

Legislation of Electronic Data and Service in Indonesian Public Institutions: A Proposed Future

Budi Agus Riswandi^a, ^aFaculty of Law Universitas Islam Indonesia, Email: budiagusr@uii.ac.id

The use of information technology has been having implications on legal life. One of them involves the impacts of legislation on data and electronic services for public institutions. Indonesia is one of the countries that have not yet developed legislation regarding electronic data and services based on the convergence paradigm as a fundamental principle in the utilization of information technology. As a result, various legislation problems pertaining to data and electronic services have emerged. Therefore, Indonesia should attempt to renew its legislation on data and electronic services. The concrete attempt is performing legislative action in terms of electronic data convergence and telematics, which will be served as a legal protection, and it will be followed by the process of synchronizing existing laws and regulations. This study was conducted using normative legal research methods, which are based on the legal system and drafted a legal system related to electronic data and services in Indonesia and other previous literatures.

Key words: *Legislation, data, services, electronics, public institutions.*

Introduction

The use of information technology has had two different impacts on people's lives. On one hand, the use of information technology has offered a number of conveniences, namely speed and reduced costs for every member of the community when carrying out their activities. On the other hand, the use of information technology has caused various problems. These problems include: social, political, economic, cultural and legal issues, and these can impact work internationally (Land, 2013).

From the perspective of public institutions, the use of information technology is believed to

improve the quality of public services, and is expected to lead to public welfare. To promote this, there are prerequisites that must be fulfilled. The prerequisites include proper information technology, management, and law. Good and proper information technology, management, and legal prerequisites basically lead to a certain standard, by taking into account the characteristics and dynamics of information technology.

However, as a matter of fact, this is sometimes not realized and the proper legal requirements are frequently ignored. Law as an instrument that optimally utilizes information technology should be based on certain legal standards. They are mainly related to the use of legal paradigms. There are two legal paradigms that must be considered in strengthening the law related to the use of information technology, namely the paradigm of neutral technology law and convergence. To streamline the attention to this law's paradigm, it can be initiated since the legislation drafting process made use of information technology by public institutions.

In this context, it is interesting to study the various drafting of legislations in the use of information technology in Indonesia, by looking at the use of the convergence paradigm. The use of this convergence paradigm applies also in the formulation of electronic data and service legislation that are used by Indonesian public institutions as an integral part of information technology. The definition of electronic data includes all of the information and statements produced by public institutions through electronic systems. Meanwhile, electronic services refer to a particular service using electronic systems that the government uses to produce, store, transmit and collect data by public institutions. For the public institution itself, it is intended that the executive, legislative, judiciary, and other bodies whose functions and tasks are related to the state administration. In a case that a part or all of the funds sourced from the State Revenue and Expenditure Budget and / or Regional Revenue and Expenditure Budget, or organization non-government as long as part or all of the funds are sourced from the State Revenue and Expenditure Budget and / or Regional Revenue and Expenditure Budget, donations from the public, and/or abroad.

The issue of electronic data and services for public institutions has become a serious and strategic legal problem in Indonesia. As known, electronic data produced by public institutions are of important instrument for the community, especially for those who need electronic data. With electronic data produced by public institutions, certain parties can benefit from effective law enforcement or an improved quality of public services and human resources. Electronic data is produced by public institutions and can increase people's welfare.

This condition has become somewhat difficult to realize in Indonesia for several reasons. Firstly, electronic data available at public institutions cannot be presented properly and accessed by those who need it. Problems with the proper and accessible data in public

institutions are increasingly noticed when electronic data in public institutions are now produced massively through the use of an electronic service system that adheres to the divergence/sectoral paradigm in its legislation. This condition is increasingly accelerated with the phenomenon of advanced information technology which has led to the acceleration of globalization and a big leap for information and communication dissemination throughout the world (Isnaeni, 2009). As a result of these symptoms, electronic data in public institutions are abundantly available, but its validation and accuracy are not necessarily guaranteed and can be accounted for. Added to this, along with the abundance of electronic data produced by public institutions and its open access, this is not surprising that it can lead to data misuse which might be contrary to the law. This condition has initiated the crime called identity theft. According to the FTC, "Your identity can be stolen by co-opting your name." Identity theft occurs when a person provides personal information without having the knowledge of fraud or theft (Braumer and Poindexter, 2002). The use of electronic data produced by public institutions is also vulnerable to all kinds of actions contrary to law, including those for fraud. Moreover, electronic services provided by the government do not provide security guarantees, both in terms of technology and law.

On this basis, this paper was made to describe the arrangement of data and electronic services in Indonesian public institutions. This study also attempts to reveal the problems arising from the regulation of electronic data and services in Indonesian public institutions. At the end of the paper, practical implications will be discussed on the arrangement of electronic data and services within this context.

