Business & Social Science
IJRBS

Research in Business & Social Science

IJRBS VOL 10 NO 1 ISSN: 2147-4478

Available online at www.ssbfnet.com
Journal homepage: https://www.ssbfnet.com/ojs/index.php/ijrbs

The urgency of digital right management on personal data protection

Bayu Sujadmiko [(a)] *Intan Fitri Meutia*[(b)*] *Didik Kurniawan*[(c)] *A Negra Mardenitami*[(d)]

[(a,b)]*Universitas Lampung, Indonesia*
[(c)]*Attorney General's Office, Indonesia*
[(d)]*National Land Agency Lampung Province, Indonesia*

ARTICLE INFO

Article history:

Received 21 December 2020
Received in rev. form 12 Jan. 2021
Accepted 13 January 2021

Keywords:

Digital Right Management, Data Protection, Governance, Policy

JEL Classification:
L5 K2

ABSTRACT

Today, the utilization of technology is not merely for the sake of entertainment, but also the exchange of information, trade, study, and governance. Followed by the increasing level of the technology application in various activities, not a few people become victims or perpetrators of a personal data breach in the cyber world. Thus, it is necessary to implement digital right management (DRM) by the manager of electronic systems, the Government and rights holders in the cyber world in computer systems. The research method in this article is a normative legal research method. The approach used in this research is the statute approach and the case approach. The Indonesian government has validated the rules that accommodate the protection of the personal data of each citizen in cyberspace, namely, Act number 14 of 2008 concerning Openness of Public Information, Act Number 19 of 2016 concerning Amendments to Act Number 11 of 2008 concerning Information and Electronic Transactions, Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems and Presidential Regulation Number 39 of 2019 concerning One Data Indonesia. Based on these rules, all parties involved in the management, storage and exchange of personal data in Indonesia must have an integrated and trusted DRM mechanism.

Introduction

The Personal data is currently a purchasable and exchangeable product since it has evolved into a highly valued asset and commodity (Makarim, 2003). Moreover, it has a flexible flow and portrays the strength of globalization (Kong, 2010). Recent researches estimated 20% of the world's data has been gained (Zyskind et al., 2015). The global community's awareness in regards to their personal data must be enhanced, considering the usage of cyber area is increasing in 2017, which reaches more than 4.2 billion people compared to 2016 which only reached 3.7 billion internet users. Based on these data, internet users have overcome 54.4% of the whole human population that is approximately 7.6 billion people (MMG, 2020). In 2020, Indonesia's Internet users have reached 175.4 million people with a 64% penetration. This means that 64% of 272.1 million Indonesian populations are actively using the Internet (Pertiwi, 2020). Moreover, in 2006, the sale value of personal data is assumed to reach 3 billion US dollars and counting. Until this day, there are approximately 550 corporations that perform consumers' personal data transactions (Peek, 2006).

The cyber-world provides every party an opportunity as a potential victim or criminal perpetrators either aware or not (Aisyah, 2020). As an example, in social media, social media's feature enables people to share their personal data about themselves such as photos, videos, address, places they go to and other intimate information, it misconducts the benefit of the internet usually used to harass, threaten, and intimate people (Hazelwood, et al., 2013). Eventually, it creates new forms of crime such as cyberstalking, which are online assault or repetitive stalking and dangerous threats. Cyberstalking cases are unique, because society normalized it; this is because the tools used are sophisticated (Pittaro, 2007). Some perpetrators compromise details of their crime act's form which is planned for the victim in order to cause psychological and physical pressure (Suryanegara, 2019).

According to the Author, the usage of social media and internet culture in society has become a dilemma where every person has their right on their privacy but through the merge of social media and its utilization, the right to someone's privacy is as given for granted. Privacy of rights discussed in this research means a person's rights to give or not give their personal data to other parties as

* *Corresponding author. ORCID ID: 0000-0001-9818-8459*

https://doi.org/10.20525/ijrbs.v10i1.990

stipulated in Article 17 of the Right Committee General Comment No. 16 (1998) on the Right of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation.

