The Influence of Indonesian Culture Toward Attitudes and Surveillance of Data Privacy in Financial Sectors

Anjar Sri Ciptorukmi N[1], Umi Khaerah Pati[2], Pujiyono[3], Anugrah Muhtarom Pratama[4], Muammar Azmar M. Faruq[5]
{ anugrah@gmail.com[1] , umikhaerah@staff.uns.ac.id[2] , pujifhuns@staff.uns.ac.id[3] , pratamanugrah23@gmail.com[4]}

Department of Private Law, Faculty of Law, Universitas Sebelas Maret, Indonesia[123]
Faculty of Law, Universitas Sebelas Maret, Indonesia[4]
Judge of the Indonesian District Court[5]

Abstract. This paper examines how the culture of Indonesia contributes to the nation's behaviour regarding its privacy data and its legal products in the form of regulations implemented by the government in anticipation of the risk of data breaches in the financial sector in Indonesia. It is socio-legal research that examines how the law relates to the societal context or how effective it is and its relation to its ecological context. The results show that the communalistic culture that develops in Indonesia affects how the nation views privacy and how the readiness of regulation, supervision and law enforcement in the courts

Keywords: Attitudes, Data Pivacy,Indonesian Culture, Surveillance,

1 Introduction

Based on the 2020 Indonesian Digital Literacy Status Research by Katadata Insight Center (KIC), it was revealed that the public's understanding of the importance of personal data confidentiality has not been high [1]. Furthermore, A total of 67.4% of internet users in Indonesia shared their date of birth, and 53.7% wrote down their phone number on social media. Meanwhile, a survey conducted by the Public Perception Survey on The Protection of Personal Data through Computer Aided Web Interviewing (CAWI) revealed that as many as 28.7% of the public has experience of misuse of Indonesian personal data. Some experts argue that a nation's behavior towards privacy is influenced by several factors, one of which is culture [2]. Not only how citizens' attitudes to privacy, culture also affects the readiness of regulators and law enforcement to the urgency of regulation, supervision and dispute resolution related to privacy data. In this paper will examine how the culture of the Indonesian affects their attitude towards privacy data and current legal product in both at the supervisor level and the court level, especially privacy data in the banking and fintech sectors.

2 Method

This research is socio-legal research with a qualitative approach. Socio-legal research positions the law in a broad societal context, with various methodological implications [3]. This study examines how the law relates to the societal context or how effective the law is and its relation to its ecological context [4] This paper tries to provide a view of the influence of

MALAPY 2022, May 28, Tegal, Indonesia

DOI 10.4108/eai.28-5-2022.2320440

Indonesian culture on behavior on data privacy and the legal products specifically in the financial sector.

3. Result & Discussion

Regulation of internet privacy is currently being debated, particularly in Europe. According to researchers, concerns about information privacy are not universal, but are influenced by a variety of factors such as demographic differences, privacy attitudes, cultural dimensions, and contextual/situational factors [2].

Law as a system, it can be judged from 2 sides that are different are as follows [5] The law was seen as a value system, where the entire law-enforcement in order based on the grundnorm which later became the source of the values at the same time guidelines for law enforcement itself; The law is seen as part of the Community (social reality), in which the law cannot be separated from the environmental community because, in this case, the law is one of the subsystems of the subsystem-other social subsystem.

Regulatory involvement responds to individual concerns about online privacy. The ideal creation of a unified privacy regulatory framework to accommodate disparate concerns appears to be impossible. These disparate issues are mostly related to different cultures and different views on privacy [6]. Citizens respond to privacy data depending on their country's culture, according to the Hofstede's cultural dimensions theory (firstly developed in the 1960s and 1970s at IBM [7]) Geert Hofstede's framework for cross-cultural communication, which demonstrates the effects of a society's culture on its members' values and how these values connect to behavior, recently identified the six cultural dimensions models [8]. It is called Hofstede's cultural dimensions, Individualism versus Collectivism is one of Hofstede's cultural dimensions, which is related to the integration of individuals into primary groups. Individualism is defined as a preference for a loosely-knit social framework in which individuals are expected to care for only themselves and their immediate families. Cultural values and norms largely determine how online privacy is perceived and negotiated [9].