The Importance of Data and Electronic Services in the Use of Information Technology by Public Institutions with the Convergence Law Paradigm

The use of information technology has been encouraged, shifting every aspect of human life from the implementation of paper-based activities (paper document) into the implementation of paperless document activities. Then this activity tends to lead to a model of convergence activity rather than divergence. The word 'divergence' means "to be branched; in a state of spread", while the word convergence implies "towards one meeting point; are centred." (Suharso and Retnoningsih, 2009). From this context, the tendency of activities with the use of information technology is centralized at one meeting point. Along with this, this is one of the factors that influences the public body activities that begin to shift to non-paper-based activities and are convergent in nature. Activities of public institutions that began to shift non-paper-based and convergence-based activities were accelerated with various types of electronic service delivery platforms, such as email, e-learning, e-banking, e-government and so on.

The shifted implementation of public body activities as above also occurs for public institutions in Indonesia. Therefore, it is not surprising that there are many developing types of data in the forms of electronic data produced by many parties in public institutions through various electronic service platforms themselves. This situation has created to two paradoxical things. The use of technology by public institutions can provide convenience, but on the other hand the use of technology by public institutions can lead to legal problems. This is as stated by Nora C Porter stating:

Technology is supposed to make our lives easier. When used judiciously, it can expedite things and allow enormous flexibility both at work and home. Untamed, however, it can speed things up to an intolerable pace, creating unrelenting stress and complexity, and dominate our lives. Leaving aside major Internet issues like Big Brother, pornography, paedophilia, crimes of fraud and deceit of every sort, and the crippling assaults of hackers on any and every system, here are some thoughts on dealing with it.

Understanding two paradoxical situations, strengthening the administrative framework and enforcing the law relating to the activities of public institutions that produce electronic data from the development of electronic services are an absolute prerequisite. This is as revealed by Cain quoted by Sharif N As-Saber et al. (2006) who stated:

Seamless communication and information flow and data management are the primary preconditions of an effective e-government structure. It requires reasonable assurance not to be affected by illegal activities by computer hackers and cyber criminals. In this regard, it is important that the sufficient safeguards are in place to ensure the security and privacy of information and data management. Therefore, a strong administrative framework together with the ability to enforce law is an important precondition for a country's economic development and stability. Appropriate legislation needs to be addressed to the legal needs of specialized, complex and highly technical ICT sectors. Any obstacles, either legal or administrative, may be the implementation and progression of e-government activities (As-Saber et al., 2006).

From the above context, the legal requirements could anticipate the amount of electronic data that is generated through electronic services, and the regulation of data and electronic services becomes important and strategic. In fact, many countries have done this, such as the Philippines and China. The Philippine government has made a program called the e-procurement system initiative in the Philippines. This program has provided legal guidelines on how to do electronic business, and how to advertise and post offers or notifications in new electronic systems. In addition, the e-Commerce law was enacted to provide legal protection for electronic documents. China created a program called Beijing's Business e-Park initiative.

Through this program, government officials learnt to do their jobs more quickly and efficiently. Then the government leaders were educated to be responsible for explaining what e-Government is and what its benefits are to society. In the end, basic computer and Internet training are provided for government staff and public users of e-Government systems (Ndou, 2004).

The issue of electronic data and services in public institutions is one of the most crucial aspects in the utilization of information technology by public institutions. The crucial value of this aspect, where electronic data and services in the utilization of information technology by public institutions is a vital aspect in the utilization of information technology by public institutions and both cannot be separated. If the data used in the utilization of information technology are both accurate and valid and are supported by safe and reliable electronic services. The implementation of public services through public institutions can be realized with quality. This certainly can apply otherwise. Therefore, the availability of legal rules can create accurate, valid, safe and reliable electronic data and services are prerequisites for delivering quality e-government.

In line with that, Indonesia is a country that is actively increasing the use of information technology in public institutions (e-government), and has also taken steps to strengthen the administrative and legal framework. Law reinforcement is carried out through the establishment of various kinds of statutory provisions that have relations with the utilization of information technology in public bodies. Some legal provisions include: (1) Law No. 43/2009 concerning Archives; (2) Law No. 17/2011 concerning State Intelligence; (3) Law No. 11/2008 concerning Information and Electronic Transactions; (4) Law No. 14/2014 concerning Public Information Openness; (5) Law No. 36/1999 concerning Telecommunications; and (6). Law No. 32/2002 concerning Broadcasting.

In its development, the above legislation that was created to anticipate and facilitate the use of this technology seems to have lagged behind the progress of information technology itself. Some of the things that are considered to be lagging behind the in Indonesian legislation include several aspects. Firstly, it appears that the available legislation is still in the context of the divergence/sectoral paradigm. This can be seen, for example, in the issue of public and telecommunications information disclosures that are still separate, where the fact is in the use of information technology, especially the use of e-government, there has been a paradigm of convergence between public and telecommunications information disclosure. In fact, legislation that regulates broadcasting information and electronic transactions is also a part that is not separated from the issue of divergence paradigm. Therefore, the drafted legislation is related to the data and electronic services that should be designed with reference to the convergence paradigm, not divergence.