Responding to this matter, there are numerous ways that the government, parties of technology corporations and individuals can overcome to have their rights to privacy managed under protection. One of the ways is by applying a security management system or usually known as Digital Right Management (DRM). DRM was first introduced in the World Wide Web Consortium (W3C) through a workshop held in January 2004. The DRM system functions as a security procedure that uses certain algorithms from the preparation to the distribution process which is connected to a digital or non-digital infrastructure and computation that protects a creator's or digital material owner's rights (Prayudi, 2004). Algorithms are usually a solver in system ambiguities (Sahlani, 2020). The DRM system has a variety of forms, such as Cryptography, The Open Group Architecture Technique (TOGAF) (Ekawati, 2017), Information Right Management (IRM) (Pratama, et al, 2017), eXtensible Right Markup Language (XrML) and other based systems. These systems are applied by private sectors to guard confidential information or control their use of an intellectual property. In this scientific world, inventions of distribution have become a high world phenomenon, thus it is needed (Arshad et al, 2020).

The government as its society's protector must consider the massive benefits of DRM and start introducing the DRM system towards the society thus the pressure of a person's rights to privacy is not solely aimed at the government. Therefore, it is natural for the government to commend a policy that could accommodate and provide convenience and safety for the society regarding their personal data. As for now, the protection of personal data is regulated in Law No. 14/2008 on Public Information Transparency, Law No. 19/2016 on the Amendment of Law No. 11/2008 on Information and Electronic Transaction, the Ministry of Communication and Information Regulation No. 20/2016 on Personal Data Protection in the Electronic System, and the President Decree No. 39/2019 on Indonesia's One Data. It is very important to make sure regulations and policy to be executed since policy implementation is an interpretation of enforcement (Meng, 2020).

After continuously analyzing, there are several flaws found in these regulations. Then, what actions should the government of Indonesia determine to formulate a regulation that supports the RDM system regarding personal data protection? The author will further discuss the weakness of the ongoing regulations and actions that the governments should consider in terms of protecting personal data through this research based on a normative-judicial method approach and using the qualitative technique in data analysis.

The research method in this article is a normative legal research method. The approach used in this research is the statute approach and the case approach. Furthermore, the legal materials used are primary, secondary and tertiary legal materials, which are then analyzed using qualitative juridical analysis techniques. An empirical juridical approach is carried out to study law based on facts or facts objectively obtained in the field, in the form of opinions, attitudes and behavior of apparatuses. Based on Soemitro (1982), the empirical juridical approach is an approach carried out by conducting research by collecting primary data obtained directly from the object of research through interviews with respondents and resource persons related to the research. The approach is carried out by making direct relationships with parties who are considered to know things which have something to do with the problems that are being discussed in this thesis. The empirical approach is carried out by observing or observing legal behaviors or symptoms and legal events that occur in the field.

Law No. 14/2008 on Public Information Transparency

Generally, Law No. 14/2009 on the Public Information Transparency has already been regulated regarding personal data protection ruled in Article 6, Article 17 letter (g) and (h), Article 18 Paragraph (2), Article 35, Article 43, and Article 54. Based on Article 6 Paragraph (3) letter c of Law *a quo* emphasizes the public agency to not share public information in relation to personal rights. These personal rights are information about a person's personality as regulated in Article 17 letter (g) and (h) which is an authentic deed that is personal or last will nature and information in correlation with a personal confidence states as an excluded information. Information that could reveal personal data are related to:

i. History and condition of a family member;
ii. History, condition and maintenance, physical health medication, a psychic of a person;
iii. Financial state, asset, income, and bank account of a person;
iv. Evaluation results in regards to capability, intellectual, and recommendation of a person's skill; and/or
v. Record on a person in regards to formal education or non-form education activities.