Individualism Culture (Europe and North America) and Collectivism Culture (Asia, Africa, South America and Pacific Rim) are two broad categories of world culture [10]. Different cultures, different ways people treat privacy. People in individualistic cultures tend to be more concerned about online privacy. They tend to value private life more, whereas collectivistic societies are more accepting of groups' and organizations' intrusion into an individual's private life [6]. These findings imply that countries with higher levels of individualism will have less government involvement and more individualistic approaches to information privacy regulation. This, however, is not the same as the effect of individualism on attitudes toward information privacy. Individualists generally believe in the right to privacy. Individualistic cultures prefer less government intervention, but they are more concerned about the privacy of their personal information than collective cultures [11]. The GLOBE variables capture in-group collectivism, which is the degree to which individuals express pride, loyalty, and cohesiveness in their organizations or families. People emphasize group relatedness. Based on the arguments presented above, these societies should embrace stronger regulation if they are the polar opposite of individualism. Individualism with a high score indicates that people are only loosely connected to society and are expected to look after themselves. In contrast, in a collectivist society, people can be protected by some strong cohesive groups throughout their lives as a reward for their unwavering loyalty. However, the relationship between individualism and time preference is unclear. On the one hand, social connection in a collectivist culture may provide its citizens with a "cushion" or safety net in the event of a loss.[12]. Bellman et al.(2004) developed an alternative theory implying that such societies will be less concerned with

information privacy and will feel less compelled to seek government intervention [13]. The reason they suggest is that low individualism and high collectivist societies have a greater acceptance that groups, including the government, can intrude on the private life of the individual. In support of this intrusion theory they cite Milberg et al [14].

The group collectivism dimension refers to how much pride members of a society take in belonging to small groups such as their family and close circle of friends, as well as the organizations in which they work. Being a member of a family and a close group of friends is important in countries with high group collectivism scores, and there is a tendency to prioritize friends and family over society's rules and procedures. This focus and proclivity to share may cause people to be less concerned about information privacy, resulting in less stringent codification of these elements in law such countries include the Asian countries Singapore, Malaysia and Japan. One explanation for this apparent anomaly is that the right to privacy is not a basic tenet of such societies. Furthermore, societies with a high level of group collectivism (Reflects the degree to which individuals express pride, loyalty and cohesiveness in their organizations or families) are less likely to include laws governing the transfer of personal data to third countries, and sanctions are less likely to be present [11]. Thus, the communal culture of Indonesian people greatly affects concerns about privacy data, not only the general public but also regulators.

Justus M van der Kroef, in his article entitled "Collectivism In Indonesian Society," mentioned that Indonesia is a communal state, this can implicitly be concluded in Article 33 of the Constitution 45 that water, land and natural resources shall be organized cooperatively, and that those branches of economic life effecting most people shall be held in common[15]. To explain these tendencies by citing Indonesian leaders' fondness for traditional communal patterns in the inventive peasant society is to beg the question. The collectivist trend is a reaction to colonial capitalism, but it is also a reaction to the peculiar social structure of the time [15]. According to Made Suwitra, the communalistic Culture of the Indonesian nation departs from the noble values that developed from the philosophy that underlies the Indonesian nation, namely religious communalism, in the sense that the relationship between personal people and society always prioritizes the interests of society [16]. Indonesia as a collective country is also strengthened based on surveys. Survey data conducted by the Indonesian Survey Institute (LSI) on July 18-28, 2009 of 1,265 respondents spread across all provinces in Indonesia.[17] To measure the tendency of communalism-individualism of society, the survey put forward two dichotomous statements. Respondents were asked to provide a score on a scale of 1 to 10 against the two statements. And the results show that Indonesian society tends to be communal rather than individualism.

