DATA PRIVACY LAW IN THE APPLICATION OF SMART CITY IN INDONESIA

Sinta Dewi Rosadi, Padjajaran University
Suhardi, Bandung Institute of Technology
Samuel Andi Kristyan, Bandung Institute of Technology

ABSTRACT

Smart cities have the ability to transform data of the physical world into data in the cyber world and monitor it in real time, also contribute to intelligent services for users in terms of entertainment, transportation, and health care, the environment and energy. However, concerns arise about the security, because intelligent city apps not only collect sensitive information from people and their environments, but also affect people's lives. One of the main challenges on the smart city application is the privacy where the smart city infrastructure enables to monitor and surveillance a massive data that can share, process, generate, and analyse large amounts of personal data such as their geo location, characteristics, activities and if it links this data together, it could create profiles or people that against their privacy right. The result is found that in the application of smart city in Indonesia, data privacy is still at stake since Indonesia has not yet had a specific data privacy law that will provide maximum protection.

Keywords: Smart City, Privacy Challenges, Application.

INTRODUCTION

Smart cities concept has been evolving for decades and helping city leader to utilize the information technology to provide a better service and ensure that citizen get to increase their quality of life. Like many cities around the world, smart city has become a trend in Indonesia and is seeking to become a smart city that utilizes the information and communications technology (ICT). The main goal of smart cities is to improve the lives of the citizen and manage city resources in addition to provide better services for communities, improve the governance, provide better service delivery, create more resilient and critical infrastructure for better community mobility, crime prevention and traffic control. According to Datafloq report from "*The Benefits of Becoming a Smart City*", "*smart cities are becoming necessary due to the world's growing populations is moving to urban centers and currently the world is home to 7,1 billion people and by 2025, it will grow to 8 billion*" (Willis, 2015). The population of Indonesia is projected to increase to 271.1 million in 2020 and increase again to 305.6 million by 2035 (Sub directorate of Statistical Demographic, 2013). With the same research from Sub directorate of Statistical Demographic (2013), the population of urbanization is predicted reaching 5 billion, this means reach 60 percent from total world population. Indonesia's level of urbanization will reach 66.6 percent in the year 2035 for several provinces especially in Java and Bali, which their level of urbanization are higher than the other province. Given these conditions that show majority population living in urban environment, the concept of smart city in Indonesia is needed to establish the growing demand for efficiency and resources, thus the concept of smart city emerges as the management model of cities (Gamero, 2012). It is urgent to improve the concept

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

of smart cities in Indonesia to foster increasing demand for efficiency and resources. Smart cities can also take many advantages from technology, such as big data analysis, cyber-physical-system, IoT and real time control to support intelligent services. Smart city is also able to integrate various sensors, RFID, and other wearable devices that are used as real time monitoring and sensing which then transmit data over heterogeneous network to be processed on cloud servers then it can be reused in the real world in order to improve the quality of user service. Once the city becomes smart, people may face security and privacy because of the intelligent city app vulnerabilities. For example, an attacker can manipulate the resulting data or perform denial-of-service that can make the smart city lose its paradigm or interfere with sensing and transmitting so as to degrade the service quality. In addition, CCTV in some cities can also be used by the attacker to collect the information about the area of a house or track the path of a person in travel. Without security protection and privacy, the public may be holding back for using smart city application.

Beside many advantages, smart cities also pose challenges, one of them is privacy due to minimum understanding of privacy from the local government and businesses considering they collect and process personal data without providing community with the opportunity and mechanism for consent. The main purpose of this paper is to analyze and explore what are the privacy challenges in smart cities in Indonesia and how far is the privacy expectation in Indonesia.

RESEARCH METHODOLOGY

The methodological foundation in this study is normative juridical conducted by tracing and analyzing literatures and documents related to the substance of the research (Soekanto & Mamudji, 2004). The research specification that used is analytical descriptive due to the intention of the research to provide a detailed, systematic, and comprehensive description of the impact of smart city application to data privacy (Soemitro & Hanitijo, 1983). The data collection technique that used is literature studies, which collects data and conducts research on the literature and documents that are closely related to the protection of data privacy. The data analysis method used in this study is qualitative juridical analysis, which is an analysis that emphasizes more on the process of deductive and inductive conclusions and the analysis of the relationship of the phenomena faced by using scientific logic with the assistance of legal interpretation methods.