Secondly, further consequences of the available legislation are still based on the divergence/sectoral paradigm, so in reality there have been a variety of institutional and divergent/sectoral institutions. As a result, the roles and duties of these institutions have become ineffective and inefficient. Thirdly, the existence of legislation that still uses the divergence/sectoral paradigm is also potentially weak in preventing data misuse. Data availability becomes very diverse. On the other hand, some legislations that have a divergence/sectoral paradigm that seem to have given a rise to terminology, concepts and substances that differ from the legislation itself. In fact, the terminology, concepts and substance when approached from the convergence paradigm should not have happened.

Based on the facts above, the drafted legislation on the use of information technology, specifically in the case of e-government by changing the divergence/sectoral paradigm into convergence, becomes very urgent. In addition, the availability of legislation regarding data protection using convergence paradigm is another important part that must be performed. This meeting needs to be done so that drafted legislation in terms of the utilization of information technology can be made to be responsive, facilitative and visionary in the future.

The Nature of Electronic Data in Indonesian Legislation

As stated above, the drafted legislation with a convergence paradigm including electronic data protection, becomes significant. At least, this can be experienced by not creating new terminology, concepts, or any substances when drafting legislation on the use of information technology based on the convergence paradigm. On the contrary, drafted legislation when approached by the divergence/sectoral paradigm, has resulted in different terminology, concepts and substances.

The evidence can be seen in the process of electronic data interpretation and the nature of the electronic data itself. From this point of view, Indonesia has formulated the nature of electronic data in several laws and regulations which governed data, especially electronic data. This can be seen in the provisions of Law No. 43/2009 concerning Archives, Law No. 17/2011 concerning State Intelligence, Law No. 11/2008 concerning Electronic Information and Transactions and Law No. 14/2008 concerning Public Information Openness.

Based on these laws, some terminologies which have a relationship with data can be found. There is "archive" in Law No. 43/2009, "intelligence secrets" in Law No. 17/2011, "electronic information" and "electronic documents," in Law No. 11/2008, and "information" and "public information" in Law No. 14/2008. The consequences of different terminologies in some of these laws creates a different understanding of the terms. The term 'archive' is defined as an activity or event recording in various forms and media, in accordance with the development of information and communication technology made and accepted by state

institutions, regional government, educational institutions, companies, political organizations, community organizations, and individuals in the promotion of social life within the local and national scope. 'Secret intelligence' is defined as the information, objects, personnel, and/or efforts, work, and intelligence activities that are protected by confidentiality so they are unknown, cannot be accessed, and cannot be owned by unauthorized parties. The term 'electronic information' is defined as one or a set of electronic data, including but not limited to, writing, sound, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail (electronic mail), telegram, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or processed perforations that can be accessed by those who are able to understand them. The term 'electronic document' is defined as any electronic information that is created, forwarded, transmitted, received, or stored in an analog, digital, electromagnetic, optical form, which can be seen, displayed and/or heard through a Computer or Electronic System, including but not limited to, writing, sound, images, maps, designs, photos, letters, signs, numbers, access codes, symbols or perforations that can be accessed by those who are able to understand them. The term 'information' is defined as information, statements, ideas, and signs that contain values, messages, data, facts and explanations that can be seen, heard and read that are presented in various packages and formats in accordance with the development of information technology and communication electronically or non-electronically. Meanwhile, the term 'public information' is the information that is generated, stored, managed, sent, and/or received by a public institution related to the organizer and administration in accordance with this law and other information pertaining to the public interest.

From some of the provisions above, it is clear that the term 'data' in Indonesian positive law embodies many terms. In addition, having lots of terminologies could also imply many different meanings. This is certainly a consequence of the different aims and objectives of the legislative arrangements.

Based on the data arrangement in public institutions, the data in public institutions can be divided into two types of data, namely data on public institutions, which are confidential and open. For confidential public institution data, it can be found in the provisions of Law No. 17/2011 and Law No. 14/2008. Open public institution data can be found in Law No. 43/2009 and Law Number 14/2008. Furthermore, it can also be stated that the data of public institutions in Indonesia's positive law are not only produced by public institutions, but also include those that are stored, managed, sent, and/or received by a public institution either by using non-electronic services or electronic services.

Terms and Meanings of Electronic Services in Indonesian Legislation

The importance of drafting legislation on the use of information technology with the convergence paradigm of is important for all aspects. This is not only applied in the formulation of electronic data legislation, but also for the formulation of the electronic service legislation. However, in reality the compilation of the electronic service legislation should be based on the convergence paradigm that still embodies the divergence/sectoral paradigm used. As a result, there are many problems that arise, and if the problem is simplified in terms of terminology, the arranged concepts and substances become different. One of the highlights in this context was when Indonesia compiled legislation on electronic services, and the legal parties still adhered to the divergence/sectoral paradigm. In this regard, it cannot be denied that there are various interpretations of the used terms, concepts and substances about electronic services in Indonesia.

