal issues in personal data protection in the fintech sector. The results of this exploration will be a construction of regulations and mitigations of personal data protection in the fintech sector.

2. Methodology

This legal research used three approaches: conceptual, comparative, and statute-based. In order to implement the statutory method, all laws and regulations pertaining to the legal concerns of information technology, fintech, personal data security, and protection are reviewed. By contrasting the laws governing the protection of personal data in several nations and regions, including South Korea, Hong Kong, Malaysia, and the European Union, the comparative approach is used.

The conceptual method was then used to further examine the findings of the statute approach and comparison approach investigations. The end product would be a legislative framework for the development of personal data protection laws in Indonesia's fintech industry.

Principal and secondary legal materials served as the study's primary data sources. Legislation, official documents or treatises used in the drafting of legislation, and judicial rulings make up the majority of primary legal material. On the other hand, all unofficial publications and papers, including legal dictionaries, legal periodicals, textbooks, and analyses of court decisions, are categorized as secondary legal materials (Marzuki, 2019).

The Act analyzed in this research is the Indonesian Personal Data Protection Act No. 27 of 2022. This research looks at primary legal sources from other nations in addition to the laws and regulations that are now in effect in Indonesia. Some of these regulations include the Malaysia Personal Data Protection Act No. 709 of 2010 (PDPA Malaysia), the Hongkong Personal Data Privacy Ordinance of 2012 (PDPO Hong Kong), Europe Union Data Protection Directive and other various laws governing the protection of personal data in some other countries.

Due to the nature of the sources of data, this study mainly used literature study and document observation to collect the data. Then, legal interpretation, legal reasoning, and legal argumentation are all included in the qualitative juridical analysis.

3. Findings

3.1. Urgency of personal data protection in the fintech sector

The process of drafting a regulation should consider the philosophical, sociological, and the juridical aspects; so that the regulation meets the needs and problems that exist in the society (Rohendi, 2015). In other words, the urgency of a new regulation can be seen through the analysis from the points of view from the philosophical, sociological, and juridical aspects.

3.1.1. Philosophical aspects of personal data protection

The term "philosophical aspects" refers to all facets of life philosophy, legal consciousness, and legal concepts (rechtsidee) that influence Indonesian culture and

philosophy, which are drawn from Pancasila and the Preamble of the Republic of Indonesia's 1945 Constitution (Kharisma, 2020).

Pancasila (Five Principles) is the philosophical underpinning of personal data protection in Indonesia's fintech industry, the Indonesian state philosophy. Pancasila is the rechtsidee which is a construction of thoughts that lead the law to what the Indonesian nation aspires to.

Pancasila's second precept is "A just and civilized humanity". Accordingly, the goal of protecting personal data should be to build a civilized society that can ensure lawfulness and order. This objective can be reached through the responsible and safe use of fintech, prioritizing consumer protection, especially through a well-managed protection of consumers' personal data. "Social justice for all Indonesian people" is the fifth principle, and it represents another solid base. In the fintech industry, protecting personal data also attempts to establish social fairness for all Indonesians. It is also one of the forms of government responsibilities, especially in terms of consumer protection from illegal practices of fintech.

Since Pancasila mandates the protection of personal data as the fundamental standard of the state, all laws and regulations should further expound on this topic.

3.1.2. Sociological aspects of personal data protection

According to the sociological viewpoint, laws are created to address different societal demands. A few sociological factors demonstrate the significance of protecting personal data in the fintech industry. Priorities must be set for safeguarding people's rights in society with regard to the gathering, using, storing, and sharing of personal data. Adequate protection of data and personal privacy will create a trust that people willingly provide personal data for a greater range of public interests.

Second, there have been several instances of theft, loss, and misuse of personal data. A rise in incidents of personal data leaks has coincided with the development of Indonesia's digital economy. After this, the information is exploited for online loan applications, bank account theft, and fraud. Some P2P lending providers, for example, have even threatened their customers that they would spread their personal data when they fail to pay the installment on time (Hidajat, 2019).

The financial industry's misuse of personal data has reached an emergency proportion. Data breaches have become an emerging threat in the fintech industry sector (Wiwoho and Kharisma, 2021). Ignoring this will have more detrimental effects on the long-term viability of Indonesia's digital economy. The fact that Indonesia does not yet have an Act that mainly governs the security of personal data in the fintech industry makes the problem worse.