Smart Cities Application

Many intelligent applications appear when the intelligent City paradigm is gaining popularity that serves to connect the real world with the cyber world. Smart city applications bring benefits to cities and communities in various aspects such as environment, living, energy, industry, and services. Here are the main applications on smart city (Martinez-Balleste et al., 2013) (Figure 1):

1. Smart energy: utilizing various sensors to monitor energy distribution, energy generation, energy transmission and also energy consumptions. From this application is expected user not only reduce energy consumption in various aspect but also reduce the failure of energy use.
2. Smart industry: this application uses a variety of sensors to support the industry such as optimizing production and distribution so as to reduce the consumption of materials and resources.

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

3. Smart environment: using a variety of sensors to monitor waste gas, noise, forest conditions, greenhouses, air and water pollution, and so on. This app is built to support a user-friendly environment.
4. Smart living: This application uses a variety of sensors to support the creation of comfortable homes and homes by controlling household appliances tailored to the climate, for energy saving as well as for surveillance, entertainment and education.
5. Smart service: This application uses a variety of sensors to combine public facilities with public services to be useful directly to users, such as the use of intelligent transmission so that users can avoid traffic congestion or manage travel planning and so on .

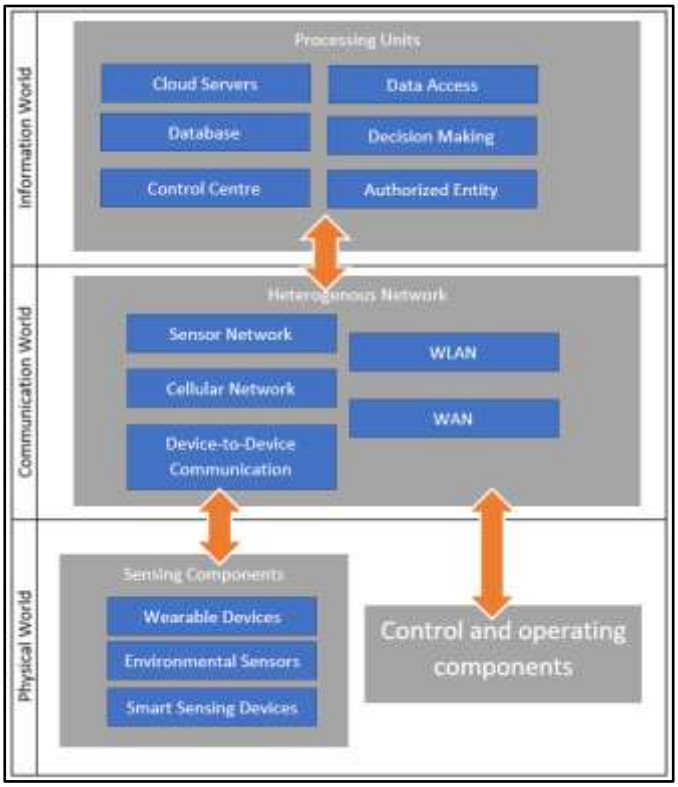

FIGURE 1
SMART CITY ARCHITECTURE

While to achieve a good city management, smart city transforms data in the real world to the world of information to be processed and provide information on intelligent services. Retrieving the scheme of "*Architecture for smart city: physical world, communication world, and information world*" from Zhang, et al., (2017), some of the components of the smart city builder are:

1. Sensing components: The Bridge that connects the information world with the physical world. This component uses sensors, smart devices and wearable devices to capture information from the physical world and send it to the processing unit for intelligent services.
2. Heterogenous network: With the existence of various sensing devices and also how to collect different information then it takes a heterogeneous network in support of smart city. Heterogeneous networks combine Device-to-device communications, cellular networks, sensor networks, wireless networks (WLANs), WAN networks, and so on. So heterogeneous network represents smart city communication that connects information world and physical world.

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

3. Processing units: These components utilize in cloud computing servers, varied data sensing, and system controls to analyse and process the sensing information collected from the physical world for intelligent services.
4. Control and operation component: This component utilizes data manipulation in the physical world which aims at data optimization for processing units so can reach good quality of service that can be provided in smart cities.