In terms of regulating electronic services to public institutions in Indonesia's positive legal system, Law No. 36/ 1999 concerning electronic services outlines "telecommunications networks." Telecommunication networks are a series of telecommunications equipment that are used in telecommunications. Meanwhile, electronic services in Law Number 32/2002 outlines the term "radio and television broadcasting." Radio broadcasting is interpreted as audio-based mass media, which distributes ideas and information in the form of general and open voices. This medium can broadcast information in the forms of regular and irregular programs. Television, in addition, is interpreted as a media of audio-video mass media, which channel ideas and information in the forms of sound and images in general, both open and closed, in the forms of regular and continuous programs.

The term electronic service is also found in Law No. 11/2008. In Law No. 11/2008, the term electronic service is known as "electronic system." In Article 1 point 5 in Law No. 11/2008, it is stated that electronic systems are a set of electronic devices and procedures that function to prepare, collect, process, analyse, store, display, announce, send, and/or distribute Electronic Information. In the general section, Law No. 11/2008 states: "Electronic systems are computer systems in a broad sense, which do not only include computer hardware and software, but also includes telecommunications networks and/or electronic communication systems. Computer software or programs are a set of instructions that are realized in the form of language, code, schema, or other forms. If this system is combined with media that can be read with a computer, it could enable computers to perform special functions or to achieve special results, including preparation in designing the instruction."

Law No. 11/2008, in its regulation, does not stipulate a certain type of electronic system to carry out public institution activities. This is because Law No. 11/2008 adheres to the principle of neutral technology. However, in Article 16 paragraph (1) Law No. 11/2008, it

has set minimum standards for the operation of electronic systems. The minimum requirements are presented as follows.

1. It should re-display Electronic Information and/or Electronic Documents by invitation;
2. It should protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the Implementation of the Electronic System;
3. It should operate as listed in procedures or instructions in the Implementation of the Electronic System;
4. It should be equipped with procedures or instructions announced with language, information or symbols that can be understood by the parties concerned with the Implementation of the Electronic System; and
5. It should embody a sustainable mechanism to maintain novelty, clarity, and accountability for procedures or instructions.

Law No. 32/2002 concerning broadcasting is burdened with the obligation to fulfil basic broadcasting techniques and technical requirements of broadcasting devices. Further the provisions regarding the basic plan of broadcasting techniques, and the technical requirements of broadcasting equipment, shall be further prepared by the Indonesian Broadcasting Commission with the Government. By understanding electronic service arrangements in the aforementioned laws, several things can be concluded. Firstly, the terms and meanings of electronic services are varied. It becomes the case because the objectives of the statutory regulations are different. Added to this, the scope of electronic service regulations still contains sectoral nuances, where these need to be harmonized and synchronized. Thus, it is expected that these rules can be applied effectively. Lastly, institutions that regulate electronic services also tend to be carried out separately. It has been regulated in Law No. 36/1999 known as the Regulatory Body, and in Law No. 32/2002 known as Indonesian Broadcasting Commission, while it has not been regulated in Law No. 11/2008.

Research Methods

This study employs normative legal research methods based on the applicable rules or norms related to data and electronic services in Indonesia. To conduct normative legal research, the data is in the form of primary legal materials which comprise (1) Law No. 43/2009 concerning Archives; (2) Law No. 17/2011 concerning State Intelligence; (3) Law No. 11/2008 concerning Information and Electronic Transactions; (4) Law No. 14/2014 concerning Public Information Openness; (5) Law No. 36/1999 concerning Telecommunications; and (6) Law No. 32/2002 concerning Broadcasting. Secondary legal materials include books, journals, reports and articles that are relevant to the field of study, while tertiary legal materials in the form of dictionaries were used.

Identification of Problems in Data Management and Electronic Services in Indonesian Public Institutions

After understanding the arrangement of data and electronic services to public institutions in Indonesia, it can be revealed that the macro-regulation is a government effort to respond to the development of the use of information technology. In addition, this responsive effort is also micro-related to security and legal certainty on the use of information technology, media and communication. Therefore, there are three approaches to ensure safety and security in cyber space, namely the approach of legal aspects, technological aspects, social, cultural and ethical aspects. To overcome the security problems in electronic system, the legal approach is of importance because the issue of the use of information technology could not be optimal without legal certainty.

