Do We Have Privacy in The Big Data Era?
A Study of Privacy as a Legal Concept in Indonesia

Masitoh Indriani[1] and Amira Paripurna[2]
[1]*Department of International Law, Universitas Airlangga, Surabaya, Indonesia*
[2]*Department of Criminal Law, Universitas Airlangga, Surabaya, Indonesia*

Keywords: Big Data, Crime Prevention, the Right to Privacy.

Abstract: Do we have privacy in the Big Data Era? This is the main question with the emergence of the internet with its negative excess in our daily life specifically in the field of privacy. Big Data is increasingly used as the main source for predicting internet users' behaviour by collecting and processing users' personal data. Those predictions enable and transform society insight in the digitalised era. As a result, there is no doubt that Big Data is a valuable tool to generate money for business entities, to predict consumer behaviour, to predict certain criminal activity in the security field, and even beyond this, to be able to control citizens' behaviour in every aspect of life. Thus, the debate over the use of Big Data is whether it leads to disruption of the right to privacy. In addition, there is a relative view of the right to privacy; while one society considers privacy to be an important thing, it could be less important in another society. Addressing those backgrounds, this paper will analyse the right to privacy in Indonesia using Kurbalija's triangle on privacy and the response of the Indonesian Government to protect privacy.

1 INTRODUCTION

In recent years, the development of Big Data technology has changed many sectors. In the private sector, Big Data has been used to understand, identify and to analyze new opportunities for organizations for smarter moves, more efficient operations, higher profit and happier customers (Davenport, 2013). Big Data for companies is able to reduce business cost in terms of cloud-based business analytics and data storing; as a result, Big Data provides faster and better decision making in for business moves. These decisions lead companies to create new products and services that fit with consumer needs.

Meanwhile in the government sector, the rise of Big Data can be seen by the utilization of e-government services. Despite the fact that e-government has helped to achieve efficient and effective services for the citizen, the infrastructure for running an e-government system is also facing a complex and risky task. In the context of law enforcement, Big Data is gathered to produce a more accurate analysis of a criminal pattern. Therefore, the information provided would be a consideration in terms of the decision-making process. However, the information provided is expanding and becoming more complex, ranging from focusing on how the information is gathered and processed to storage. Yet, the issue of data protection and security is increasing in significance since the new search suggests that capture, discovery and analysis of respected data might be invading privacy (Institute, 2018).

Privacy itself can be defined as the right of the person to control their own personal information and whether to disclose information or not (Kurbalija, 2014). The right to privacy is a legitimate right as it recognized in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) and in many international and regional human rights conventions. Therefore, as a fundamental right, privacy should be protected in all respects. Speaking of the protection of privacy, data protection would be the legal mechanism to guarantee the protection of privacy (Kurbalija, 2014).

Despite the great advantage of Big Data in several areas of public life, undoubtedly there are challenges for Big Data and analytics. The challenges particularly relate to the issue of citizens' privacy, data quality and data security. The violation of privacy may occur when there is an absence of data protection principles in terms of how personal

Indriani, M. and Paripurna, A.
Do We Have Privacy in the Big Data Era?.
DOI: 10.5220/0008819702370242
In *Proceedings of the 4th International Conference on Contemporary Social and Political Affairs (ICoCSPA 2018)*, pages 237-242
ISBN: 978-989-758-393-3

information is gathered, processed and analyzed. The challenge for data quality relates to processing and analysis in the form of the algorithm in use; as a result, there will be disruption since this algorithm is used to as a tool of data analytic. The issue for data security may be caused by the software and system used by the organization to process such data. In line with those phases, Kurbalija highlighted that the challenge for privacy could be seen in the triangle of states, business and individuals (Kurbalija, 2014).

Considering the broad area in which Big Data is commonly used, the discussion on Big Data in this paper will focus on the use of Big Data in the context of crime prevention. Furthermore, this paper aims to discuss the legal problems of the various regulations enacted by the government to tackle such issues on privacy. In addition, this study uses Kurbalija's triangle on privacy to analyze the impact of using Big Data on citizens' privacy.

