International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 8, Issue 12, 2019

The Urgency of Personal Data Protection Laws in Indonesia

Nynda Fatmawati[a], Tolib Effendi[b], Anissatul Ulfa[c], [a,c]Faculty of Law, Universitas Narotama, Surabaya, Indonesia, [b]Faculty of Law, Universitas Trunojoyo Madura, Bangkalan, Indonesia, Emaill: [a]ninda.fatmawati@narotama.ac.id, [b]te.effendi@trunojoyo.ac.id, [c]anisatululfa17@gmail.com

This research aims to observe the regulations of personal data protection in Indonesia and the urgency in establishing personal data protection laws. The research method used is a normative legal research method that reviews the laws and regulations in Indonesia. This will be applied in terms of Human Rights Act, ITE Law (Electronic Information and Transaction Law), Law on Population Administration, and Public Information Disclosure Act. The results show that personal data is each individual's unique data and the owners of such personal data will be harmed by irresponsible people who violate it. Protection of personal data has been mentioned in several laws. However, more detailed arrangements that contain sanctions for violation are still needed so that people have legal protection.

Key words: *Personal data, Urgency, Protection.*

Introduction

Data is an important entity for humans because it is related to an individual's life. Data can be categorized as information that is owned or will be owned by the data controller (England Data Protection Art 1988). In the current technological era, information becomes very valuable because it becomes a determining factor for economic development in both developing and developed countries (Dewi, 2009:53). In the past, individual's information or personal data was managed by the government and private sector manually. Today, personal data is managed by a computer-based system. Although the arrival of the computer age facilitates human work, it also creates a greater threat to the privacy of the individual. Severe damage may happen due to inaccuracy or information leakage (Marret, 2002:95). The digital age also allows personal data to be stored and transmitted on computers and mobile devices,

broadband and internet, and media sites (Shilling, 2011:1). In addition, the internet generates the presence of new crimes called cybercrime, among others (Suhariyanto, 2014: 14):

1. Computer data or information crimes.
2. Software Crimes of its operations interests.
4. Computer operations interfering actions.
5. Computer and its supporting tools damaging action.

Literature Review

Personal Data

First of all, the definition of personal data should be elaborated. Data is the plural form of datum, which is in Latin means "something given". Data is the basic material of information. It can be dictated as an organized group of symbols that represent actions, quantities, objects, and so on. Data is formed from various characters such as alphabet (letters), numbers, and other special symbols. Data is compiled then processed into a data structure, data base, and file structure (Purwanto, 2007:13-14).

As explained earlier that data is an important matter, it must be protected by the government. The term data protection itself was first used in Germany and Sweden in the 1970s, at which time the data was protected by law (Dewi, 2009:37). Data protection was carried out because computers were used as tool to store population data. At that time, there were many violations committed both by the government and private parties. A rule was established to protect personal data so that it would not be misused (Nugraha, 2018:19).

In Indonesia, information about individuals is called personal data. Each country uses different terms. Other countries might use the term personal information or personal data. However, those terms have almost the same meaning, therefore the two are often used interchangeably (Dewi, 2009:71). The United States, Canada, and Australia use the term “personal information” while the European Union and Indonesia, as stated in the Electronic Information and Transaction Law, use the term “personal data” (Nugraha, 2018:19).

Jerry Kang mentions that personal data describes information thoroughly related to an individual that distinguishes the characteristics of each individual (Kang, 1998:5). Basically, the form of data protection is divided into two categories: first, data protection in the form of physical data security for both visible and invisible data,(Dewi, 2009:7) and second, the existence of regulations governing the use of data by unauthorized persons, misuse of data for certain purposes, and destruction of the data itself (Nugraha, 2018:20).

The history of privacy protection itself starts from the protection of one's residence, which has grown to include the protection of information and communication through letter correspondence. The regulation of privacy rights protection was first applied in European countries and The United States. At that time, the law, on a limited basis, regulated the protection of having conversations inside the house without being afraid of eavesdropping. In addition, there was also protection for an individual to not engage in illegal activities (Djafar, 2015).