When paying attention to the arrangement of electronic data and services to public bodies in Indonesia, several problems can be found, namely; First, the laws and regulations in Indonesia have regulated data on public bodies, but data on the public body itself in fact has many terms and meanings. Several terms and meanings do not follow the arrangement of data in a public institution in a structured manner, so this is sometimes only understood in the legislation context, while it is not necessarily understood equally for other legal contexts. For example, the provisions in Law No. 17/2011 stated that: the data interpreted as information does not have detailed explanation; while the data as information is described in detail in the Law No. 14/2008. Then, it can be inferred that information in Law No. 14/2008 was used as a basis for explaining information in Law No. 17/2011. If this is also the case, it will be difficult for people who are bound to the statutory to easily understand this practice. Secondly, the data regulation on Indonesian public institutions are still sectoral and subtle. For example, data related to archives is only intended for archiving, and data related to the public information disclosure is only intended for the benefit of public information disclosure. The problem related to the nature of data regulation on public bodies becomes irrelevant if it is contextualized with the progress of information technology is known for having a tendency to push in a convergent direction rather than towards divergence. With this direction, data on public institutions resulted from various sectors will also experience changes, so the regulation should reach data from various sectors and this process surely involves synchronization.

Indonesian legislation has distinguished open and confidential data both conventionally and electronically, but this distinction has not yet led to a comprehensive understanding. For example, confidential data seems to be interpreted as limited types of data, such as intelligence and personal data protection. Before being defined as such, there is a general explanation of what is meant by confidential data. Also, institutional management in

Indonesian laws and regulation are carried out through different institutions. This might become inappropriate if data development currently heads towards converging data itself. Besides, a rule related to data exchange between institutions and the State has not yet established in data regulation in Indonesian legislation. Hence, this would be very vulnerable to data misuse on public institutions.

Furthermore, related to the regulation of electronic services for public institutions, the Indonesian government only regulates a series of electronic devices and procedures, although the progress of electronic systems has developed rapidly. Such rapid technological development has also given a rise to convergent new services that are not only limited to the scope of telecommunications, but have expanded to the direction of media (broadcasting) and informatics which in Indonesia is abbreviated as Telematics. Based on the Telematics Convergence Law Draft, radio and television broadcast services are no longer the domain of broadcasters, but can provide telecommunication service customers with existing networks and access using telecommunications (terminal) devices.

The Telematics Convergence Law Draft also states that the development of telematics requires a unification of regulations and policies, with the intention to harmonize or not even separate the rules/laws regarding telecommunications and broadcasting. The push for an open market has changed the order of telematics activities from monopoly to competition. These changes must be addressed wisely and there is a need for the relevant infrastructure support. The role of the regulators is "independent", which implies that they are free from the interests of any party except national and public interests. They should be credible and authoritative so they could act as a good regulator and referee.

Cases of Data Abuse and Electronic Services in Indonesian Public Institutions

With the identification of various legal issues in the regulation of electronic data and services for public institutions, this has led to further implications for its implementation. Various cases have emerged in the community related to data and electronic services.

The first case happened on October 12, 2012, when there was a fraud case committed by Indonesian citizens against US citizens through online sales. In this case, the perpetrator uses the website www.audiogone.com which contained product advertisements. Then, the US citizen contacted the Indonesian via email to purchase the item, and an agreement took place between the two parties. Payment was made by transferring funds using a credit card into one of the American banks. In the settlement, the transaction was not going well, because the American citizen could not claim the payment since his credit card number did not belong to Indonesian citizens. Therefore, the Indonesian citizens felt cheated. In this case the Indonesian citizens used other people's ID cards and TIN.

Secondly, on March 6, 2013, based on the results of analysis and sharing between banks, it was known that the initial data theft was suspected. Data theft was carried out by a store merchant in two Jakarta malls. Data theft in this case had spread to the United States, Mexico, the Philippines, Turkey, Malaysia, Thailand and India. In this case, a number of banks had blocked the affected cards.

Third, during the time January - March 2013, there had been cases of fraud. The fraud began with buying and selling cheap gadgets online offered through the site www.gudangblackmarket008.com. The perpetrator asked the victim to transfer money for the product offered, but after the money is transferred, the offender did not send any of the advertised items to the victim. Two perpetrators were arrested in Medan by the police. One of the perpetrators served as the website operator, while the other perpetrator acted as a fund collector.

Fourth, on 18 December 2017 there was an electronic data theft case in Jakarta. In this case, the Metro Jaya Regional Police were successful in apprehending nine foreigners and three Indonesian citizens on several cases of forgery, theft, as well as theft of electronic data, with evidence of various debit cards, hundreds of millions of dollars, and several skimming devices.

Fifth, on January 31, 2018 there were cases of data misuse by 12 perpetrators. They registered as online taxi drivers, then they rooted the software on their cell phones in order to manipulate the information data. They controlled the grab system as if the perpetrator was carrying out or picking up the customer when it was fake.

Sixth, on April 5, 2018 there was an abuse of Facebook personal data related to Cambridge analytics, and data from around one million Indonesians were leaked. The misused personal data was obtained from quiz applications that allowed third parties to get personal data from Facebook users. In this case, the Ministry of Communication and Information has written a warning to the Facebook representative.