In summary, Indonesia has to pass a particular Act on the protection of personal data in the fintech industry immediately. This will act as the legislative foundation for risk systemic minimization, consumer protection, and the avoidance of illicit fintech practices.

3.1.3. Juridical aspects of personal data protection

From a legal perspective, rules are created to address legal issues or close legal loopholes in order to maintain legal stability and a sense of legal fairness throughout society. Among other things, some of these legal concerns include out-of-date rules, regulations that need to be more consistent or consistent, and regulations that have

fewer enforcement powers than Acts. In certain instances, there are regulations in place, but they need to be more present.

Different from some other nations like Hong Kong, Singapore, Malaysia, and some other countries in Southeast Asia and the European Union, Indonesia does not yet have an Act that mainly controls the protection of personal data.

3.2. Legal issues of personal data protection in the fintech sector

Due to Indonesia's ongoing legal challenges about the security of personal data, the number of cases of personal data misuse in the fintech industry rises annually. This section will elaborate those existing legal issues.

3.2.1. No personal data protection commission

Regulation, supervision, and guidance concerning personal information in Indonesia remain sectoral. That is, each ministry or institution regulates and supervises the acquisition, use, utilization and disclosure of personal data.

The Ministry of Communication and Informatics, Bank Indonesia, and OJK oversee the fintech industry's compliance regarding personal data protection. This is so because an Act authorizes each of them.

Act No. 21 of 2011, for instance, gives OJK the power to oversee and manage bank and non-bank financial entities. Act No. 23 of 1999, recently revised by Act No. 6 of 2009, offers Bank Indonesia comparable jurisdiction. Based on Act No. 11 of 2008, as most recently updated by Law No. 9 of 2016 on Electronic Information and Transactions, the Ministry of Communication and Informatics is also empowered to regulate and control electronic systems.

In summary, personal data protection in Indonesia's fintech industry remains sub-sectoral and subject to many institutional authorities. This does not happen in other countries, because they have a special commission of personal data protection. Hong Kong has the Privacy Commissioner for Personal Data; Singapore has the Personal Data Protection Commission and Administration; Malaysia has the Personal Data Protection Commissioner; South Korea has the Personal Information Protection Commission (PIPC); and the UK has the Information Commissioner's Office. Most of these commissions are in charge of monitoring and enforcing everyone's adherence to the rules regarding protecting personal information.

3.2.2. No criminal sanctions for data breach perpetrators

The lack of a specific Act governing personal data protection causes those who commit data breaches not to be subject to criminal penalties. Actors involved in data breaches can use this legal vulnerability.

The Minister of Communication and Information Technology's Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, Article 32, gives the owner of damaged personal data the option to file a civil lawsuit for the breach of personal data confidentiality. A civil lawsuit may be filed if attempts to settle a disagreement over the breach of personal data confidentiality have failed to reach an amicable agreement or through other alternative resolution methods. The terms of enacted laws and regulations may be followed while filing a civil action.

Owners of personal data who feel wronged may bring a civil complaint for the failure of confidential personal data protection under Article 32 of the Regulation of

the Minister of Communication and Informatics No. 20 of 2016 on the Protection of Personal Data in Electronic Systems. If attempts at alternative settlement have failed to resolve concerns about the breach of confidentiality or protection of personal data, then civil actions may be filed.

Regarding punishments, some Bank Indonesia and Financial Services Authority regulations solely govern administrative penalties for fintech companies that violate personal data privacy laws. Put differently, fintech operators face only administrative penalties when they acquire, gather, process, analyze, keep, display, announce, transmit, and/or distribute personal data. Administrative punishments can be written or verbal warnings, activity suspensions for a set period, online notices on websites, and/or verbal warnings.

However, administrative sanctions are not effective enough for personal data protection. Therefore, criminal sanctions are another alternative, especially to deal with the problems of data breaches. Strict penalties, such as fines, incarceration, the loss of particular rights, or the seizure of specific items, should be used to protect personal data, depending on the seriousness of the crimes committed. Therefore, criminal sanctions need to be constructed in the Act of the Protection of Personal Data in the Fintech Sector.