In the United States, privacy protection established with the legitimation of the Bill of Rights of the United States Constitution. The third amendment "places restrictions on the quartering of soldiers in private homes". The fourth amendment, "Prohibits unreasonable searches and seizures and sets out requirements for search warrants based on probable cause." The search and seizure are required to obtain approval from the Court through a search warrant, supported by sufficient preliminary evidence. And the fifth amendment "protects the right to due process, and prohibits self-incrimination" (Anggara, 2015:3).

In Indonesia, the modern history on privacy started from Dutch colonial era. Decree of the King of the Netherlands No. 36 issued on July 25, 1893, could be considered the oldest regulation regarding the protection of communication privacy in Indonesia. Since October 15, 1915 through Koninklijk Besluit No. 33 (Stbl.1915 No.732), privacy protection arrangements have been written in the Criminal Code. Although the regulation of the privacy right protection has been long enough in Indonesia, the protection of the privacy right has only become a constitutional protection by the enactment of the Second Amendment of the 1945 Constitution through Article 28 G paragraph (1) and Article 28 H paragraph (4). However, rules on the privacy right protection still contribute citizens' weak protection from violation of their privacy right.

European countries, for example, have had regulations on protecting personal data for more than a decade. There are several examples of developed countries that already have comprehensive arrangements related to personal data protection. The United Kingdom regulates the protection of personal data in the Data Protection Act 1998, which came into force in 2000. This Act is a substitute of previous regulations (Data Protection Act 1984). The Data Protection Commissioner whose job is to oversee all data users who control personal data was established. Protection of individual privacy rights is evidenced in the provisions of Data Protection Act 1998, which allows data subjects to obtain information on the processing of their personal data to prevent processing mistreatment that potentially endanger their interests. Data can only be used as long as necessary and may not be stored longer than is necessary for certain purposes. The protection of personal data is quite strong

because Data Protection Act prohibits personal data to be transferred to other countries unless the guarantee is provided (Latumahina, 2014:18).

Some important principles based on Part 1 of Data Protection Act 1998 are as follows:

1. *Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes*.
2. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
3. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*
4. *Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
5. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data*.

Malaysia regulates the protection of personal data in Personal Data Protection Act (PDPA) 2010, while Singapore regulates it in Personal Data Protection Act (PDPA) 2012. Malaysia's PDPA 2010 is applied started from August 2013, while Singapore's 2012 PDPA started from July 2014. The two regulations drawn up by Malaysia and Singapore have many similarities because they have the same source. Both of these rules are sourced from rules on personal data protection held in European Data Protective Directive. An interesting difference from the PDPA 2012 owned by Singapore is that it facilitates the establishment of a body called Do Not Call (DNC) Registry. The public can register their telephone number with DNC Registry and formally refuse to receive calls or messages such as SMS and MMS from marketing or organizations they don't want (Latumahina, 2014:19)

In Part II of Personal Data Protection Act 2010 contains seven legal principles for each data user, as described as follows: "*The Malaysian PDPA requires users of data to comply with a number of principles, the General Principle, the justification for the processing, such as consent; the Notice and Choice Principle, the right to be informed about the purposes for the processing; the Disclosure Principle, no disclosure except in connection with the purpose; the Security Principle, the obligation to take practical steps to protect data; Retention Principle, not to keep the data for longer than necessary; Data Integrity Principle, ensure that data is accurate and up to date; and the Access Principle, an individual's right to have access to his or her data.*"

These seven principles have comprehensively regulated the protection of personal data. In the Retention Principle, for example, personal data that is processed for any purpose must not be stored longer than is necessary as they aim to fulfil the protection of personal data. In this case, it will be the duty of the data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted. With PDPA 2010, security guarantees for personal data of internet users in Malaysia have also increased. Other countries have realized the importance of protecting personal data. Now is the time for Indonesia to realize the importance of protecting personal data.

Research Methods

The research method used is the normative method, which examines laws that have been conceptualized as norms or rules that have been applied in society. This normative method examines library materials or secondary data. Therefore, this study reviews the Human Rights Act, the ITE Law (Electronic Information and Transaction Law), the Law on Population Administration, and Public Information Disclosure Act.