Law No. 19/2016 on the Amendment of Law No. 11/2008 on Information and Electronic Transaction

Law No. 19/2016 on the Amendment of Law No. 11/2008 on Information and Electronic Transaction has regulated provisions of personal data usage in Article 26 that determines for each person that seeks to utilize information through electronic media that concerns personal data must be in respect with the data owners' consent. Every electronic system organizer must delete irrelevant electronic information and/or documentation under the request of the concerned party based on the court's enactment and provides mechanisms of irrelevant electronic information and/or documentation deletion in accordance with the regulations' provisions.

The government further emphasizes towards all-electronic system organizer to arrange an integrated electronic system as stipulated in Article 16 Paragraph (1) that reads:

"As long as the Law does not regulate otherwise, every electronic system organizer is obligated to operate an electronic system that fulfills minimum requirements as follows:

i. *Has the ability to re-display electronic information and/or documentation as a whole in accordance with the retention period enacted by the regulation;*
ii. *Has the ability to protect availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the electronic system organizer;*
iii. *Has the ability to operate accordingly with the procedure or guidance in the electronic system enforcement;*
iv. *Equipped with a procedure or guidance which is announced through a language, information, or symbol that could be easily understood by parties that has a correlation with the electronic system organizer; and*
v. *Has a sustainable mechanism to protect novelty, clarity, and accountability of a procedure or guidance."*

The Ministry of Communication and Information Regulation No. 20/2016 on Personal Data Protection in the Electronic System

The Ministry of Communication and Information Regulation No. 20/2016 on Personal Data Protection in the Electronic System merges as an implementing rule of personal data protection which is previously discussed in No. 14/2009 on the Public Information Transparency and Law No. 19/2016 on the Amendment of Law No. 11/2008 on Information and Electronic Transaction. According to Article 2 of the Ministry Regulation No. 20/2016, personal data protection in an electronic system includes protection towards gaining, collecting, managing, analyzing, restoring, displaying, publishing, delivering, disseminating, and deletion of personal data. The government obligates the electronic system organizer to implement personal data protection principle which involves:

i. Respect for personal data as privacy;
ii. Personal data is confidential based on agreement and/or the provisions of regulations;
iii. Based on an agreement;
iv. Relevance in aims to towards gaining, collecting, managing, analyzing, restoring, displaying, publishing, delivering, and disseminating;
v. The qualification of the used electronic system;
vi. Good deeds to immediately inform data owners through a written notice for ever personal data protection failure;
vii. Availability of personal data protection management's internal rules;
viii. Responsibility on personal data under the users' acknowledgment.
ix. Accessibility and correction towards personal data by personal data owners; and
x. Integrality, accuracy, legality, and update of personal data.

Policy Implications

As the Author previously stated above, the government has authorized several regulations in respect of personal data protection starting from types of data including personal data, parties that are authorized to manage data, the obligation of a data manager, rights of data owners, dispute settlement, and even criminal sanction towards violators as fulfillment form of Article 28 of the 1945 Indonesian Constitution's mandate. This is very vital since we have shifted to industry 4.0 which is revolutionary and innovative in their operation (Baloutsos, 2020). The following description is an analysis of Law No. 14/2008 on Public Information Transparency, Law No. 19/2016 on the Amendment of Law No. 11/2008 on Information and Electronic Transaction, the Ministry of Communication and Information Regulation No. 20/2016 on Personal Data Protection in the Electronic System, and the President Decree No. 39/2019 on Indonesia's One Data.

However, the mentioned information in Article 17 letter (g) and (h) is accessible or is not in the category of excluded data if the parties who experienced confidence exposure agree to arrange a written agreement as stated in Article 18 Paragraph (2) letter (a). The *a quo* Law also provides opportunities for the parties that receive decline from the requested information based on the reason of exclusion in Article 17, by applying a written objection towards the Officials of Information and Documentation Manager. As an act of repression in confidential information protection, the government will impose sanctions of imprisonment for a maximum 2 (two) years and/or a fine for a maximum 10.000.00 IDR (ten million Indonesian Rupiah) towards parties who illegally accessed excluded data as defined in Article 17.