3.3. Regulation and mitigation of personal data protection in the fintech sector

Data breach, personal data misuse, and personal data trade are the three main legal issues surrounding personal data. A data breach occurs when private or sensitive information is accessed without authorization. This incidence results from illicit conduct in cyberspace when specific individuals obtain sensitive and private data by breaking into a computer system or network without authorization. he Department of Justice in the United States provides an additional definition, which reads as follows: “The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic.” The key is the unauthorized activities (PUSFID, 2020). In other words, a data breach occurs when someone obtains or steals information from a system without the owner’s knowledge or approval.

Data breach can also happen to either fintech start-ups or large fintech companies. The stolen data are usually in the form of sensitive information, Population Identity Number (ID number), biological mother’s name, transaction password, and other confidential data such as customer data or national security issues. The data is then used to access fintech accounts and to steal more personal data that result in financial losses.

Not only because of system vulnerabilities, data breaches can also occur due to phishing. Phishing is a crime in the form of false communications that appears as if it came from a trusted source. Phishing can harm all kinds of data sources (Kharisma and Hunaifa, 2022). Phishing can take access to online accounts and personal data such as ID number, credit card numbers, ATMs, or other important data. Sometimes the victim of phishing is not aware that he is the target of a crime. Phishing victims

will divulge critical information, including passwords for financial apps, credit card and banking information, and personally identifiable information.

In the fintech industry, the trade of personal data also raises the risk of criminal activity. The practice of e-KTP (e-ID) trade is rife on social media forums, marketplaces, to cyber-crime sites (dark web). Many apply for online loans on illicit fintech peer-to-peer (p2p) lending platforms using this publicly available personal data.

This case is due to the easy registration and application of funds on illegal loan platforms. Prospective borrowers usually only need an e-KTP, bank account number, and telephone number. With such easy loan application requirements, the practice of personal data buying and selling is increasingly common. On Facebook, for example, there are still several groups that offer e-KTP services that can be used as online loan requirements, at relatively low prices (Katadata, 2021).

Personal data breaches also occur in the payment collection process of the P2P lending fintech. When payments are not received on time, fintech companies frequently threaten their clients, their families, managers, or supervisors at the client's place of employment. They even can access data from the customer's smartphone (Hidajat, 2019). They then threaten the customers of distributing the data.

In Indonesia, every citizen is genuinely entitled to protect their data under the constitution (Dewi, 2016; Djafar, 2019). In other words, it is acknowledged that protecting personal information is both a human right and a means of ensuring the lives of Indonesian individuals.

The Republic of Indonesia's 1945 Constitution mentions personal data protection in Article 28 G paragraph (1) and Article 28 H paragraph (4). Therefore, it is against human rights to violate someone's personal information. Furthermore, the 1945 Constitution's guarantee of personal data protection makes it legally required for the State to act as each citizen's guardian (Makarim, 2019; Rosadi and Pratama, 2018).

As a result, Indonesia needs to move quickly to develop laws to mitigate personal data protection in the fintech industry. The following are some topics that need to be discussed during construction.

3.3.1. Creation of the commission for the protection of personal data

The Personal Data Protection Commission, Hong Kong, Singapore, and the United Kingdom have successfully protected their citizens' personal information, this commission was set up to oversee, regulate, and encourage everyone involved in protecting personal information. These powers should be in a single organization to ensure efficient oversight and control.

One tactic the government may use to strengthen citizen data privacy is creating a commission to protect personal information. Establishing a Commission to oversee the security of personal data is imperative for Indonesia (Makarim, 2019). The Commission will be in charge of advising and monitoring digital platforms regarding the handling and security of users' data (Belwal et al., 2020; Combe, 2009).

Ideally, the Personal Data Protection Commission will also have the power to function as a substitute forum for resolving disputes about personal data other than the court. Alternative dispute resolution forums are important because the process of resolving personal data disputes tends to be faster, more effective, less costly, and resolved by expert mediators or arbitrators.

3.3.2. Financial literacy improvement

Another factor that may cause data breach is the low financial literacy of the consumers. For example, many consumers use weak username and password to access fintech. Hackers can more easily decipher a weak and unsafe password if it comprises whole words or phrases. Customers may inadvertently download malware or viruses by visiting a hacked website. This may happen when they use not updated browsers, applications, or operating systems with security flaws.