Personal Data Protection in Smart City Application in Indonesia

In practice, cities will often have no alternative but to collect significant amount of data about the city's citizen personal data or identifiable information if they are going to become "*smarter*" (Hiller & Blanke, 2016; Woo, 2017; Young, 1989). Therefore, smart city apps have some challenges in terms of privacy and security (Ismagilova et al., 2020). Data in intelligent city applications should be able to withstand modification, disruption, inspection, unauthorized access, disclosure, and annihilation. Smart cities will collect a significant amount of data about city residents; they need to in order to carry out their "*smart*" functions. In order to gather these data, many smart cities rely on the internet of things (IoT):

Smart cities should also use basic security and privacy requirements that include confidentiality, integrity, availability, nonrepudiation, access control, and privacy that several national and international organizations have identified privacy as a key policy, regulatory and legislation challenge of the 21st century (Zoonen, 2016; Zhang et al., 2013).

Smart city data is vulnerable to information leakage because collected data is sent and processed through the network. This data can be the information about identity, health condition, user location, lifestyle, home condition and so on. To maintain the privacy of the user during data sensing, some security techniques can be applied such as encryption, anonymity and access control. However, some personal information may be inadvertently opened to untrusted entities. For example, CCTVs can point to the life, day-to-day style of the resident population, although the CCTV was originally designed to monitor criminal behavior in the real world as well as in the cyberspace. Another example of such a smart home, an attacker can use the data from CCTV to gain personal information and monitor the condition around the house although the purpose of this CCTV installation is to monitor the theft and abnormal events around the house. Almost most of the privacy and security protections that are developed aim against outside wiretaps and attacks. But there are also unanticipated inner security potentials such as security guards and employees, who can access data records like surveillance records to steal user data or allow loopholes for outside attackers to enter. In addition, smart city data has a detailed and diverse scale so that privacy requirements have different types of requirements as well. In addition, smart cities also have the ability to process and store information in the cloud server, but it also faces the threat of security because the cloud server cannot be trusted. Several national and international organizations have identified privacy as a key policy, regulatory and legislation challenge of the 21st century (Zoonen, 2016)

According to Warren & Brandeis who published a seminal idea about privacy in Harvard Law Review, at the first time express their opinion that there is a right that has to be recognized and protected by the law, it is "*the right to privacy*" as a result of technological development that caused a great harm for people's comfort and since then the right of privacy always referred to the "*right to be let alone*" as one of the most important and significant chapter in the history of privacy law where for the first time privacy has been recognize as a legal right that needs to protected by the law. The privacy concept was recognized due to the recent invention of

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

instantaneous photograph and newspaper enterprise have interfere the private and domestic life, and the law should grant any redress for the invention of privacy (Warren & Brandheis, 1890; Solove & Schwartz, 2006). Later on, this concept is established to the data privacy law that applies where personal data is subjected to certain forms of processing personal data (Lloyd, 2008), and everyone has the right to decide whether they will to exchange or share their personal information and also, they are entitled to specify what conditions to do so. Lloyd (2008) found that data privacy laws generally combine protection that protects the use of personal data and the subject to regulatory framework and individual or data subject that have the right under personal data law to claim if the processing of their personal data against basic principles which is common under global privacy standards. Alan Westin for the first time define privacy as the right of the individual to decide under what circumstances and to what extent their personal data will be exposed to other and his theory is named as information privacy or data privacy (Bainbridge, 2008). After Westin, people divided privacy into several facets (Westin, 1986; see also Banisar & Davies, 1999; Munir et al., 2014):

1. Since the concept of privacy established, it is always conflict with the advantages in technology. Many technologies Information/data privacy, involves establishing rules governing the handling, processing and collecting of personal data.
2. Bodily privacy, is concerning protection of people's physical conditions against invasive procedure; Bodily privacy, concerning about the physical protection of people's conditions against invasive procedure;
3. Privacy of Communications, concerning the protection and respecting personal communications;
4. Territorial privacy, concerning the setting of limit on intrusion into home or people's workplace.