Electronic Data and Service Regulations for Indonesian Public Institutions: A Proposed Future

Various legal problems arise in terms of data management and electronic services for public institutions. The cases of data misuse also emerged. This phenomenon certainly requires the government to be more progressive in managing various types of electronic data and services in public institutions. The regulation of electronic data and services on public institutions

should be able to be comprehensively carried out. They should also be able to anticipate development from electronic data and services to rapidly expand public institutions.

In the global context, the arrangement of data and electronic services leads to the specific role of the government in managing data on public institutions, comprising both confidential and open data. That data was created, stored, used and received by utilizing information technology, which was collected from various sources, and had a tendency towards converging data on public institutions. Even with the government's role in managing data in public institutions, these institutions can produce significant productivity in creating data, especially if the government actively uses big data. This is as stated by Manyika and Kim, Trimi, & Chung. Manyika et al. (year) stated that the public sector can boost productivity by actively using Big Data, while Kim, Trimi, & Chung stated that big data offers the solutions for many public-sector problems, such as enhancing efficiency and productivity, transparency and well-being (Fredriksson, et al., 2001).

By focusing on the role of government, it constructs a concept known as Open Government Data. Open Government Data is "information contained in government databases and private servers that can be freely accessed, used and published by people and businesses" (The Economic Strategic Unit (ESU), 2019). In Germany, Open Government Data is defined as the data which is available to third parties for their reuse. The provided data can be described as open due to various factors, such as accessibility, formats and the legal conditions under which data may be used (Federal Ministry of the Interior (FMOI), 2012).

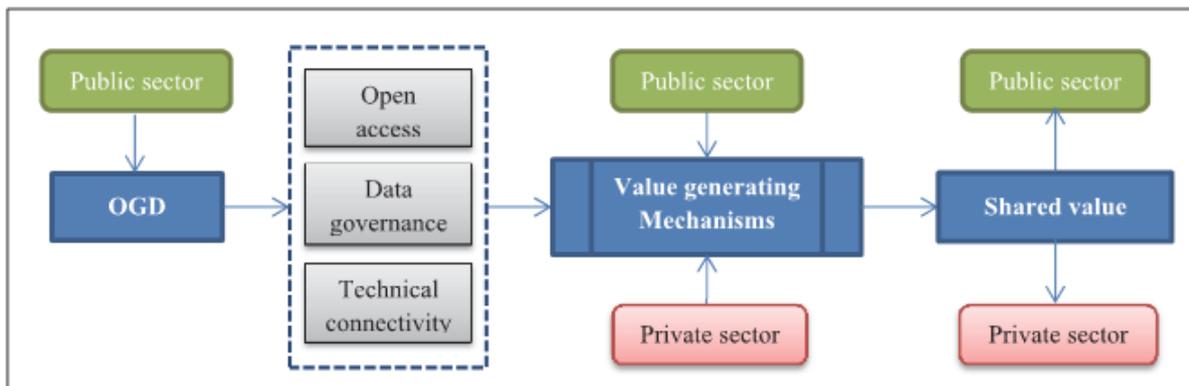
Gonzalez-Zapata & Heeks suggests that Open Government Data is attributed to three perspectives, namely Government Data, Open Government and Open Data (Kumar; 2018). Government Data are collectors and generate a large amount of data and datasets. These datasets contain welfare payment data, social welfare scheme impacts, unique identification data, and other types of data related to public services. Open Government is a government that shows a tendency of governance by opening their maximum data in forms of open data. Openness aspects also involve a more civilized and transparent passing right to information acts. Open Data, meanwhile, is a matter of overcoming barriers to accessibility through uniformity which concerns the way the data are captured, stored, processed, and resulted. Open data is any data that can be freely used, reused and redistributed by anyone (Kumar; 2018).

Open Government Data is used to help community to better understand what the government is doing and how well they perform, thus making it accountable for deciding whether or not they achieve good results (Ubaldi, 2018). Open Government Data can be divided into two categories, namely (1) Government data, which consists of any data and information produced or commissioned by public institutions; and (2) Open Data, which can be used

freely, reused, and distributed by anyone. This is only subject to the requirements by which the user connects data and makes their work available for redistribution (Ubaldi, 2018).

In order to define and provide Open Government Data, technical connectivity is needed by giving adequate infrastructure, including electronic services owned by the government. Linkages to Open Government Data with technical connectivity can be seen as described by Jetzek (2013) below.

Figure 1. OGD value generating ecosystem



According to Jetzek (2013), technical connectivity in Open Government Data is conceptualized as a technical infrastructure that provides the public sector with open data experimenting. It provides users with data access through technology which allows them to transform data into something valuable, such as knowledge, services or products (Jezek, 2013).