Result and Discussion

Indonesia is not a state based on power (machstaat) but a state of law (rechstaat). Thus, the order should be written in the Government Regulations, Ministerial Regulations, Laws and so forth. This regulation must contain sanctions for violators. The implementation of law and power must not leave the social values of society. This means that it should not obstruct the development of society, and the norms are made by the community based on mutual agreement (Budiyanto, 2002:17). One of the developments is the participation in the use of technology, such as browsing or sharing information or using social media. Social media has become free communication media in society, but social media requires its users to input their personal data before accessing. This causes anxiety.

Personal information (personal data) of internet users which is easily accessed and spread by irresponsible parties, becomes the flaw of submitting personal data. In other words, personal data is vulnerable to piracy in cyberspace. This piracy is classified as a cybercrime. The term “piracy” is only used to describe various types of illegal sharing activities, illegal downloading, and falsification of data. Generally, Andi Hamzah described cybercrime as an illegal crime in the computer field (Hamzah, 1987:18)

Personal data leakage cases are often mentioned in the discussion of personal data. In 2018, more than 1 billion social media users were involved in the Cambridge Analytica scandal. At that time, more than 80 million Facebook users’ personal data was leaked to other parties. Furthermore, in the same year, large companies such as Twitter and Google also experienced

personal data leakage. It is estimated that more than 1 billion users are affected by data leakage. Google experienced a leak of personal data of about 500,000 Google+ accounts to other parties. While 330 million Twitter user's data was leaked. The online taxi company, Uber has also experienced a similar issue. It was recorded 57 million users' personal information was leaked. The data is the name and telephone number information of 50 million passengers and 7 million Uber drivers worldwide (Pratomo, 2018)

Another case of personal data misuse is related to online loans or financial technology (fintech). A resident of East Jakarta reported one of the companies engaged in the field of fintech or online loans to Jakarta Police because his personal data was being disseminated. In addition, he also reported alleged defamation (Wildansyah). In a recent case, the Twitter account @Hendralm revealed the existence of data trading practices such as Custom Identification Numbers (NIK/*Nomor Induk Kependudukan*), family cards, and selfies when holding an Indonesian Identity Card (KTP/KArtu Tanda Penduduk). This data is 'sucked up' through various channels that offer fast loans. This data trading site is carried out on various social media such as Instagram and Facebook. These people deliberately use other people's data to register loans online to the peer-to-peer lending platform or pay later features provided by big e-commerce. As a result, the original identity card owner becomes the victim (Aldila).

The disclosure of the sale and purchase of NIK data has caused unrest among the people. The guarantee of the protection of personal data has been echoed in the international community. On June 28, 2019, world leaders adopted the Osaka Track on digital governance rules with the concept of "*Data Free Flow with Trust*". The declaration was adopted by 24 signatories, including Argentina, Australia, Brazil, Canada, China, European Union, France, Germany, Italy, Japan, Mexico, Republic of Korea, Russian Federation, Saudi Arabia, Turkey, United Kingdom, United States, Spain, Chile, Netherlands, Senegal, Singapore, Thailand , and Vietnam (Osaka Track, 2019), at the Group of 20 Leaders' Summit. The three main issues in the G-20 Summit are (Abe):

1. Building s strong, free, fair and mutual-beneficial international trade order.
2. Maintaining and strengthening the free and fair international trade order.
3. Digitalization of the economy to enable unique and unprecedented business model.
4. Innovative ideas to address global environmental challenges by creating an intergovernmental panel on Climate Change "Global Warming 1.5C'.

Under the Osaka Declaration, the leaders vowed, among other things, their commitment to international rule-making on trade-related aspects of e-commerce at the World Trade Organization (WTO). India did not take part in the session, while Egypt, Indonesia, and South Africa abstained. The core of this notion, first raised by Japanese Prime Minister

Shinzo Abe at the World Economic Forum in January, is that "trust" can be guaranteed only with suitable protections for personal information and intellectual property (Sim, 2019). India, South Africa, and Indonesia chose not to sign Osaka Track declaration because the agreement could damage the core principles of the WTO (Kanth, 2019). The important agreements to be achieved in Osaka track were (Osaka Track, 2019):

1. The importance of promoting national and international policies in a discussion setting to maximize the digital data and economy capability.
2. The importance of innovation continuation in the development of digital data and economy.
3. Counterbalancing the rapidly growing digital economic growth as the proof of G20 member countries' commitment to promote international policy. This is carried out in the international trade regulations discussion forums.
4. Electronic commerce in WTO is very useful in the era of digitalization and technology.
5. The member countries work together to build and commit in making agreements with high standards and invite the utmost participation of WTO members.

