International Journal of Academic Multidisciplinary Research (IJAMR)
ISSN: 2643-9670
Vol. 3 Issue 9, September – 2019, Pages: 30-34

You Can Get Me: The Urgency of Personal Data Protection in the Era of Financial Technology

Ellectrananda Anugerah Ash-shidiqqi,SH,MH

ellectra_aa@yahoo.co.id

Abstract: *Constitution plan on the Protection of Personal Data became one of the constitution plan that has not been a priority and this is a crucial issue, considering that the existing technology penetration in Indonesia is quite massive. The existence of a Ministerial Regulation on the Protection of Personal Data also only covers administrative sanctions, not including criminal sanctions for perpetrators of theft and misuse of data. In this research, the comparison of countries that already have a Personal Data Protection Act for their people and the causes for the Indonesian country to take a long time to implement this personal data protection was discussed. Besides,the things needs to be prepared in the process of educating the community in responding to the Personal Data Protection Act was also discussed in this research.*

Keywords: Personal Data, Citizenship Administration

I. Introduction

Currently, people cannot get far from the internet. The development of the internet is not only about the issue of globalization, but also becomes a separate discourse to facilitate long-distance life. Internet usage in this century is almost 3 trillion in the world based on Freedom House in 2017. The internet is also used not only as my communication tool. Many sectors have been influenced by the internet, such as education, economics, and politics.

As the internet usage is very massive in the world, some parties also want to take over the internet. Since DARPAnet opened its DNS server to the US Government, the community felt it was unfair since the access to information was limited by the government. Many technological wars in the face of globalization, especially the western bloc and the eastern bloc are fighting for the technological dominance, including cyberspace. There is a lot of the role of the internet in it as the influence of social change in the real world, such as recently, Cambridge Analytica which revealed that Facebook's platform has used its big data to influence Donald Trump's victory in the 2017 elections.

To make the internet live, a vein is needed that connects with the internet to store everything contained on the internet, data. Data is information, which is in a form that can be stored and used (Longman Dictionary English, 2017). These information are processed systematically to be able to take policy. When visiting to a doctor, the doctor asked the kinds of diseases and complaints that we felt. The doctor began to record and make it systematic until finally, the doctor made a policy with inspection measures, for example, mentioning complaints to doctors and doctors record them, it is a data process and unconsciously done, we often provide data to others. This is similar to the data on the internet, often we directly provide data on the internet through social media or job recruitment applications such as linkedin, Job Street and others. The conscious process is dedicated to certain goals similar as giving our information to doctors to get well soon, we are not attached to getting access to the data on the internet for public purposes such as transparency of reports, or facilitating access to the recipients of work. Unconsciously, our trust in storing data on the internet is ignored or query to the direction of our data is taken.

Is data important to protect? We often do not realize that we leave our traces through data. When we are browsing, we accidentally send cookies to the owner of the site visited. when we use social media, update the status there. Well, actually this action is included in deliberate actions since we already know the function of using social media. However, it will be accidental to send it publicly with the intention to be shared with friends or yourself. One time, without your knowledge, these data have been recorded and ready to be used for other parties, such as e-commerce platforms that sell their merchandise on our homepage, or other offers every time we visit a site in the browser.

Data is a gold mine for them. Our interactions are changed in an algorithm, computer calculation applications that can calculate and make structures to be processed into various expressive levels of a person's needs, behavior patterns, interests and preferences for something. When you get new friends with mutual friends from one platform, in fact you have recorded your interests and likes based on the same person. Therefore, it is a mistake if you say that your friends on social media are new people, in fact you are processed to form a room called the echo chamber to build your own comfort space, for you and your social media friends. The platform will continue to process and record your data so that it makes you attractive and when third parties offer benefits for the data owner, social media platform, with a friendly platform to consider and confirm to give this post-modern era, we cannot escape to submit data. Everyday, we definitely use any service, apply for a job by submitting our NIK, buying products online or e-commerce, registering e-mail, paying for tickets, electricity tokens, credit and others that must show the account code to cellphone number, etc. with full awareness. Since 1960, as the capabilities of improving information technology, companies and governments have stored personal data in

their databases. The database can be searched, edited, crossed data, and shared with other companies and countries around the world (Privacy International, 2018: 9). Of course, protecting data becomes very important and it is our right as citizens who have the right to obtain information to develop their personal and social environment.