Based on the theory of Individualism versus Collectivism above, it can be said the theory is align with the facts that occur in the country of Indonesia which is a country with communal culture. About 196.71 million people in Indonesia had accessed the internet 73.7% of the total 270 million) (APJII Bulletin 2020) Based on research by the Indonesian Internet Service Users Association (APJII) in 2019 . However, based on the 2020 Indonesian Digital Literacy Status Research by Katadata Insight Center (KIC), the public's understanding of the importance of personal data confidentiality has not been high [1]. A total of 67.4% of internet users in Indonesia shared their date of birth, and 53.7% wrote down their phone number on social media. Meanwhile, a survey conducted by the Public Perception Survey on The Protection of Personal Data through Computer Aided Web Interviewing (CAWI) which aims to map public perception of the right to the protection of personal data in 34 provinces against internet users aged 17 years and over as many as 11,305 respondents revealed that as many as 28.7% of the public has experience of misuse of Indonesian personal data. Based on the survey, respondents assessed

banking products such as e-wallets and bank accounts are products that are considered vulnerable to data leakage. On the other hand, 22.9% of respondents believe that banking products and financial institutions have adequate data protection so that it is impossible to experience data leakage. A total of 12.1% of respondents had experienced a financial data leak. As a result of the data leak, the thing they experienced the most was a reduction in savings in bank accounts (44.1%), followed by reduced balances in e-wallets (32.2%). Other losses felt by respondents are such as making transfers or purchases because they are contacted by certain people or companies.

Here are the results of a survey that shows how Indonesians share their privacy data Personal Data that has been shared to the Public over as many as 11,305 respondents conducted by kdepartment of Communication and Informatics and Katadata Insight Center

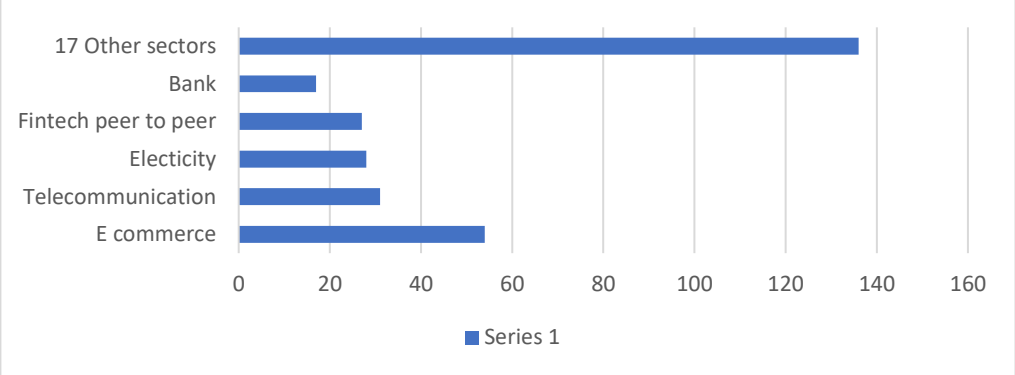
Table 1. Indonesian Personal Data Shared to Public

Data Name	Percentage amount	sum	Percentage of Regrets
Full Name	58,3%	5,586	31,7%
Gender	53,7%	6,070	11,2%
Mobile Number	48,2%	5,444	72,5%
Religion	45,7%	5,094	10,6%
Date of Birth	44,3%	5,007	30,4%
Email Address	38,2%	4,324	42,9%
Statehood	31,6%	3,575	8,5%
Home Address	30,0%	3,389	38,8%
Workplace	25,3%	2,863	26,4%
NIK	10,2%	1,353	60,8%
Diploma	4,8%	541	22,6%
TIN	2,9%	331	26,9%
Marriage Book	1,3%	147	27,2%
Sensitive Personal Data			
Location Data/GPS	16,4%	648	35,0%
Photos of <17-year-old family members	13,7%	693	44,6%
Opinions/views/political choices	13,1%	475	32,1%
Birth mother's name	10,0%	316	27,9%
Child data	6,8%	250	32,7%
Online purchase data	5,8%	223	34,3%
Website search data	4,2%	184	38,6%
Train/plane tickets	3,8%	92	21,2%
Sexual life/orientation	3,6%	130	31,7%
Biometry data	3,4%	129	33,2%
Health data / medical records	2,8%	80	25,6%
Financial/banking data	2,3%	116	44,1%
Crime record	0,8%	42	45,2%

Judging from the survey, Indonesian people have not been able to distinguish which data sensitive and non -sensitive data, whereas Categorization of personal and sensitive data, determined based on a country's discrimination, what is the source of the country's discrimination, that determines the list of sensitive data such as race, ethnicity, religion, validity data and others. [19].