If we pay attention closely, the Public Information Transparency Law has universally regulated personal data protection, yet it is unspecific. Nevertheless, the *a quo* Law has provided space for the authorized government in handling the information system which is the Ministry of Communications and Information, to apply an integrated data protection system or DRM in order to protect rights upon data of every civil in Indonesia.

The *a quo* Law also regulates the interception activity or private information tapping such as debt and medical records or other personal data which either could not cause changes or could cause changes, deletion, and/or termination to transmission process or data exchange unless it is done by the law enforcement based on the provision that is stipulated in Article 31. Every person is also prohibited from illegally changing, adding, reducing, transmitting, destructing, deleting, moving, hiding, and causing accessibility to a person's electronic document/information by the public as stipulated in Article 32.

If in the future, a violation occurs or the data owner feels aggrieved by the electronic system organizer, the data owner could file claims towards the organizers based on the ongoing regulation. The Law on Information and Electronic Transaction also provides options in regards to the dispute settlement that is regulated in Article 39 Paragraph (2) of the Law on Information and Electronic Transaction, which explains that other than civil charges, the parties could solve their disputes through arbitration or other alternative dispute settlement institutions.

The weakness of Law *a quo* is that it does not determine what data are categorized as personal data nor does it categorize online activities that are included as a personal data crime. Furthermore, the government is passively enrolled by fully submitting the responsibility towards the data owners. This situation makes it difficult for the data owners for there is no supervision from the government to the data organizers regarding data that are shared, thus data owners have a hard time realizing any data leakage.

Afterward, the electronic system organizer must undergo an electronic system certification that is used to gain, collect, manage, analyze, restore, display, publish, deliver, disseminate, access, and delete personal data. The government also requires a personal data protection system if potential circumstances could cause data leak and violations towards the right to personal data in Article 5. This Article places guidance to electronic system organizers in designing the digital right management in their system. It also clarifies the data owners' right regulated in Article 26 that includes the right to:

i. Personal data confidentiality;
ii. Propose complaints to the minister in a personal data dispute settlement for the failure of personal data's confidential protection by the electronic system organizer;
iii. Gain access or opportunity to alter or renew personal data without interrupting the personal data management system, unless it is regulated otherwise;
iv. Gain access or opportunity to a personal data record that was submitted to the electronic system organizer as long as it is in accordance with the regulation; and
v. Request certain personal data abolishment in the electronic system that is managed by the electronic system organizer, unless it is regulated otherwise.

This regulation has completely ruled the provisions on personal data protection. However it is very unfortunate that this regulation is in the forms of a ministry regulation instead of a technical Law. Moreover, this regulation only charges administrative sanctions which are:

i. Verbal warning;
ii. Written warning;
iii. Postponing an activity; and/or
iv. Announcement in a network's site (online web page).

The Bill of Personal Data Protection Law

The urgency of personal data protection is greeted well by the government through the enactment of the Bill of Personal Data Protection Law that. Considering there is a few weaknesses from the enforced Laws, which are regulations on:

i. Types of personal data;
ii. The rights of personal data owner;
iii. Exception towards personal data;
iv. The obligations of the personal data manager and controller;
v. Personal data protection officials;
vi. Personal data transfer;
vii. Guidance on personal data manager behavior;
viii. Dispute settlement;
ix. International cooperation;
x. The government's and society's participation; and
xi. Criminal prohibition and provisions.

This bill also determines that the personal data manager is obligated to protect and ensure the processed personal data's safety, by performing:

i. Formulation and implementation of operating technical steps to protect personal data from the interruption towards personal data processing which is against the regulations; and

ii. Determination of personal data's safety level by paying attention to the personal data's nature and risk that should be protected in the personal data's processing.

Furthermore, the personal data processor manager must appoint an official to execute functions of personal data protection, including supervising function. If this bill has passed in the future, then the government's role in personal data protection will no longer be passive. The government will be obligated to supervise every party that is correlated to the personal data management in Indonesia. Besides that, public agents or organizations/institutions must own a good plan and possess digital right management in a computation system that is constantly under monitor and updates.