Regulation regarding data protection in Indonesia is still in the form of design or plan. As of October 2018, the DPR considers the Personal Data Protection Plan in PROLEGNAS 2018. The Data Protection Plan specifies the definition of personal data as data about a person both identified and/ or can be identified separately or combined with other information directly or indirectly through electronic and/ or electronic systems (Personal Data Protection Plan Article 1, Updated on October 2018 or you can download it here). We can also see the specific purpose of personal data through other articles which mention the following as personal data, namely: Religion/ belief; health data; biometric data; genetic data; sexual life; political views; crime record; child data; financial data; information about physical and/ or mental disability; and/ or other data in accordance with the provisions of the Law (Personal Data Protection Plan Article 6 Paragraph (3), Update October 2018). Thus, the government regulates all personally identifiable data for all systems, both electronic and manual.

Regarding this law, it is considered ironic to see the reality that currently happening. The number of data that is centrally not systematic and ends politically, one of which is the Population Registration Number (NIK) in the Identity Card (KTP). The formulation of the E-KTP with the NIK number in it is allegedly able to recapitulate all population data nationally. The protection of personal data is now disrupted by the existence of one of the candidates for political parties who will advance in the next election asking KPU and Disdukcapil to open all data from the website or all data on upcoming election participants in the name of transparency. This was assessed, the party was lazy to enter data manually into the community. In addition, the NIK in the KTP is very vulnerable to just being uploaded through the internet or other media, because NIK includes birth dates, provincial codes, and district/ city codes that can endanger individuals for cybercrime.

This plan or design does not represent the personal data. The affirmations in each of the articles are shown to the private parties who manage individual personal data. Personal data controllers consisting of individuals, public bodies, the private sector and community organizations as outlined in Article 7 of the Constitution cannot be separated from criminal threats of at least one billion or three years imprisonment. The administration implementation in this constitution plan is very ineffective, considering the absence of definite rules for integrated and safe data centralization in the country. Not to mention the sanctions if they violate, this will make e-commerce businesses in Indonesia sluggish. New players from the country will lose to long-time business watchers and are afraid to do business with such rules. Alignment of the constitution plan with the protection of personal data only sees the internet as a public economization, such as the previous Law Number 11 of 2008 concerning ITE.

Article 11 Paragraph (3) states that "Personal Data Controllers may reject requests for delays in the use of Personal Data if; a. There are laws and regulations that do not allow delays made by Personal Data Controllers; b. It is possible that delays in the management of Personal Data may endanger the safety of others; and the Owner of Personal Data is bound to a written agreement that does not allow delays in the management of Personal Data. "Personal data controllers, whether platforms, banks or anything else that actively holds individual personal data online or offline is responsible for managing data for specific purposes with certain time retention which is worth keeping and cannot be disseminated without the data owner's decision. If not explicitly, data controllers can play tactically to avoid punishment. The case of fintech in the form of cash loans is one of the violations committed by the platform, spreading the personal data of debtors on the internet. LBH Jakarta stated that they had handled 120 cases of online loans by threatening and disseminating personal data from the debtor's mobile phone. Billing from online loans is timeless with an ever-increasing interest rate. The platform creditor always cursed and even sexually harassed the debtor. By those, it can be stated that platforms as personal data controllers can be tactical by outsmarting individual personal data for its benefits.

The encouragement of this constitution plan must be encouraged to achieve the national security regularity. It does not guarantee that the ratification of this bill will become the basis of invulnerable law that suppresses cybercrime or misappropriation of data in the Maya world or real. However, this constitution plan will add to the definite argument that the government has initiated the need to protect the personal data for its citizens. I also kept moving despite the many loopholes like the previous constitution, the ITE Law, the interests of certain groups and the barter of law in court. Since in fact, the ITE Law took place quite a lot to become a law which is now the basis of online world law or constitution. This is the right for citizens, access to information, far from fear. Digital right is also a human rights!

II. Statements of the Problem

How is the Personal Data Protection Model in the Perspective of Indonesian Administrative System and Positive Constitution?

III. Theoretical Review

1. Personal Data

Based on the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 Year 2016 Article 1 concerning Protection of Personal Data in Electronic Systems, Personal Data is certain

personal data that is stored, maintained and maintained by the truth and protected by confidentiality. The Owner of Personal Data is an individual attached to the Certain Individual Data, the Approval of the Owner of Personal Data, which is a written statement both manually and/ or electronically provided by the Owner of Personal Data after obtaining a full explanation of the act of obtaining, collecting, processing, analyzing storage, appearance, announcement, delivery, and dissemination and confidentiality or confidentiality of the Personal Data.

Based on the Constitution of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions Article 26 paragraph 1, states that the use of any information through electronic media relating to one's personal data must be done with the approval of the Person concerned.

Europa Union, 'personal data' means all information relating to identifiable or identifiable individuals ('data subjects'); identifiable people are people who can be identified, directly or indirectly, specifically by referring to identifiers such as names, identification numbers, location data, online identifiers or for one or more specific factors for physical, physiological, genetic identity, mental, economic cultural, social, and natural people.