Thus, according to the complaint data of the Indonesian Consumer Institute Foundation (YLKI) in 2019, there have been 96 complaints related to online loan persons. A total of 54 of them occurred in illegal online loans . The complaints include complaints related to high interest rates that are not in accordance with the rules, but also related to access to consumer data used to terrorize relatives during the debt collection process. In 2020, data leaks in the financial sector derived from fintech and banking were committed to approximately 18% of privacy data leaks from 22 sectors that were analyzed or the second most for data leakage cases of privacy data.

Table 2: Data leak by sectors, June 2020



Nowadays, Indonesia still does not have a personal data protection law. So it is still not able to determine how the form of independent agency supervisory commission, form of authority, whether plural, single or dual.

In the midst of lateness in responding to the urgency of the privacy data protection law due to an entrenched cultural background, the popularity of fintech in Indonesia is currently increasing rapidly amid the Covid-19 pandemic. Indonesia is the country that has the largest fintech and e-commerce market share in Southeast Asia, [20] Not only fintech, the Bank also began to transform its services by utilizing the advantages of digital technology such as forming a digital bank and implementing an open banking API. In 2020, the distribution of financial financing by fintech P2P lending has reached Rp128.7 trillion or an increase of 113 percent year-on-year [21]. The financial inclusion of developing countries was initiated in 2010 led by the G-20 and the World Bank to increase financial inclusion and reduce poverty levels in developing countries [22]. Like a double-edged sword, fintech and digital financial institutions are present for the purpose of accelerating exclusion, but on the other hand present crucial legal problems, including the danger of misuse of data privacy. Meanwhile, the Indonesian government in collaboration with relevant agencies for the past 7 years has been trying to draft personal self-protection that in the near future will be passed, considering that in ASEAN countries Indonesia is late to include in the establishment of the data privacy Law compared to

neighboring countries such as Malaysia, Thailand, Singapore etc [23]. To control the rate of privacy data leakage cases, Indonesia issued a regulation specifically for the protection of personal data that is contained in an electronic system, namely Ministry of Communication and Informatics (Ministry) Regulation No 20 of 2016 regarding the Protection of Personal Data in Electronic Systems.

The Ministry of Communication and Informatics is Indonesia's primary data protection regulator. In the event of a dispute, the Ministry may delegate authority to its Director General of Informatics Application, who will form a data privacy dispute resolution panel. This panel may recommend to the Ministry that administrative sanctions be imposed against the relevant Electronic system provider (ESP), though the dispute can also be resolved amicably or through any other alternative dispute resolution process between the ESP and the data owner. In the event of misuse of personal data or even a system provider company 'fails' in protecting the user's personal data, there are two legal steps that users can take. **First**, users can file a *complaint* with the Ministry of Communication and Information technology of the Republic of Indonesia ("Kominfo") on the basis that the provider of the electronic information system has failed to protect the user's personal data. In the context of legal efforts pursued is *a complaint,* then the element of loss generated in the case of a personal data breach that occurs does not need to be proven. As for the sanctions for violations of personal data protection provisions, stipulated in Article 36 Ministry of Communication and Informatics regulation 20/2016, namely in the form of verbal and written warning sanctions, temporary suspension of business activities and / or announced through online sites (online *websites*). It's just that if the user wants compensation, more precisely can take the **second** step, which is to file a lawsuit with the court.

In the financial services sector, regulations regarding privacy data on fintech are regulated by the Financial Services Authority specifically for peer-to-peer landing fitech and crowdfunding. The sanction of personal data violations in online loan services has been stated in the Financial Services Authority Regulation No. 77/POJK.01/2016 concerning Information Technology-Based Money Lending Services, which is affirmed in Article 26 that the organizer is responsible for maintaining the confidentiality, integrity and availability of users' personal data and in its use must obtain approval from the owner of personal data unless otherwise specified by the provisions of the laws and regulations. As for banking and fintech payments, supervision and regulation related to privacy data are within the authority of Bank Indonesia through Bank Indonesia Regulation No. 22/20/PBI/2020 concerning Bank Indonesia Consumer Protection, Forms of Handling Consumer complaints carried out by Bank Indonesia in the form of: education; consulting; and facilitation. Both regulations apply administrative sanctions, but for customers to be able to sue for damages can file a lawsuit with the district court. Actually, in Indonesia the regulation of privacy data is still spread in various rules and there is overlapping of regulations and authorities [24].