The Urgency of Digital Right Management (DRM) in the Personal Data Sector Protection Sector in Indonesia

Generally, the Digital Right Management (DRM) is a technique, process, procedure, and algorithm from preparation to distribution process that is connected to a digital or non-digital infrastructure and a safe and trusted computation which aims to protect the creator digital material owner's rights (Prayudi, 2004). The DRM system used by private sectors such as corporations, organizations, or individuals varies from simple to complex systems. DRM is usually automatically installed in a windows or iOs system in a firewall or antivirus form. However, the software is only effective in protecting computer systems from digital viruses.

Therefore, as an effort to protect a personal document in a computer system, experts created a data protection system that locks a document with an algorithm or other supporting application as well as Information Right Management (IRM) that we find in the application such as Ms. Office, Adobe, etc.IRM systems will encrypt a document, so if a person wishes to open it, they have to insert a password. It is possible to create DRM in a web form where Web Service based DRM Server, DRM Database Server, Directory Service, and CA Server is needed. Shortly, this system will provide public and private keys in every electronic that will be applied with DRM and create a license that contains information on the addressed rights towards the document and restore all DRM data in every document in the database server section (Kurniawan, 2008). Another way is by using a watermarking application. This system possibly enables the data owner to sign or provide a picture or video type data that is useful to prove the picture's or video's owner (Yucel, 2005). A handful of people are aware of the merge of DRM in their gadgets or computers, therefore the government must be present in delivering socialization regarding DRM operation and activation in a person's electronic document.

The implementation of DRM in every personal data is not an exaggeration considering personal data have become a highly valued commodity with its own market. Therefore, the government must deliberate which DRM designs to use in protecting personal data that is computed in harmony with the discourse or e-government optimize operation based on President Regulation No. 39/2019 on Indonesia One Data. If we refer to Regulation No. 39/2019 on Indonesia One Data, there are six government agencies in coordination which is led by the head of BAPPENAS, these six institutions include:

i. Minister of Administrative and Bureaucratic Reform;
ii. Minister of Communications and Informatics;
iii. Minister of Home Affairs;
iv. Minister of Finance;
v. The Head of Central Bureau Statistics;
vi. The Head of Geospatial Information Agency.

Afterward, the Ministry of Communication and Information also needs to consider a division enactment that has a duty to protect personal data and supervise the data exchange traffic, which involves an Indonesian citizen. The government could also cooperate with a third party in maintaining the effectiveness of the DRM system. Not the least important, the government must also arrange a public dialog with academicians consisting of law and technology experts in order to immediately pass the Bill of Protection Data Law.

Conclusions

Based on the discussion above, it is concluded that the ongoing Law of Indonesia in correlation with personal data is passive and has not ruled comprehensively. The Ministry of Communication and Information Regulation No. 20/2016 on Personal Data Protection in the Electronic System thus far does regulate on personal data protection as an executor or ethnic wise. The government needs to arrange socialization in regards to the usage and operation of Digital Right Management (DRM) to have a more aware society on their safety of privacy and personal data protection. Furthermore, the government needs to deliberate the utilization of DRM personal data protection, from the planning to the protection process in a digital system by inserting a DRM program in every government and citizen's data.