Indonesia, as one of the countries that did not sign the Osaka Track Agreement, may lose the opportunity to maximize the data potential and digital economy. It also lost the opportunity to develop the International digital economy.

The most important element of personal data protection is the personal data itself. This personal data is very unique because each person has a different personal data, among other things, Custom Identification Number (NIK). This number has become important since the enactment of NIK in Law Number 24 of 2013 on Amendment to 23 of 2006 concerning Law on Population Administration (Aminduk Law). NIK consists of unique 16 digits, every person has different number series, one and only, and attached to someone for life. The number will also not change when the person moves his/her domicile to another place. The unity of NIK is maintained through a biometric identification system, fingerprints, iris and face recognition in the Electronic ID Card Implementation program. NIK is given to everyone when registered as a resident of Indonesia, and this NIK cannot be changed; it sticks to the end of one's life. Thus, the data is very important to be protected because if misused, the affected person will be the owner of the NIK, even though the owner did not commit a crime.

NIK was first introduced by Directorate General of Population and Civil Registration in the implementation of a computerized national Indonesian Identity Card (KTP) system. NIK was first nationally used in 2011 and has been managed through a population administration information system. This system becomes a population database which is then updated

through the population registration and civil registration services at the Population and Civil Registry Office, subdistrict and Village. The application of NIK is regulated in PP No. 37 of 2007 on the Implementation of Law Number 23 of 2006 concerning Population Administration, article 37 states that the NIK consists of 16 (sixteen) digits and its constituent code; the first 6 (six) digits are the province, regency / city and sub district, the second 6 digits are the date, month and year of birth and the last 4 (four) digits are the serial number of the issuance of NIK which is automatically processed by SIAK and placed in a horizontal position.

The misuse of personal data is not only related to buying and selling NIK. In the banking sector, Bank Indonesia has issued Bank Indonesia Regulation Number 7/6/PBI/2005 Concerning Transparency in Bank Product Information And Use Of Customer Personal Data to prevent the violation of personal data. In this provision, Banks are required to protect customers' personal data. If used for commercial purposes, it must be done transparently and have written approval from the customer. The personal data includes:

a. Address;
b. Date of birth and or age;
c. Phone number;
d. Biological mother's name; and
e. Other information which is a personal identity and is commonly given by the Customer to the Bank in the utilization of Bank Products.

The misuse of personal data that violates customers in banking world is the leakage data information of credit card customers. The contract contains a standard clause that states consumers authorize the Bank to use customer data both for themselves and for other interests. Thereby, it encourages the case of buying and selling personal data of customers by the Bank. In this case, the consumer has no choice but to agree to the clause. Another violation is the customer's personal data that is traded at an outsourcing company hired by a credit card issuing bank. The data is used to fill out credit card submission forms. It is therefore not surprising that letters containing credit card applications and its credit cards are suddenly sent to the customers' houses, when they in fact never applied for those cards (Dewi, 2011:210).

Victims of personal data violation can sue civilly based on Law Number 18 of 2008 on ITE and Government regulation Number 28 of 2012 on PSTE. Unfortunately, this civil litigation is limited only to compensation demand of e-commerce providers who abuse personal data. Whereas the violation of privacy data is broader and not limited to the civil law. Therefore, more specific legal regulations which contain stronger legal remedies are needed (Indriyani, 2017:207).