However, obstacles were also found in the litigation stage related to proof. Privacy data that is generally collected and transferred through electronic systems poses obstacles in law enforcement in court. Since Individualist societies' legal institutions frequently emphasize adversarial trial procedures in which individuals can file claims if their rights are violated. A communal purpose of law, on the other hand, is concerned with preserving harmony for the greater good. Individual rights are supplanted by the good of the community [25]. so that the justice system is inquisitorial (judges play an important role) in directing and deciding a case he handles. This system makes judges strict towards the rules of law, which are rigid and slow to adapt to changing circumstances.

In general, the regulation of civil procedure law, the provisions regarding electronic evidence as one of the valid evidence tools and can be used as a basis in court in principle have

not been specifically regulated, although its status as a means of evidence has been accommodated in various laws of a special nature both in the form of media and electronic information. Provisions regarding what legitimate evidence has been regulated in civil procedure law, Article 164 HIR/284 RBg and Article 1866 BW, have regulated imitatively regarding the evidence tools that can be used in the resolution of civil disputes to the Court and compiled sequentially starting from the evidence of letters, witness statements, disclaimers, confessions and oaths. Limiting valid evidence and can be used as evidence in the trial in the regulation, in practice makes the existence of electronic evidence as a means of evidence that can be used in the trial depends heavily on the judge's interpretation of the use of electronic evidence in the trial. In some cases there are judges who reject and exclude electronic evidence on the grounds that the civil event law in HIR and RBG has not accommodated electronic evidence as a valid evidence so that it can be used as a basis in the trial, one example is in the verdict in the divorce case examined in Jombang District Court with Number 81 / PDT.G / 2020 / PN.Jbg, which in its consideration rejects the electronic evidence submitted by the plaintiff, taking into account:

> ".....in civil evidentiary law the Judge is bound by valid evidence, which means that the Judge may only make decisions based on evidence using evidence that has been determined by the Law only."

Furthermore, based on these considerations, the Panel of Judges in the case excluded the electronic evidence submitted by the Plaintiff with the following interpretation:

> "Considering, that after the panel of Judges reviewed, researched, paid attention to electronic evidence tools connected with the renewal of national civil event law, has not been accommodated in the civil event law which, because civil event law does not regulate explicitly about the electronic evidence tool and the arrangement of electronic evidence that exists until now only in the material law level only, among others in the Electronic Information and Transaction Law so that from the electronic evidence tool P-8, P-9 submitted by plaintiff at trial must also be ruled out."

In addition to its arrangements in the regulation of event law as a condition for the use of electronic evidence in the trial, in practice, the use of electronic evidence at the trial as the basis for the panel of judges to determine whether or not a trial fact is true also depends on the material requirements of electronic evidence, for example related to the integrity and validity of electronic evidence as required in the law governing it. There are several cases where the Panel of Judges excludes electronic evidence submitted in civil trials, because the parties do not include experts who can assess the material requirements of the electronic evidence, for example in the case of child custody revocation (hadhanah) with case number 192 / Pdt.G / 2020 / PA. Bitg was examined at the Bitung Religious Court. Where in the case the Panel of judges has basically recognized in force the electronic evidence presented by the Plaintiff, with its consideration:

> "Considering that the evidence of P-1, P-2 and P-3 is a proof of photocopy of screenshots of Whatsapp conversations between Defendants and Plaintiffs dated October 21, 2017, and November 02, 2017 has been sealed sufficiently and has been matched in accordance with the original, according to the Assembly the evidence tool can be categorized as electronic evidence or electronic documents and qualify Formil as evidence".