2. Example of Personal Data

Based on the Constitution of the Republic of Indonesia Number 23 of 2006 concerning Population Administration article 58 paragraph 2, Individual data includes, KK number, NIK, full name, gender, place of birth, date/ month/ year of birth, blood type, religion/ belief, marital status, relationship status in the family, physical and/ or mental disability, recent education, type of work, biological mother, biological mother's name, father's NIK, father's name, previous address, birth certificate/ birth certificate, number birth certificate/ birth certificate number, ownership of marriage certificate/ marriage book, marriage certificate/ marriage book number, marriage date, ownership of divorce certificate, divorce certificate/ divorce number, date of divorce.

IV. Discussion

To overcome the problems that can arise between the interests of protecting privacy and the importance of continuing to maintain information and data transparency, better regulation is needed so that these two rights do not overlap with each other and can still support the progress of democracy and human rights.

To understand this, the legislation model developed must ensure accountability of the State both to protect privacy and ensure information and data transparency. Because both rights have the same level and weight. And if there are cases that arise due to conflicts between the protection of privacy and the interests of transparency, then this must be explored on a case-by-case basis. Therefore, designing good legislation is very important so that both laws are produced, the application of the rules and supervisory institutions can properly balance the two rights.

In the world, there are two legislative models related to information and data openness and privacy protection. The first model is the existence of one legislation regarding the protection of privacy and information disclosure. This model is at least followed by Canada, Hungary, Mexico and Thailand. According to the Supreme Court of Canada, this model is a good regulation with complementary provisions that can and must be interpreted harmoniously. Tothis model, David Banisar states that there are disadvantages when privacy protection legislation and information disclosure are united. Arranging two functions simultaneously will cause confusion at the level of legislation for the purpose of the regulation. This confusion will lead to two conflicting parties because it supports one action. And when there are weaknesses, it is difficult to change legislation.

Meanwhile, there is a second model that adopts two legislation governing information disclosure and privacy protection. Therefore, if there are new legislation to be ratified, there must be a harmonization between the two legislation. If this harmonization is ignored, the two legislation will clash and efforts are needed to revise the information disclosure legislation and privacy protection.

In the Indonesian context, it follows a second model where information disclosure and privacy protection are regulated separately. At present, information disclosure is regulated in Law No. 14 of 2008 concerning Public Information Openness, while privacy protection will be regulated in the Minister of Communication and Information Regulation concerning the Protection of Personal Data in Electronic Systems. The draft Ministerial Regulation according to the Minister of Communication and Information is a mandate from:

Article 15 paragraph (3) Government Regulation No. 82 of 2012 concerning Implementation of Electronic Transactions and Systems. Therefore, the discussion of the Draft Minister of Communication and Information Regulation concerning the Protection of Personal Data in Electronic Systems was discussed jointly with the Directorate General of Immigration, the Indonesian National Archives, the Financial Services Authority, YLKI, Bank Indonesia, and the Ministry of.

The plan of Minister of Communication and Information Regulation concerning the Protection of Personal Data in this Electronic System received criticism from Elsam. In his criticism Elsam stated that the protection of personal data is part of the right to privacy that requires legal

legitimacy equal to the Act. 38 In addition to criticism of the model of legislation, Elsam also noted 4 other weaknesses, namely the criterion of personal data accessible to law enforcement, rights recovery mechanisms, monitoring the implementation of the protection of personal data in the electronic systems, and finally concerning the need for an independent authority to settle disputes.

Despite the criticism, this policy is actually according to the Minister of Communication and Information as a transitional phase towards the Personal Data Protection Constitution which shall be included in the 2016 National Legislation Program.

To compile two separate legislative frameworks, there are five things to consider, namely: Definition of personal information, prioritization of laws, exclusion of privacy in the Information Disclosure Act, who can request access to personal information, and oversight mechanisms and appeals. The supervision mechanism also needs special attention, especially to reduce the possibility of "conflict" between institutions. It is best to have one institution to carry out the oversight mechanism based on public information disclosure legislation as well as privacy protection. With a model of 1 institution to run the oversight mechanism, good experiences will be divided and reduce the potential and risk of conflict. As previously explained, these two rights have a strong relationship because it is important to have one institution to carry out oversight mechanisms for information disclosure and maintaining privacy protection.

Referring to the second model, the Indonesian government is preparing a Constitution on Data and Personal Information Protection (PDIP Constitution) which has been included in the 2016 National Legislation Program. This constitution contains provisions on definitions and classifications regarding the types of personal data that must be protected. In addition, this constitution also draws up a procedural framework that must be followed when collecting, ordering and managing personal data. And most importantly, this constitution also provides guidance on the use of video recording equipment and the role of the Central Information Commission as an institution for monitoring and implementing personal data protection.