Regulation of the Minister of Communication and Information Technology Number 12 of 2016 on Telecommunications Services Customer Registration (Permenkominfo RPJT) sets restrictions on 3 prepaid cards for one family card and KTP. The results of this regulation cause people difficulty in accessing information using the internet with a package card. Thus the enactment of this rule is contrary to Article 28 F of The 1945 Constitution of the Republic of Indonesia states that: "*Every person shall have the right to communicate and to obtain information for the purpose of the development of his/her self and social environment, and shall have the right to seek, obtain, possess, store, process and convey information by employing all available types of channels*". Moreover, the stronger rules governing registered prepaid cards haven't been established, so it is hard to protect the human rights especially data privacy. This raises public concern over the misuse of personal data through registration using KK and KTP (Hadita, 2018:193-202)

The violation of personal data also occurs in the aviation business. In general, the processing of personal data is extraterritorial. The threat of terrorism triggers many countries to take extra measures, which among others by storing personal data of passengers. This aims to protect the country from the threat of terrorism. In Germany, the government implemented a policy to store personal data of foreign citizens (non-German), both EU citizens and non-residents, who settled for more than three months. The data is used for various purposes, ranging from statistical matters to as an effort to reduce crime rates. However, this policy only applies to foreigners and does not apply to German citizens. This made Huber take this matter to the German court which was then forwarded to the Court of Justice of the European Union (CJEU). Huber is an Austrian who has lived in Germany for more than three months. He claims that the process of personal data contained in Germany is not in accordance with the principle of non-discrimination and fundamental values that live in European Union society. This case ended with the CJEU ruling stating that processing personal data violated the principle of non-discrimination. The status of a German citizen is not a justification for differentiating other EU citizens. This applies to processing personal data (European Commission Legal Service, 2018).

The Huber case is very likely to be repeated in the name of aviation security both for commercial purposes and flight security. The Passengers Name Record polemic between the European Union and the United States has created a new era regarding the protection of aircraft passenger privacy. However, these arrangements are returned to the jurisdiction of each country. This is because there are no universal laws such as binding international law (Nugraha, 2018:73).

Threats against the violation of personal data also threaten Indonesia, which is increasingly in an uproar with the introduction of an electronic Indonesian Identity Card (e-KTP) program,

where the government records the personal data of all Indonesian citizens. Indonesian citizens are required to do the recording in each of their domiciles. This becomes controversial because the possibility of data leakage. It is also likely to be misused by irresponsible parties, especially if it is lacking in security (Latumahima, 2014:2)

In the end, the problem of data transfer will lead to a dispute between the original owner of the personal data with the company that also claims ownership of the personal data. In the perspective of data subjects, the personal data is an individual right and the ownership remains attached to the subjects of each individual. On the other hand, the company will probably claim the ownership of a person's personal data based on the exchange of services this person enjoyed so far. In addition, they can also argue that one data has no financial value, so it does not harm anyone. New data will be valuable if analysed with other people's data, which becomes big data. Thus the company should have such data, both in raw or processed (Anggraeni, 2018:823-824)

In reality, the company claims to be the owner of personal data. Moreover, they also trade personal data without the relevant consent. This practice can only be stopped with reports from affected users. The concrete steps from the government should also be taken by providing legislation similar to "Do Not Call Registry" provisions applicable in Singapore. This is the right time for the government to establish the applicable regulations. It can be started by using The *EU General Data Protection Regulation* (*GDPR*) as a reference in drafting regulations. Because the provisions explicitly state that legal subjects are entitled and free to determine how their data is processed by the company (Anggraeni, 2018:824)
The company claims to be the owner of personal data. Several reasons to highlight the importance to protect personal data because its relation to privacy rights (Dewi, 2011:208)

1. Every person has a personal life that cannot be shared with others, in order to maintain his position at a certain level.
2. Everyone needs alone time (solitude) so privacy is needed (Randall, 1992:25).

3. Privacy is an independent right and this right will be gone if the owner publishes that private matters to the public.

4. The privacy right also includes the right to be in a marriage; other people should not involve in such personal relationship. Warren mentioned this as the right against the word.

In addition, privacy rights must be protected because if not, the owner will suffer significant losses. Such loss is greater than the physical loss, because the personal life has been disturbed. So, if there is a loss, the victim is entitled to compensation (Griswold, 1960:12).