Low financial literacy is also evident when consumers access illegal fintech applications. Some of them are not able to distinguish licensed from illegal fintech operators. As a result, many are trapped in illegal fintech and investment practices. When they access an illegal P2P lending fintech application, for example, the personal data entered to the application is vulnerable to misuse and trade.

The results of the National Survey of Financial Literacy and Inclusion, which reveal a financial literacy index of 38.03% and a financial inclusion score of 76.19%, further demonstrate the poor level of financial literacy among Indonesians. This indicates that most Indonesians need to be better versed in the features of the economic goods and services provided by official monetary institutions.

Financial inclusion, consumer protection, individual well-being, and community empowerment all depend heavily on financial literacy (OJK, 2021). Therefore, the government, Bank Indonesia, OJK, and all associations of financial services providers need to collaborate to educate the public and raise their awareness of their personal data protection, especially when accessing financial services.

4. Conclusion

One of the biggest obstacles to the growth of Indonesia's fintech sector is the security of personal data. Cases of personal data breaches have resulted in financial losses. To overcome these challenges, the Indonesian Personal Data Protection Act Number 27 of 2022 needs to be supported by the Personal Data Protection Commission. This commission was set up to oversee, regulate, and encourage everyone involved in protecting personal information. Indonesia is recommended to establish the Personal Data Protection Commission which functions as advising and monitoring digital platforms regarding the handling and security of users' data. Besides risk mitigation, consumers also need to increase their financial literacy to prevent themselves from being trapped in illegal fintech practices. The stakeholders need to collaborate to educate the public and raise their awareness of their personal data protection, especially when accessing financial services.

Author contributions: Conceptualization, AR and DBK; methodology, AR; software, DBK; validation, AR and DBK; formal analysis, AR; investigation, DBK; resources, DBK; data curation, DBK; writing—original draft preparation, AR and DBK; writing—review and editing, AR and DBK; visualization, DBK; supervision, AR; project administration, DBK; funding acquisition, AR. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

Addae, J. H., Brown, M., Sun, X., et al. (2017). Measuring attitude towards personal data for adaptive cybersecurity. Information & Computer Security, 25(5), 560–579. https://doi.org/10.1108/ics-11-2016-0085

Da Veiga, A., Vorster, R., Li, F., et al. (2019). Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements. Information & Computer Security, 28(3), 399–422. https://doi.org/10.1108/ics-11-2018-0135

Bank Indonesia. (2021). Payment System Statistics (Indonesian). Available online: https://www.bi.go.id/id/statistik/ekonomi-keuangan/ssp/uang-elektronik-transaksi.aspx (accessed on 22 December 2023).

Bank Indonesia. (2023). Bank Indonesia Annual Meeting 2023: Synergy to Strengthen National Economic Resilience and Revival (Indonesian). Available online: https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2532123.aspx (accessed on 22 December 2023).

Bechara, F. R., & Schuch, S. B. (2020). Cybersecurity and global regulatory challenges. Journal of Financial Crime, 28(2), 359–374. https://doi.org/10.1108/jfc-07-2020-0149

Belwal, R., Al Shibli, R., & Belwal, S. (2020). Consumer protection and electronic commerce in the Sultanate of Oman. Journal of Information, Communication and Ethics in Society, 19(1), 38–60. https://doi.org/10.1108/jices-09-2019-0110

Combe, C. (2009). Observations on the UK transformational government strategy relative to citizen data sharing and privacy. Transforming Government: People, Process and Policy, 3(4), 394–405. https://doi.org/10.1108/17506160910997892

CNN Indonesia. (2022). Endless Personal Data Leaks in RI, read more here (Indonesian). Available online: https://www.cnnindonesia.com/teknologi/20220112191045-185-745842/kebocoran-data-pribadi-yang-tak-berujung-di-ri (accessed on 22 December 2023).

CNN Indonesia. (2020a). Full Chronology of 91 million Tokopedia Accounts Leaked and Sold (Indonesian). Available online: https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual (accessed on 22 December 2023).

CNBC Indonesia (2020b). 91 million User Data Leaked, Tokopedia Sued for Rp 100 M (Indonesian). Available online: https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-digugat-rp-100-m (accessed on 22 December 2023).