It is expected that during the approval of this constitution, this constitution would be the first regulation specifically regulating the protection of privacy and personal data in Indonesia. At present, the protection of privacy and personal data is governed by various regulations in certain sectors such as banking regulated by Law No. 7 of 1992 and health regulated in Law No. 36 of 1999 concerning Health.

There are four objectives to be achieved by this constitution, namely; First, protect and guarantee the basic rights of citizens related to the privacy of personal data; Second, guaranteeing the community to get services from the government, business people and other community organizations; Third, to encourage the growth of the technology, information and communication industry; and Fourth, to support increased competitiveness of domestic industries.

In the context of understanding personal data, this constitution divides it into two types, namely ordinary personal data and sensitive personal data. Sensitive personal data is defined as personal data which includes: religion/ belief, health conditions, physical and mental conditions, sexual life, personal financial data, and others. Meanwhile, general personal data is data relating to a person's life that can be identified either automatically or based on a combination with other information such as names, passport numbers, photos, videos, electronic mail, fingerprints and others

Sensitive personal data can be provided through written agreement in terms of:

1. Protection of data subject safety.
2. Achieving the goal of fulfilling every right & obligation under labor law.
3. The implementation of matters relating to medical goals.
4. The process of law enforcement.
5. The implementation of functions of various parties that have authority based on legislation.
6. Sensitive personal data which is already in the public domain.

The problem is that the PDIP Constitution does not have specific provisions relating to sensitive privadi data or special procedures related to such sensitive personal data. At present the available regulations do not classify personal data especially those that can be categorized as sensitive personal data. For example, related to medical records, based on Law No. 36 of 2009 concerning Health, Hospitals are prohibited from publishing such data. Likewise regarding the financial data of a person categorized as privacy based on Law No. 6 of 1983 concerning Taxation (amended based on Law No. 16 of 2009) and Law No. 7 of 1992 concerning Banking (amended based on Law No. 10 of 1998). Meanwhile, data related to mental and physical health, fingerprints, and retina, are categorized as personal data based on Law No. 23 of 2006 concerning Population Administration (amended based on Law No. 24 of 2013).

The oversight mechanism in the PDIP Constitution uses the same monitoring mechanism as the UU KIP, namely through the Central Information Commission. The Central Information Commission has a function to ensure that private data providers comply with and comply with the provisions in the law and encourage all parties to respect the privacy of personal data. In implementing this function, the Central Information Commission is authorized to:

1. Monitoring compliance of all parties related to the protection of personal data.

2. Receiving complaints, facilitate dispute resolution, and conduct assistance.
3. Coordinating with other government agencies and the private sector.
4. Publishing guidelines for protecting personal data.
5. Providing recommendations to law enforcement. Providing first and second warning letters/ warnings.
6. Against violations by data providers.
7. Conducting research.
8. Facilitating the enforcement of personal data protection.
9. Providing opinions and suggestions for the establishment and application of other regulations relating to the protection of personal data; and
10. Negotiation

The PDIP Constitution extends the scope of authority from the Central Information Commission. Under the UU KIP, the Central Information Commission is only authorized to resolve information disputes. However, the PDIP Constitution still leaves a fundamental weakness in the event of a dispute regarding personal data. The tools that will be used by the Central Information Commission in this PDIP Constitution is still unclear.

V. Conclusion

1. Information disclosure and privacy protection basically have the same purpose, namely to encourage accountability from the government towards the people. Although overlaps and risks of conflict arise in some cases, these two rights basically complement each other.
2. Considering the issue, therefore it is important to formulate and harmonize legislation either in terms of information disclosure legislation or for the protection of personal data, especially to have a good definition of personal information. The formulation of this personal information is important to be carefully formulated in order not to interfere with the interests of public information disclosure in the name of privacy protection.

Bibliography

1. Republic of Indonesia. 2016. Regulation of the Minister of Communication and Information No. 20 of 2018 concerning Protection of Personal Data in Electronic Systems. Jakarta.
2. Republic of Indonesia. 2008. Law No. 11 of 2008 concerning Information and Electronic Transactions. Jakarta.
3. Academic Manuscript for Personal Data Protection Constitution.
4. Australia. 1988. Privacy Act.
5. Republic of Singapore. 2012. Personal Data Protection Act 2012. Singapore.
6. European Parliament. 2016. Regulation (Eu) 2016/679 Of The European Parliament And Of The Council.
7. M. Yvonne. 2017. Conceptualising the right to data protection in an era of Big Data. Sage
8. https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age