References

Aisyah, E. N., Iriyanto, T., Hardika, H., Rosyida Mayani, & Maningtyas, T. (2020). The Cyber Ethics of Academic Communication Based on Early Childhood Education Student Perception in Universitas Negeri Malang. *ATLANTIS PRESS Advances in Social Science, Education and Humanities Research*, *446*(Icli 2019), 1. https://doi.org/10.2991/assehr.k.200711.001

Arshad, M. Z., Iqbal, M. Z., & Ahmad, M. (2020). Exponentiated power function distribution: Properties and applications. *Journal of Statistical Theory and Applications*, *19*(2), 297. https://doi.org/10.2991/jsta.d.200514.001

Baloutsos, S., Karagiannaki, A., & Mourtos, I. (2020). Business Model Generation for Industry 4.0: A "Lean Startup" Approach. *The International Technology Management Review*, *9*(1), 34. https://doi.org/10.2991/itmr.k.200630.001

Ekawati, R. K. (2017). Perencanaan Infrastruktur Teknologi Informasi pada Bank dengan Framework TOGAF. *Jurnal Sistem Informasi Bisnis*, *7*(2), 156. https://doi.org/10.21456/vol7iss2pp154-160

Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. *International Journal of Cyber Criminology*, *7*(2), 155.

Kong, L. (2010). Data Protection and Transborder Data Flow in the European and Global Context. *European Journal of International Law*, *21*(2), 441. https://doi.org/10.1093/ejil/chq025

Kurniawan, A. (2008). Digital Rights Management Sebagai Solusi Keamanan Dokumen Elektronik. *Jurnal Sistem Informasi*, *4*(2), 94. https://doi.org/10.21609/jsi.v4i2.251

Makarim, E. (2003). *Kompilasi Hukum Telematika*. Jakarta: PT Raja Grafindo Perkasa.

Meng, Z., Yu, D., Wang, J., & Zhao, S. (2020). *Policy Implementation Performance and Political Trust*. *146*(Isbcd 2019), 175. https://doi.org/10.2991/aebmr.k.200708.034

Miniwatts Marketing Group (MMG), Internet Usage Statistic, dalam https://www.internetworldstats.com/stats.htm accessed on 4 Mei 2020.

Peek, M. E. (2006). Information Privacy and Corporate Power: Toward a Re-Imagination of Information Privacy Law. *Seton Hall L. Rev.*, *37*, 6–7.

Pertiwi, W. K. (2020). *Penetrasi Internet di Indonesia Capai 64 Persen*. Kompas.com. https://tekno.kompas.com/read/2020/02/20/14090017/penetrasi-internet-di-indonesia-capai-64-persen accessed on 04 Mei 2020

Pittaro, M. L. (2007). Cyber stalking: An Analysis of Online Harassment and Intimidation. *International Journal of Cyber Criminology*, *1*(2), 181. https://doi.org/10.5281/zenodo.18794

Pratama, R. H., & Siswanto. (2017). Menggunakan Information Rights Management (Irm) Sebagai Bagian Dari Pengendalian Preventif Pada Sistem Informasi Akuntansi Organisasi Publik. *Substansi: Sumber Artikel Akuntansi Auditing Dan Keuangan Vokasi*, *1*(2), 362–371. http://jurnal.pknstan.ac.id/index.php/SUBS/article/view/257

Prayudi, Y. (2004). Aplikasi Teknologi Informasi 2004 Digital Right Management (DRM) Berbasis XrML. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 56.

Sahlani, H., Hourali, M., & Minaei-Bidgoli, B. (2020). Coreference Resolution Using Semantic Features and Fully Connected Neural Network in the Persian Language. *International Journal of Computational Intelligence Systems*, *13*(1), 1002. https://doi.org/10.2991/ijcis.d.200706.002

Suryanegara, M., Harwahyu, R., Asvial, M., Setiawan, E. A., & Kusrini, E. (2019). Information and Communications Technology (ICT) as the engine of innovation in the co-evolution mechanism. *International Journal of Technology*, 10(7), 1260. https://doi.org/10.14716/ijtech.v10i7.3777

Yücel, Z., & Özgüler, A. B. (2005). An audio watermarking algorithm via zero assigned filter banks. *2005 13th European Signal Processing Conference (Pp. 1-4). IEEE.*, *1*. https://doi.org/https://doi.org/10.5281/ZENODO.39414

Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *2015 IEEE CS Security and Privacy Workshops*, 180. https://doi.org/10.1109/SPW.2015.27

Publisher's Note: SSBFNET stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.