Da Veiga, A., Vorster, R., Li, F., et al. (2019). Comparing the protection and use of online personal information in South Africa and the United Kingdom in line with data protection requirements. Information & Computer Security, 28(3), 399–422. https://doi.org/10.1108/ics-11-2018-0135

Dewi, S. (2016). Concept of Legal Protection of Privacy and Personal Data Associated with the Use of Cloud Computing in Indonesia (Indonesian). Yustisia Jurnal Hukum, 5(1), 22–30. https://doi.org/10.20961/yustisia.v5i1.8712

Dewi Rosadi, S., & Gumelar Pratama, G. (2018). The urgency of protecting private data in the era of digital economy in Indonesia (Indonesian). Veritas et Justitia, 4(1), 88–110. https://doi.org/10.25123/vej.2916

Djafar, W. (2019). Personal Data Protection in Indonesia: Landscape, Urgency, and Need for Update (Indonesian). Jurnal Becoss, 1(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030

GreenLeaf, Graham. (2014). Asian Data Privacy Laws—Trade and Human Rights Perspectives. Oxford University Press.

Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: is the industry different? Journal of Hospitality and Tourism Technology, 11(3), 511–527. https://doi.org/10.1108/jhtt-11-2019-0138

Giakoumopoulos, C., Buttarelli, G., & O'Flaherty, M. (2018). Handbook on European data protection law 2018. Publications Office of the European Union.

Hidajat, T. (2020). Unethical practices peer-to-peer lending in Indonesia. Journal of Financial Crime, 27(1), 274–282. https://doi.org/10.1108/jfc-02-2019-0028

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. Journal of Financial Crime, 22(2), 242–260. https://doi.org/10.1108/jfc-09-2013-0055

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. International Journal of Accounting & Information Management, 28(2), 275–301. https://doi.org/10.1108/ijaim-01-2019-0006

Kang, J. (2006). Information Privacy in Cyberspace Transactions. Stanford Law Review, 50(4), 1193. https://doi.org/10.2307/1229286

Katadata, Personal Data Theft in the Vortex of Illegal Fintech Business (Indonesian). Available online: https://katadata.co.id/ariayudhistira/analisisdata/609a43a46aa5e/pencurian-data-pribadi-dalam-pusaran-bisnis-fintech-ilegal (accessed on 22 December 2023).

Kharisma, D. B. (2020). Urgency of financial technology (Fintech) laws in Indonesia. International Journal of Law and Management, 63(3), 320–331. https://doi.org/10.1108/ijlma-08-2020-0233

Kharisma, D. B., & Hunaifa, A. (2022). Comparative study of disgorgement and disgorgement fund regulations in Indonesia, the USA and the UK. Journal of Financial Crime, 30(3), 635–649. https://doi.org/10.1108/jfc-01-2022-0022

Kompas, A Series of Cases of Leaked Population Data on Government Servers, click to read (Indonesian). Available online: https://www.kompas.com/tren/read/2022/01/08/163000065/sederet-kasus-kebocoran-data-penduduk-di-server-pemerintah?page=all (accessed on 22 December 2023).

Lokadata.id, More Data Leak Cases, Online Shopping Most Vulnerable (Indonesian). Available online: https://lokadata.id/artikel/kasus-kebocoran-data-semakin-banyak-belanja-daring-paling-rentan (accessed on 22 December 2023).

Makarim, E. (2019). Privacy and Personal Data Protection (Indonesian). Available online: http://www.dpr.go.id/dokakd/dokumen/K1-RJ-20200701-114522-4891.pdf (accessed on 22 December 2023).

Makarim, E. (2020). Legal Liability for Personal Data Leakage (Indonesian). Available online: https://www.hukumonline.com/berita/baca/lt5f067836b37ef/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh--edmon-makarim?page=all (accessed on 22 December 2023).

Marzuki, P.M. (2019). Penelitian Hukum, 14th Book Print. Prenada Media Group.

Muryanto, Y. T., Kharisma, D. B., & Ciptorukmi Nugraheni, A. S. (2022). Prospects and challenges of Islamic fintech in Indonesia: a legal viewpoint. International Journal of Law and Management, 64(2), 239–252. https://doi.org/10.1108/ijlma-07-2021-0162

Murray, A. (2013). Information technology law: The law and society. Oxford University Press.