That enables new forms of monitoring and recording and have often led to concerns about the impact on privacy such as technology on Smart city that creates several of potential privacy harms that also raises significant challenges to existing approaches to protecting privacy due to the capture of personal data about people and places that potential for violating privacy namely (Munir et al., 2014):

1. Indiscriminate individuals due to the increase amount of personal information that can be gathered and stored.
2. The information can be distributed across multiple devices, services and places.
3. That could easily process data flow across platforms, devices and services.
4. Data will be generated regularly and automatically (Munir & Yasin, 2002).

According to Kitchin (2016), several international legal instruments in the form of conventions, guidelines, established internationally recognized data privacy principles that have laid the foundation of most modern national Data Privacy laws such as OECD's 1980 Privacy Guidelines, The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981 that has been used as a model to regulate the data privacy in many jurisdictions.

The Guidelines has defined personal data as "*any information relating to an identified or identifiable individual*"; an identifiable person is one who can be identified, directly or indirectly, especially those referring to identification numbers or other factors specific to their social identities, mental, physical, cultural, economic, or physiological (Privacy International, 2013).

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

According to Graham Greenleaf the Guidelines (2014), were an early influence of the development data privacy law in Asia. The Guidelines is voluntary and not legally binding. However, it recognized by many countries as the basis of norms governing data privacy both by the government and private companies. This Guidelines explain that personal data as a data that relating to an identified or identifiable person. However, what exactly the type of personal data is according to many interpretations but the main point is the data that connected to individuals that will be protected either by data itself or combined with other information. The scope of data privacy such as a person's name when combined with other information about them, such as their address, sex, age, education, or medical history. These examples are not exhaustive and many other kinds of information may still qualify as personal information.

The Guidelines establish that the following principles should be adopted as a main principle to the processing of personal data:

1. The collection of personal data should be limited: One of the key elements of data privacy principles that the processing of personal data should be limited to the collection of personal data and the obtaining and processing of personal data should be conducted in lawful and fair means. These principles placed consent as an important mechanism to limit the collection of personal data.
2. Data quality principles have put an obligation to the institution that the data should be relevant and not harmful for the data subject due to the lack of accuracy, completeness and must be updated with the current information.
3. The data must be according to the purpose of specification: These principles have mandated that the purposes of collecting and processing personal data should be determined as well as the use of personal data should be limited to those specifications.
4. Use limitation: Data should not be disclosed, become available or used for another purpose than those specified except a) with the consent of the individual or b) by the authority of law.
5. Security safeguards: The rules on the security obligated the data processor and data controller to implement appropriate technical measures against accidental lost, modification, use, disclosure or destruction.
6. Openness: Both the data controller and data processor must provide a general policy that depict how far that organization used personal data and how privacy is protected. These principles will help the organization to build trust from the data subject.
7. Individual participation: In big data era this principle is very important and it give a right of the data subject that the right to access and rectification of their personal data.
8. Accountability: The principles of accountability will show how far the organization is being responsible to implement privacy protection and they have to be able to demonstrate the compliances to these principles.

Many multinational companies abide by these data protection principles as a way of ensuring minimum compliance in jurisdictions where Data Protection Laws either do not offer stringent enough protections or do not exist (Kitchin, 2016).

Existing Law

In Indonesian legal system, there is no specific regulation concerning data privacy. The initiative to provide protection upon privacy and data privacy is derived from the Human Rights Rules under the Constitution. This is also driven by the influence of information technology development where most of the Indonesian people have accessed and learned that their privacy will be in jeopardize, and also because there are so many advertising practices that collect data

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

privacy without clear regulations. Furthermore, the significant driving factor is the strong international and regional obligation either politically, economically as well as legal cooperation, since Indonesia has a strategic position in international trade, including electronic trade. Therefore, the legal basis to establish a law on data privacy in Indonesia can be drawn from several sources:

Privacy and Data Protection according to the Constitution of 1945

Similar with several other countries, Indonesia perceives privacy as a part of human rights. The Indonesian Constitution of 1945, which is the primary source of laws, does not explicitly mention privacy and protection of data privacy, but recommends protecting human rights. The Preamble of said Constitution states that human rights are the national goals and one of the goals is to protect all citizens and achieve prosperity based on peace, social justice and freedom. Furthermore, data privacy concept is elaborated in the Amendment to the Constitution of 1945, articles 28F and 28G. Even these articles do not directly mention the privacy and data protection, but it can be considered as a legal basis for regulation on the matter. Although the articles have not been applied directly in the regulation in Indonesia, but there is no doubt that the articles are concerned with human dignity as a human right.