Identity Protection in Indonesia

Several regulations standardize identity protection in Indonesia, including Law Number 24 of 2013 on Amendment to Law Number 23 of 2006 concerning Population Administration; Law Number 14 of 2008 on Public Disclosure Act; Law Number 39 Year 1999 concerning Human Rights and Law Number 19 Year 2016 concerning Amendments to Law Number 11 of 2008 on Electronic Information and Transactions. The mentioned laws can be seen in the table as follows:

Table 1: Identity Protection Regulations in Indonesia

No	Regulations	Articles	Contents	Explanation
1.	Law no. 24 of 2013 on Population Administration	84 (1)	(1) Personal data that must be protected contains: *a. Information on physical and / or mental disabilities;* *b. Fingerprint;* *c. Eye iris;* *d. Signature; and* *e. Other data elements constituting the flaws of a person.*	Article 84 Paragraph (1) mentions several protected matters which are only related to population data. In fact, face should also be protected, because each person has this specification. In addition, the protection in this regulation doesn't discuss social media which has higher probability of personal data violation.
		85	*(1) Personal Data of Residents as referred to Article 84 must be stored and protected by the state* *(2) Further provisions regarding the safekeeping and protection of Personal Data of Residents as referred to in paragraph (1) shall be regulated in a Government Regulation.*	

			(3) Personal Data of Residents as referred to paragraph (1) must be truthfully and confidentially protected by the Organizing and Implementing Institutions in accordance with the provisions of the Laws and Regulations.	
2.	Act No 14 of 2008 on Public Disclosure Act	17	Every Public Agency is obliged to open the access to obtain Public Information for every Public Information Applicant, except: *a. Public Information that if opened up and supplied to the Public Information Applicant could obstruct the process of law enforcement, such as information that could:* *1. obstruct the investigation and inquiry process of a criminal act;* *2. disclose the identity of the informant, reporter, witness and/or the victim who knows of the criminal act;* *3. disclose the intelligent data of the criminal and the plans to prevent and to handle any form of*	This law only covers some specific fields and has not reached broader interest of society.

			transnational crime; *4. jeopardize the life and the safety of the law enforcement officer and/or his/her family; and/or* *5. jeopardize the safety of the equipment, facilities and/or the infrastructure of the law enforcement officer.*	
3.	Law No. 39 of 1999 on Human Rights	29	*Everyone has the right to protection of the individual, his family, opinion, honour, dignity, and rights.*	
4.	Law No. 19 of 2016 on Amendments to Electronic Information and Transactions Law	26	*Unless provided otherwise by Rules, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned.*	

Fundamentally, the protection of personal data is regulated in Article 26 of ITE Law. In addition, Bank Indonesia Regulation No 7/6 / PBI / 2005 authorizes Bank Indonesia to set technical standards regarding the protection of personal data of customers, especially for the credit card industry. However, the two regulations have not been implemented optimally, because (Dewi, 2011:211):

1. ITE Law, as it is implied by the name, only applies to the misuse of personal data through an electronic system only.
2. The contents of Bank Indonesia Regulations are quite good, but the scope is too narrow. It doesn't examine the violations committed by non-bank companies.

Personal data consists of not only names and identities (such as NIK and others), but also people's faces. There have been recent cases which involves journalism. Technological advances have encouraged journalists to report news on social media. Social media enable people accessing the news easily and efficiently because of the easiness principle. In fact, Indonesian Broadcasting Commission Regulations standardizes journalists' codes of ethics. Although the enactment of this rule is not clearly explained, professional journalists should still obey the rules, whether in conventional media (such as television) or on social media. Stating the source of the disseminated information on social media, as well as check the personal rights of objects in photographs or videos to not violate human rights are the obligations of journalists (Fatmawati, 2019:54).

The concept of privacy data protection applied in Indonesia is cloud computing. It is employed with the concept of merging or hybrid by amalgamating legal approach and non-legal approach which is called the market mechanism approach (Dewi, 2016:29)

Conclusion

Public anxiety over the protection of personal data in Indonesia has developed due to the absence of definite rules to shield such data. Meanwhile, cases related to personal data violations have emerged in various sectors, among others, on social media, banking sector, financial technology, aviation sector and many more. The International Organization establishes the regulation with the implementation of Osaka Track. The agreement was born to overcome the anxiety of countries in the world due to the impact of using borderless internet. In Indonesia, there are no rules that generally can reach all layers of problems, so new regulations are needed.