Ng, A. W., & Kwok, B. K. B. (2017). Emergence of Fintech and cybersecurity in a global financial centre. Journal of Financial Regulation and Compliance, 25(4), 422–434. https://doi.org/10.1108/jfrc-01-2017-0013

Financial Services Authority (OJK). (2023). Press Release: Launch of Fintech P2P Lending Roadmap 2023-2028 (Indonesian). Available online: https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/Peluncuran-Roadmap-Fintech-P2P-Lending-2023-2028.aspx (accessed on 22 December 2023).

Financial Services Authority (OJK). (2020). Indonesia's National Financial Literacy Strategy (SNLKI) 2021-2025 (Indonesian). Available online: https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Documents/Pages/Strategi-Nasional-Literasi-Keuangan-Indonesia-2021-2025/Strategi%20Nasional%20Literasi%20Keuangan%20Indonesia%202021-2025.pdf (accessed on 22 December 2023).

Financial Services Authority (OJK). (2021). Fintech Lending Statistics 2020 (Indonesian). Available online: https://www.ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/-Statistik-Fintech-Lending-Periode-Desember-2020.aspx (accessed on 22 December 2023).

PUSFID (2024). Data Breach Response Team, Available online: https://forensics.uii.ac.id/data-breach-response-team/ (accessed on 22 December 2023).

Rohendi, A. (2015). Consumer Protection in E-Commerce Transactions from National and International Law Perspectives (Indonesian). Ecodemica, 3(2).

Rohendi, A. (2020). Big Data Legal Protection (Indonesian). Jurnal Sain Manajemen, 2(2), 1–5.

Rohendi, A., Asriani, A., & Kharisma, D. B. (2023). Regulation for startups in Indonesia: Problems and recommendations. Cogent Business & Management, 10(3). https://doi.org/10.1080/23311975.2023.2276993

Secretariat of the President of the Republic of Indonesia. (2020). Remarks by President Joko Widodo at the Indonesia Fintech Summit 2020 and Fintech Week 2020. Available online: https://www.presidenri.go.id/siaran-pers/presiden-jokowi-buka-indonesia-fintech-summit-2020-secara-virtual/ (accessed on 22 December 2023).

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. Information and Computer Security, 26(1), 109–128. https://doi.org/10.1108/ICS-06-2017-0039

Sudarwanto, A. S., & Kharisma, D. B. B. (2021). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime, 29(4), 1443–1457. https://doi.org/10.1108/jfc-09-2021-0193

Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: Privacy concerns about personal data on smartphones. Information & Computer Security, 23(4), 80–89. https://doi.org/10.1108/ics-10-2014-0071.

Yayasan Lembaga Konsumen Indonesia (YLKI). (2020). Data on Consumer Personal Data Leaks from January to June 2020 (Indonesian). Available online: http://ylki.or.id/category/beritaliputan-media/ (accessed on 22 December 2023).

Younies, H., & Al-Tawil, T. N. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). Journal of Financial Crime, 27(4), 1089–1105. https://doi.org/10.1108/jfc-04-2020-0055

Yusoff, Z.M. (2011). The Malaysian Personal Data Protection Act 2010: A Legislation Note. New Zealand Journal of Public and International Law, 9(1).

Watson, A., & Lupton, D. (2020). Tactics, affects and agencies in digital privacy narratives: a story completion study. Online Information Review, 45(1), 138–156. https://doi.org/10.1108/oir-05-2020-0174

Wiwoho, J & Kharisma, D. B. (2021). Isu-Isu Hukum di Sektor Fintech. Setara Press.

Wiwoho, J., Kharisma, D. B., & Wardhono, D. T. K. (2021). Financial Crime In Digital Payments. Journal of Central Banking Law and Institutions, 1(1), 47–70. https://doi.org/10.21098/jcli.v1i1.7

Wiwoho, J., Trinugroho, I., Kharisma, D. B., et al. (2023). Islamic crypto assets and regulatory framework: evidence from Indonesia and global approaches. International Journal of Law and Management, 66(2), 155–171. https://doi.org/10.1108/ijlma-03-2023-0051

Zhu, R., Srivastava, A., & Sutanto, J. (2020). Privacy-deprived e-commerce: the efficacy of consumer privacy policies on China's e-commerce websites from a legal perspective. Information Technology & People, 33(6), 1601–1626. https://doi.org/10.1108/itp-03-2019-0117