Privacy and Data Protection according to the Provisions on the Human Rights

Indonesia adopted UDHR through its National Act No.39 of 1999 concerning Human Rights (UU 39/1999) which also reiterates the right to privacy. Article 31 and 32 of this Act states that no one shall be subjected to arbitrary interference with his home and with his correspondence. Enacting this Act is an evidence that Indonesia has a moral and legal responsibility to execute, respect, and uphold the Universal Declaration on Human Rights agreed by the members of the United Nations, and several other international instruments concerning human rights ratified by the Republic of Indonesia. In the case of violations of Article 31 and 32 of UU.39/1999, it provides a mediation settlement conducted by National Commission of Human Rights (The role of National Commission of Human Rights as mediator on human rights issue can be seen in Article 76, Article 90 to 99 of UU 39/1999). Concerning with issues of data, Human Rights Law (UU 39/1999) provides Article 12, which states that every person is entitled to the protection of their personal development such as to get educations, improving human life and gain a prosperous life.

Based on the above-mentioned articles, it seems that Indonesia seeks to protect human rights, but there is no particular concern about data privacy and communication actually most closely describes the relationship between human rights to data privacy. Article 14 of Human Rights Act (UU 39/1999) states:

"(1) Every person has the right to communicate and obtain information".

Article 21 of the Human Rights Act states:

"Every person has the right to personal integrity, both spiritual and physical. And therefore, there can be no object of research without consent from him".

Article 29 states:

"(1) Every person has the right to protection of self-personal, family, honors, dignity, and his property.

(2) Every person has the right to recognition as a person before the law wherever he is".

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

Data Privacy in Electronic Transactions Law

The utilization of ICT and the growth of internet user in Indonesia led to the Enactment of Electronic Information and Transactions Law No. 11 of 2008 (the "EIT Law"). In Indonesia, up to the date of this publication there is no general law on data protection. However, there are certain regulations relating to the use of electronic data. The primary sources of the management of electronic information and transaction is EIT Law that stipulates in Article 26 paragraph (1) prohibits the use of information acquired through electronic media containing data privacy related to an individual without the consent of such person. The EIT Law further provides that anyone deliberately and without having valid rights shall be prohibited from changing, adding, reducing, transmitting, destroying, eliminating, transferring personal data. The elucidation of this article provides that the protection of personal data is a part of privacy rights, and defines privacy rights to encompass the following:

1. The right to enjoy a private life, free of any disturbance;
2. The right to communicate with other people without any espionage; and
3. The right to monitor the access of information about a person's personal life and data.

The EIT Law then amended by the Law No. 19 of 2016 regarding the Amendment of EIT Law ("EIT Law Amendment") on Article 26, Government Regulation No. 71 of 2019 on Article 14 regarding Provisions of Electronic systems and Transaction ("Reg. 71") and its implementing regulation, Minister of Communications & Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System (MOCI Regulation of Protection of Personal Data in an Electronic System, 2016).

CONCLUSION

This paper concludes that benefit of smart city applications that is very important to offer solution to improve the urban living conditions it will conflict with data privacy since the application will collect, process and storage a wide range personal data in real time. Personal data is protected under the regime of data privacy law that has a legal right and regulated and controlled both by international and national instrument. Indonesia has yet to find the regulation approach to ensure data privacy protection.

REFERENCES

Bainbridge, D.I. (2008). *Introduction to information technology law*. Pearson Education.

Banisar, D., & Davies, S. (1999). Privacy and Human Rights, An International Survey of Privacy Laws and Developments. *The John Marshall Journal of Computer & Information Law, XVIII.* Retreived from: https://www.researchgate.net/publication/242448871_Privacy_human_rights-an_international_survey_of_privacy_laws_and_developments

European Parliament and of the Council Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281*.

Gamero, R. (2012). *Why do we need Smart Cities?* Public Policy. https://www.telefonica.com/en/web/public-policy/blog/article/-/blogs/why-do-we-need-smart-cities-

Greenleaf, G. (2014). Asian Data Privacy Laws: Trade & Human Rights Perspectives (Reprint Edn.).