REFERENCES

Abe, Shinzo. *Goals for the Group of 20 summit in Osaka*. Retrieved from https://www.japantimes.co.jp/opinion/2019/06/24/commentary/japan-commentary/goals-group-20-summit-osaka/#.XblrttIzbIU

Aldila, Nindya., *Bandar Data Ilegal Bobol Fintech Lending*, Retrieved September 2019 from https://finansial.bisnis.com.

Anggara and Eddyono, Supriyadi Widodo and Djafar, Wahyudi, and Rentjoko, Antyo.(2015). *Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia*. Jakarta: Institute for Criminal Justice Reform. Retrieved from https://icjr.or.id/menyeimbangkan-hak-tantangan-perlindungan-privasi-dan-menjamin-akses-keterbukaan-informasi-dan-data-di-indonesia/

Anggraeni, Setyawati Fitri. (2018). *Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia*. Jurnal Hukum & Pembangunan, 48(4), 823-834. Retrieved from http://jhp.ui.ac.id/index.php/home/article/view/1804

Budiyanto.(2002). *Pendidikan Kewarganegaraan.* Jakarta:Penerbit Erlangga.

Dewi, Shinta. (2009). *Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjajaran.

Dewi, Shinta. (2011, November). *Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya*. Sosiohumaniora, 19(3), 208-2011. Retrieved from http://jurnal.unpad.ac.id/sosiohumaniora/article/view/11380

Dewi, Sinta. (2016, January-April). *Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia*. Yustisia, 5(1), 29. Retrieved from https://jurnal.uns.ac.id/yustisia/article/view/8712

Dinas Kependudukan dan Catatan Sipil Ponorogo., *Tau Nggak Nik itu apa.* Retrieved September 2019 Retrieved from https://dukcapil.ponorogo.go.id/1384-2/

Djafar, Wahyudi. (2015). *Memastikan Perlindungan Hak atas Privasi di Era Digital.*

European Commission Legal Service. C-524/06 *Huber v. Federal Republic of Germany*. Retrieved September 2019 from http://curia.europa.eu/juris/document/document.jsf?docid=76077&doclang=EN

Fatmawati, Nynda and Ulfa,Anisatul. (2019, June). *Aspek Hukum Jurnalistik Tentang Penayangan Video Yang Viral Di Media Sosial*. Celebes Cyber Crime Journal, 1(1), 54. Retrieved from http://journal.lldikti9.id/cybercrime/article/view/102

Griswold, E. (1960). *The Right to be Let Alone*, North Western University Law Review.(12). 55.

Hadita,Cynthia. (2018, December). *Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia*. Jurnal HAM, 9(2), 193-202. Retrieved from https://ejournal.balitbangham.go.id/index.php/ham/article/view/523

Hamzah, Andi. (1987). *Aspek-aspek Pidana di Bidang Komputer*. Cet. I. Jakarta: Sinar Grafika.

Indriyani, Masitoh, and Sari, Nilam Andaria Kusuma and W.P, Satria Unggul. (2017, Oktober). *Perlindungan Privasi Dan Data Pribadi Konsumen Daring Pada Online Marketplace System.*Justitia Jurnal Hukum, 1(2), 207. Retrieved from http://journal.um-surabaya.ac.id/index.php/Justitia/article/view/1152

Kang,Jerry. (1998, April). *Information Privacy in Cyberspace Transaction*. Stanford Law Review, 50, 5. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=631723

Kanth, D. Ravi. *India boycotts 'Osaka Track' at G20 summit*. Retrieved from https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html.

Latumahina, Rosalinda Elsina. (2014, December). *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. Jurnal Gema Aktualita, 3(2), 18. Retrieved from http://dspace.uphsurabaya.ac.id:8080/xmlui/bitstream/handle/123456789/92/Aspek%20Hukum%20Perlindungan%20Data%20Pribadi%20di%20Dunia%20Maya.pdf?sequence=1&isAllowed=y

Marrett, Paul. (2002). *Information Law in Practice: 2nd Edition*. Cornwall: MPG Books Ltd.