Although it has been recognized formil regarding electronic evidence, the Panel of judges in the procession, then excludes the evidence presented by the Plaintiff with consideration, the absence of expert information from the Plaintiff that can explain the authentication and validity of the electronic evidence submitted by the Plaintiff. Therefore, as in consideration of the verdict mentioned:

> "Considering, that although formil evidence Watsapp Plaintiff in the form of P-1, P2 and P-3 can be accepted as a valid evidence in the face of the trial but materially must be validated, conformity, authenticity, integrity and availability which of course must be strengthened by expert testimony upfront of the trial in this case specializing in digital forensic experts to provide a belief to the Panel of Judges that a means of evidence of conversation. Whatsapp on social media meets the conditions of authentication and verification and can really be used as a means of evidence in the trial."

Based on the above cases, some of the obstacles that are still obstacles in the use of electronic evidence in civil trials both formal and materiel will basically boil down to the importance of special regulations governing how electronic evidence can be applied at trial, not only as a guideline for judges in examining electronic evidence but also as a clue for the parties who will talk at the trial. In addition, the existence of digital forensic experts is also needed at trials, coupled with the importance of training for judges to be able to assess the authentication and validity of electronic evidence. This is because the obligation of the judge to authenticate electronic evidence is based on the principle of ius curia novit. This principle is a principle that attaches the obligation to judges to play an active role in finding laws, developing laws, or forming new laws, if no written law or a law is not clear.

According to Sage and Woodlock, justice sector reforms are regarded as a failure because they fail to take into account the 'cultural characteristics' of the target countries, where multiple non-state and customary norms exist. [26]. The Recent studies have returned to the 'position that culture matters,' thereby initiating a new discourse, namely legal pluralism. According to this viewpoint, legal reform fails because donor agencies frequently fail to consider the diversity of legal orders that exist in the target countries. According to Kyed [27], donor agencies' approach to legal pluralism is "surrounded by ambiguity and ideological baggage." Customary laws are respected to the point where they do not conflict with Western legal principles. In order to address the problems encountered in the practice of legal pluralism projects, proposes the concept of a 'hybrid political order' to advocate the idea that 'justice and security institutions are not only plural, but continuously overlap, influence, and transform each other [27]. Her explanation of overlapping legal orders applies primarily to developing countries, and this feature is explained as a result of the nature of the state. Kyed's response to the question of why certain states are distinguished by the presence of multiple and overlapping legal systems remains unanswered [28].

4. Conclusion

The communalistic value of Indonesian society that grows and develops contributes on how Indonesian people behave towards data privacy. Not only the readiness of the Indonesian but also the regulators have not formed Data Protection Act so that they have not been able to determine the form of Independent supervisory commission, whether plural, single or dual which causes overlapping. So far in the financial sector there are 3 authorities that regulate privacy data, namely the Minister of Communication, The Financial Services Authority and Bank Indonesia who issued their own rules and are given the authority to investigate complaint

reports, monitoring, education, consultation , facilitation and provide administrative sanctions. Meanwhile, the indemnity lawsuit can lead to litigation, and litigation is still constrained related to proof and digital forensic experts to facilitate authentication and validity of electronic evidence

Acknowledgement

This paper was supported by Universitas Sebelas Maret (Research Grant 2021) Business Law and Digital Economy Group Research, Department of Civil Law Faculty of Law Universitas Sebelas Maret, Surakarta, Indonesia.

References

[1] Informatika DJA. National Survey, 2021, Persepsi Masyarakat Terhadap Perlindungan Data Pribadi. Jakarta: 2021.

[2] Li Y, Kobsa A, Knijnenburg BP, Carolyn Nguyen M-H. Cross-Cultural Privacy Prediction. Proc Priv Enhancing Technol 2017;2017:113–32. https://doi.org/10.1515/popets-2017-0019.

[3] Irianto S. Kajian sosio-legal. 2012.

[4] Otto JM. Some Introductory Remarks on Law, Governance and Development. Van Vollenhoven Institute, Faculty of Law, Leiden University; 2007.

[5] Abd. Asis , Andi Muhammad Sofyan ,Aswanto, Slamet S. THE INFLUENCE OF THE CULTURE OF LAW IN LAW ENFORCEMENT CRIMINAL ACTS IN THE FIELD OF FISHERIES. J Humanit 2015;3.