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9

Oxford University Press.
Indonesian Law No. 19 of 2016 *on Amandment of Electronic Information and Transactions.* (2016).
Indonesian Law No. 11 of 2008 *on Electronic Information and Transactions.* (2008).
Indonesian Law No. 39 of 1999 on Human Rights. (1999).
Hiller, J.S., & Blanke, J.M. (2017). Smart City, Big Data and the Resilience of Privacy. *Hasting Law Journal*, *68*(2). Retrieved from: https://repository.uchastings.edu/hastings_law_journal/vol68/iss2/3
Ismagilova, E., Hughes, L., Rana, N.P., & Dwivedi, Y.K. (2020). Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. *Information Systems Frontiers*. Retrieved from: https://doi.org/10.1007/s10796-020-10044-1
Kitchin, R. (2016). *Getting Smarter about Smart Cities: Improving Data Privacy and Data Security*. Department of the Taoiseach.
Lloyd, I. (2008). *Information Technology Law*. Oxford University Press.
Martinez-Balleste, A., Perez-martinez, P., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6), 136–141. Retrieved from: https://doi.org/10.1109/mcom.2013.6525606
The Regulation of The Minister of Communication and Informatics of the Republic of Indonesia Number 20 of 2016 regarding Protection of Personal Data in Electronic System. (2016).
Munir, A.B., & Yasin, S.H.M. (2002). *Privacy & Data Protection*. Sweet & Maxwell Asia.
Munir, A.B., Yasin, S.H.M., & Karim, M.E. (2014). *Data Protection Law in Asia*. Thomson Reuters Hong Kong Limited/Sweet & Maxwell.
Privacy International. (2013). *A Guide for Policy Engagement on Data Protection*. Retrieved from: https://privacyinternational.org/sites/default/files/2018-09/Part%201%20%20Data%20Protection%2C%20Explained.pdf
Solove, D.J., & Schwartz, P. (2006). *Information Privacy Law (Aspen Casebook)*. Aspen Publishers.
Sub directorate of Statistical Demographic. (2013). *Indonesia Population Projection* [E-book]. BPS - Statistics Indonesia. Retrieved from: https://www.bappenas.go.id/files/5413/9148/4109/Proyeksi_Penduduk_Indonesia_2010-2035.pdf
Soekanto, S., & Mamudji, S. (2011). *Penelitian Hukum Normatif: Suatu Tinjauan*. Rajawali.
Soemitro & Hanitijo, R. (1983). *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia.
The 1945 Constitution of the Republic of Indonesia and 1999 Amendment. (2004).
Warren, S.D., & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5). Retrieved from: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C
Westin, A.F., & Solove, D.J. (1986). *Privacy and Freedom*. Ig Publishing.
Willis, A. (2015). *The Benefits of Becoming a Smart City*. Datafloq. Retrieved from: https://datafloq.com/read/the-benefits-of-becoming-a-smart-city/1644
Woo, J. (2017). Smart Cities Pose Privacy Risk and Other Problems, But That Doesn't Mean We Shouldn't Built Them. *University of Missouri-Kansas City Law Review, 85*. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040397
Young, M. (1989). *Technical Writer's Handbook: Writing with Style and Clarity*. University Science Books.
Zhang, K., Lu, R., Liang, X., Qiao, J., & Shen, X.S. (Eds.). (2013). *PARK: A privacy-preserving aggregation scheme with adaptive key management for smart grid*. Retrieved from: https://doi.org/10.1109/ICCChina.2013.6671121
Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X.S. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, *55*(1), 122–129. Retrieved from: https://doi.org/10.1109/mcom.2017.1600267cm
Zoonen, L.V. (2016). Privacy Concerns in Smart Cities. *Government Information Quarterly*, *33*(3), 472–480. Retrieved from: https://doi.org/10.1016/j.giq.2016.06.004

Citation Information: Rosadi, S.D., Suhardi, & Kristyan, S.A. (2021). Data privacy law in the application of smart city in Indonesia. *Journal of Legal, Ethical and Regulatory Issues, 24*(S4), 1-9