Nugraha, Radian Adi. *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-undang Informasi Dan Transaksi Elektronik*.Jakarta. Retrieved from http://webcache.googleusercontent.com/search?q=cache:aitI-xgPw8YJ:lib.ui.ac.id/file%3Ffile%3Ddigital/20336476-Radian%2520Adi%2520_Perlindungan%2520Data%2520Pribadi%2520Cloud%2520Computing_Universitas%2520Indonesia_2012.pdf+&cd=1&hl=id&ct=clnk&gl=id

Nugraha, Ridha Aditya. (2018, June). *Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era Big Data. Mimbar Hukum,* 30(2), 19-73. Retrieved from https://jurnal.ugm.ac.id/jmh/article/view/30855

Osaka Track, Retrieved from pada https://www.g20.org/pdf/special_event/en/special_event_01.pdf.

Osaka Track on digital rules launched at G-20 summit, retrieved September 2019 Retrieved from https://www.straitstimes.com/asia/east-asia/osaka-track-on-digital-rules-launched.

Pratomo, Yudha. (2018) *Lebih dari 1 Miliar Data "Netizen" Bocor pada 2018*, kompas. Retrieved from https://tekno.kompas.com/read/2019/01/07/19310087/lebih-dari-1-miliar-data-netizen-bocor-pada-2018.

Purwanto. (2007). *Penelitian Tentang Perlindungan Hukum Data Digital.* Jakarta: Badan Pembinaan Hukum Nasional.

Randall, B.P. (1992). *The Right to Privacy Revisited: Privacy, News and Social Change.* California Law Review, 80(5), 25. Retrieved from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1764&context=californialawreview

Shilling, Cameron G. (2011). *Privacy and Data Security: New Challenges of The Digital Age*. New Hampshire Bar Journal.

Sim Walter. *Osaka Track on digital rules launched at G-20 summit*, Retrieved from https://www.straitstimes.com/asia/east-asia/osaka-track-on-digital-rules-launched

Suhariyanto, Budi. (2014). *Tindak Pidana Teknologi Informasi* (*Cybercrime*) *: Urgensi Pengaturan dan Celah Hukumnya*, Jakarta: PT RajaGrafindo Persada.

United Kingdom Data Protection Act 1998. Retrieved September 2019 Retrieved from http://webcache.googleusercontent.com/search?q=cache:4rR1tk7Q-FEJ:www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf+&cd=14&hl=id&ct=clnk&gl=id

Wildansyah, Samsudhuha. *Data Pribadi Disebar hingga Diancam*, *Nasabah Fintech Lapor Polisi*. Retrieved September 2019 Retrieved from https://news.detik.com/berita/d-4650403/data-pribadi-disebar-hingga-diancam-nasabah-fintech-lapor-polisi.

Biographies

Nynda Fatmawati Octarina, Faculty of Law, Narotama University, Surabaya, Indonesia
ninda.fatmawati@narotama.ac.id
A Lecturer and Head of Quality Assurance in the Faculty of Law at Universitas Narotama, Surabaya, Indonesia. She earned her a Bachelor's Degree from Faculty of Law at Universitas Narotama, Surabaya, Indonesia, and then continued her studies and obtained a Master Degree and a Doctoral Degree in Law from Universitas Airlangga, Surabaya, Indonesia. She is Active in publishing books and writing academic papers. Her research interest is in Cyber Law, especially Cyber Law Regulation establishment in Indonesia since 2008.

Tolib Effendi, Faculty of Law, University Trunojoyo Madura, Indonesia.
te.effendi@trunojoyo.ac.id
Senior Lecture in the Faculty of Law University Trunojoyo Madura, Bangkalan, Indonesia. He is former Head of Department of Criminal Science, former Vice Dean of academic at Faculty of Law University Trunojoyo Madura, Indonesia. Now he is Head of Quality Assurance at University of Trunojoyo Madura, Indonesia. He is graduated from Faculty of Law University of Brawijaya, Malang Indonesia and earned his Masters Degree from University of Padjadjaran, Bandung Indonesia. He has published some books and papers journal especially in Criminal Justice System and Criminology.

Anissatul Ulfa, Faculty of Law,Universitas Narotama, Surabaya, Indonesia
anisatululfa17@gmail.com
Obtained her Bachelor Degree from the Faculty of Law at Universitas Narotama, Surabaya, Indonesia. Interested in researching Cyber Law and has participated in many researches on the mentioned subject. She has big curiosity to learn the application of Cyber Law in society.