In the context of Open Government, this data has produced two different points of view, namely data re-use perspective and Open Government perspective. In the data re-use perspective, the focus is on economic value from government data, while the Open Government perspective focuses on how the use of Open Government Data can contribute social values for generation in collaborative settings. With the existence of two perspectives in terms of Open Government Data, Open Government Data discourse itself is very influential. However, if two different perspectives in terms of Open Government Data are synergized in terms of government data management, it could have an impact.

According to the Bureau of Communications Research Australia there are two advantages of Open Government Data, namely direct benefit and indirect benefit. Direct benefits, with Open Government Data, can encourage the development of new services carried out by businessmen, government and society. Some of the new services include efforts to create



jobs, encourage entrepreneurship climate and contribute to the country's opinion with new service development (Bureau of Communications Research (BCR), 2016).

For example, the US Government released a GPS (global positioning system) in the 1980's. Originally used for military and defence, GPS became publicly available. It paved the way for various innovation from the private sector such as precision crop farming and navigation systems. Fast forward to 2011 and beyond, there are more than 3 million jobs now relying on GPS technology. Taking into account the equipment sale and commercial applications, the GPS industry has contributed direct economic benefits for the US economy which is estimated at between \$91.2 billion and \$165 billion per year (BCR, 2016).

Regarding the indirect benefit with Open Government Data, it can empower communities and improve government services. Some indirect benefits in several countries have been presented as follows (BCR, 2016).

a. Improving government services.

Open government data entailed power to revolutionize government services, especially in the digital age where technological change is constantly constant. The US Government Blue Button Initiative (<http://bluebuttonconnector.healthit.gov/>) gives millions of Americans an access to their own health information by downloading it electronically, for use and re-use.

b. Providing a more efficient operation and improving business practices

Various initiatives have been established by the Government of India's Ministry of Tourism to encourage local and international tourists to visit India. There are several challenges for tourist to visit some areas in India, including geographical distance, tourist destinations, cultural diversity, access to local food, accommodation, transportation and personal safety. The GoTourist application uses business intelligence analysis to identify trends and predict tourist behaviour and feedback mechanisms that collect user views. It also provides the government with real-time responses about the quality of services offered by providers. The data obtained from the platform helps government to develop, improve, and implement solutions to the challenges.

c. Improving information exchange

Citizens can see, monitor and analyse how their taxes are spent by the UK government through the website platform at <http://wheredoesmymoneygo.org/>. Users can view national and regional expenditures for services including health, defence, education, order and safety, environment and general government.

d. Improving policy and planning

Melbourne has begun publishing data on light, humidity and temperature levels online as part of its efforts to study the impact of canopy cover on urban cooling. An open data product called Urban Forest aims to develop new systems that can help the city administrators to monitor, understand, and interpret real-time information from the urban environment remotely. The data can be used to advise local government planning decisions regarding diversity and equity.

Karakiza (2014) stated that new technologies and social media can change the communication style between government and the citizens. They contribute decisively for transformation of public administration towards a new and open format that is characterized by 1) active participation of citizens in public affairs, 2) close collaboration among public services, government, and citizens, and c) transparency of the State activities (Karakiza, 2014).

From understanding the concept of open government data and technical connectivity, data and electronic services on public institutions is an essential element to be optimized in Indonesia. The importance of electronic data and services for public institutions is also due to many values that will be generated if this can be optimized in Indonesia. Hence, the Indonesian government should immediately do three things, which are establishing the legal protection regarding convergence telematics; establishing legal protection regarding data protection; and renewal of laws and regulations concerning recent electronic data and services to public institutions.

The need for the establishment of legal protection regarding convergence telematics emerges for several reasons. Firstly, the trend of using technology, which includes providing electronic services, has led to convergence telematics (telecommunications, media and informatics). It is where telematics becomes one of the important infrastructures in order to support economic, educational, health, defence, national security and international relations. In addition, there is a telematics paradigm, which states that electronic services could have strategic values and could control livelihoods and thus, become tradable commodities. On the other hand, the national government commonly controls over telematics. They hold the beliefs that electronic services should be maintained because telematics is closely related to, but not limited to, the use of radio frequency, numbering, satellite orbit slots. These resources belong to limited and non-renewable natural resources.

The need for legislation data protection is based on several reasons. Data is a strategic and vital instrument in the context of digital society. Data can be provided abundantly and can be utilized for the development of a nation. Abundantly available data have a certain level of vulnerability which in the end can lead to illegal actions and even cause national losses. Therefore, guarantees of security and safety should be realized through the establishment of

legislation data protection. Data security guarantee is largely determined by information technology security. According to Icove, IT security weaknesses based on security holes can be classified into four main parts, namely (1) physical security; (2) personal security; (3) security of data, media, and communication techniques; and (4) management security (Warno and Iffano, 2009).