[6] Omrani N, Soulié N. Culture, privacy conception and privacy concern: evidence from europe before PRISM. 14th Int. Telecommun. Soc. Asia-Pacific Reg. Conf. "Mapping ICT into Transform. Next Inf. Soc., 2017.

[7] Eckhardt G. Culture's Consequences: Comparing Values, Behaviors, Institutions and Organisations Across Nations. Aust J Manag 2002;27. https://doi.org/10.1177/031289620202700105.

[8] Hofstede G. Dimensionalizing Cultures: The Hofstede Model in Context. Online Readings Psychol Cult 2011;2. https://doi.org/10.9707/2307-0919.1014.

[9] Trepte S, Reinecke L, Ellison NB, Quiring O, Yao MZ, Ziegele M. A Cross-Cultural Perspective on the Privacy Calculus. Soc Media Soc 2017;3. https://doi.org/10.1177/2056305116688035.

[10] Neuliep JW. Intercultural Communication: a contextual approach. Intercult. Commun. a Context. approach, 2015.

[11] Cockcroft S, Rekker S. The relationship between culture and information privacy policy. Electron Mark 2016;26:55–72. https://doi.org/10.1007/s12525-015-0195-9.

[12] Wang M, Rieger MO, Hens T. How time preferences differ: Evidence from 53 countries. J Econ Psychol 2016;52. https://doi.org/10.1016/j.joep.2015.12.001.

[13] Bellman S, Johnson EJ, Kobrin SJ, Lohse GL. International differences in information

privacy concerns: A global survey of consumers. Inf Soc 2004;20. https://doi.org/10.1080/01972240490507956.

[14] Milberg SJ, Burke SJ, Smith HJ, Kallman EA. Values, Personal Information Privacy, and Regulatory Approaches. Commun ACM 1995;38. https://doi.org/10.1145/219663.219683.

[15] van der Kroef JM. COLLECTIVISM IN INDONESIAN SOCIETY. Soc Res (New York) 1953;20.

[16] Suwitra IM. KONSEP KOMUNAL RELIGIUS SEBAGAI BAHAN UTAMA DALAM PEMBENTUKAN UUPA DAN DAMPAKNYA TERHADAP PENGUASAAN TANAH ADAT DI BALI. Perspektif 2010;15. https://doi.org/10.30742/perspektif.v15i2.51.

[17] Indonesian survey Institute. Communalism and Populism Indonesian Society. Jakarta: 2009.

[18] Buletin APJII. Survey Pengguna Internet APJII 2019-Q2 2020. Jakarta: 2020.

[19] European Union Agency for Fundamental Rights (FRA). BigData: Discrimination in data-supported decision making. FRA Focus 2018.

[20] Google, Temasek, Bain & Company. E-Conomy SEA 2021—Roaring 20s: the SEA Digital Decade. 2021.

[21] Asosiasi FinTech Indonesia. Indonesia Fintech Summit 2020. 2020.

[22] Ozili PK. Impact of digital finance on financial inclusion and stability. Borsa Istanbul Rev 2018;18:329–40. https://doi.org/10.1016/j.bir.2017.12.003.

[23] Rizal MS. Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. J Cakrawala Huk 2019;10. https://doi.org/10.26905/idjch.v10i2.3349.

[24] Satwiko BS. Privacy and Data Protection: Indonesian Legal Framework. Corp Trade Law Rev 2021.

[25] Zartner D. THE CULTURE OF LAW: UNDERSTANDING THE INFLUENCE OF LEGAL TRADITION ON TRANSITIONAL JUSTICE IN POST-CONFLICT SOCIETIES. IND INT'L COMP L REV 2012;22:303.

[26] Sage C, Woolcock M. Introduction: Legal pluralism and development policy-scholars and practitioners in dialogue. Leg Plur Dev Sch Pract Dialogue 2012. https://doi.org/10.1017/CBO9781139094597.002.

[27] Maria Kyed H. Introduction to the special issue: Legal pluralism and international development interventions. J Leg Plur Unoff Law 2011;43. https://doi.org/10.1080/07329113.2011.10756655.

[28] Mudhoffir AM, A'yun RQ. Doing business under the framework of disorder: illiberal legalism in Indonesia. Third World Q 2021;42. https://doi.org/10.1080/01436597.2021.1967738.