To be able to optimize the regulation of electronic data and services, these two laws are ratified. The second position of the legislation should be used as a legal protection in terms of data and electronic service regulation. After occupying both as legal protection in the context of electronic data and services, the next step entails renewing the existing legislation. This renewal is in an effort to synchronize laws with legal protection in terms of promoting convergence telematics and data protection. Synchronization itself intends to enable the legal protection to become a reference for all of the legislation products that have previously been established. If the established laws and regulations are not in accordance with the legal protection, then the consequences must be declared null and void. However, if the legal protection does not contrast the established regulation then these regulations can continue to be enforced. This is in line with the principle which proposes *Lex superior legal adagium derogat legi inferiori*, or higher law defeats lower law.

By taking the three steps outlined above, the hope of having electronic data and service arrangements for effective, efficient and structured public institutions can truly be realized. Attempts to minimize law violations related to the use of information technology, specifically data misuse, can be performed well. In addition, this arrangement allows officials to provide convenience to law enforcement for all kinds of crimes related to the use of information technology.

Conclusion

Data and electronic service legislation on public institutions in relation to the use of information technology should be prepared based on the convergence paradigm. This is carried out by considering the characteristics of information technology itself, which now leads to a pattern of convergence as opposed to divergence/sectoral paradigm. Indonesia is a country that has concerns over the regulation of electronic data and services in terms of the use of information technology. Public institutions have enacted several laws and regulations that are based on the divergence paradigm. As a result, this situation has caused a number of problems. The problems are related to terminologies, concepts and substances which are regulated diversely. This is no exception in interpreting data and electronic services. Based on this reality, Indonesia really needs special efforts to solve the electronic data and service problems. Meanwhile, the efforts that can be made are immediately establishing a legal protection regarding telematics convergence; and immediately establishing legal protection



regarding data protection; and searching for updates to ratify the legislation on telematics convergence and data protection. After the ratification, the synchronization between laws and regulations related to electronic data and services is carried out in the current public institution, this is either existed or enforced by the legislation on telematics convergence and data protection which is located as the legal umbrella. With these three steps, the regulation and law enforcement on electronic data and services in public bodies can be realized well and easily.



BIBLIOGRAPHY

- Barbara Ubaldi. (2018). Open Government Data Empirical Toward Analysis of the Open Government Data Initiative. *OECD Working Papers on Public Governance*, No. 22, OECD. accessed <http://dx.doi.org/10.1787/5k46bj4f03s7-en> on October 16.
- Bureau of Communications Research. (2016). Open government data and why it matters. *A Critical Review of Studies on the Economic Impact of Open Government Data*.
- Braumer and Poindexter. (2002). *Cyberlaw and E-Commerce*, New York: McGraw-Hill.
- Cecilia Fredriksson, et al. (2001). "Big Data in the Public Sector: A Systematic Literature Review," *Scandinavian Journal of Public Administration* 21 (3).
- Federal Ministry of Interior. (2012). *Open Government Data Germany*. Berlin, July 2012.
- Maria Karakiza. (2014). The impact of Social Media in the Public Sector. *Procedia - Social and Behavioral Sciences* 175 (2015), 384 – 392.
- Molly Land. (2013). Toward an International Law of the Internet. *Harvard International Law Journal / Vol. 54 Number 2, Summer 2013, 1*.
- Nora C Porter. (2000). *Technology is A Double-Edged Sword*, Pennsylvania Bar Association.
- Riyanarto Warno and Irsyat Iffano. (2009). *Information Security Management System*, Surabaya: ITS Press.
- Sharif N As-Saber, et al. (2006). Information Technology Law and E-government: A Developing Country Perspective. *JOAAG, Vol. 1. No. 1*.
- Thorhildur Jetzek. (2013). The Value of Open Government Data. in *the NR Perspective* 23.
- Suharso and Ana Retnoningsih. (2009). *Big Dictionary of Indonesian Language*, Semarang: CV. Widya Karya.
- The Economist Intelligence Unit. (2019). Open Government Data: Assessing demand around the world. *Research Report*, sponsored by the Government Technology Agency of Singapore.
- Vinit Kumar. (2018). Open Government Data Initiatives: a comparison of India and China. Available from:



https://www.researchgate.net/publication/305768855_Open_Government_Data_Initiatives_a_comparison_of_India_and_China [accessed Oct 16 2018]

Valentina (Dardha) Ndou. (2004). E - Government for Developing Countries: Opportunities and Challenges. *The Electronic Journal on Information Systems in Developing Countries (EJISDC)* 18, 1.

Yusron Isnaeni. (2009). *Copyright and its Challenges in the Cyberspace Era*, Jakarta: Ghalia Indonesia.

Law Number 36 of 1999 concerning Telecommunications

Law Number 11 of 2008 concerning Information and Electronic Transactions

Law Number 32 of 2002 concerning Broadcasting.

Law Number 43 of 2009 concerning Archives

Law Number 17 of 2011 concerning State Intelligence

Law Number 14 of 2014 concerning Public Information Openness

Telematics Convergence Law Draft