2 DISCUSSION

2.1 Big Data and Crime Prevention

As mentioned above, many people may be aware that Big Data has been frequently used in business matters such as targeted ads. But not many people are aware that Big Data has been used as an important tool for law enforcement to stop crime before it happens. In the era of information, law enforcement agencies are having access to vast amounts of data from emails, video and chat files as well as from fingerprint files, police records, drivers' licenses, car registries and other public databases.

Not only do the law enforcement agencies benefit in the digital and information age, but also the criminals have made great use of it for their criminal activities. Therefore, law enforcement agencies are in need of more advances in technology than the criminals. It is of paramount importance because the criminals are usually one step ahead; they are becoming smarter and more creative at utilizing and benefitting from the advancement of technology. With these data and the use of advanced analytics, law enforcement officials can identify trends and patterns that older crime prevention methods simply did not have the capacity to accomplish.

All around of the country, there is proof that the advance of analytics has offered significant benefits for crime prevention efforts. By accurate analysis, the unconnected data and sources that are owned by the law enforcement agencies can be used to identify threats and halt potential crimes. Therefore, data analysis of Big Data certainly can assist law enforcement agencies to solve a crime problem faster when incidents happen.

Some countries have been using Big Data analytics in preventing crimes. This trend, popularly known as 'predictive policing', has already become popular in countries such as the US, UK and China, where the authorities are not just using data to understand past criminal activities but are also trying to predict the future crime pattern. The Chinese government has been using artificial intelligence (AI) technologies to identify human faces in surveillance video. By applying predictive analytics and machine learning to vast sets of data, police departments can more easily forecast where and when violent crime will break out, and ensure that they have the resources in place to prevent it. However, there are concerns about such AI surveillance; violation of privacy is designated intentionally by the authorities to tackle criticism over the government (Shimbun, 2018). Meanwhile in the US, several police-led initiatives began making the most of surveillance information about 20 years ago. Surprisingly in the UK, a report on Big Data's use in policing published by the Royal United Services Institute for Defense and Security Studies (RUSI) said British forces already have access to huge amounts of data but lack the capability to use it (Babuta, 2017; Dearden, 2017).

In the context of Indonesia, Big Data has been used under the counterterrorism framework. The main objective is to address terrorism and transnational crimes. Based on a recent study, "In connection with counterterrorism, especially in the pro-active counterterrorism whose strategy is focused on the pre-crime aspects such as preventing and stopping, and disrupting terror plots, exchange of biometric data among law enforcement officers across the countries becomes highly relevant" (Paripurna, Indriani & Widiati, 2018). The law enforcement officers in the field are facing many hurdles because of the growing trend of using false aliases, falsification of travel documents and tactics of deception misleadingly suggesting a person has died in a conflict area.

As part of counterterrorism measure, law enforcement conducts systematic collection and recording of the DNA and fingerprints of suspects or defendants as well as collecting and sharing biometric data in their efforts to arrest foreign terrorist fighters (FTF) crossing the border under fake names and travel documents. In Indonesia, the biometric data recorded, collected and stored are Big Data. As it is a relatively new technological system in Indonesia, within the law enforcement and crime prevention processes, these Big Data are used in a limited way; for example, as comparative data (Paripurna, Indriani & Widiati, 2018). In terms of gathering, storing and sharing biometric data, the recent study has shown that there are indications of violations of personal data and privacy (Paripurna, Indriani, & Widiati, 2018). The violations include the absence of a mechanism for data retention, consent, processing, notification, and disclosure (Paripurna, Indriani, & Widiati, 2018).

An example of the use of Big Data in some countries as described above has shown that law enforcement may be a powerful weapon in predicting and preventing crime. However, civilians should remain critical and concerned about Big Data in terms of how it is being used. With the easy accessibility of Big Data, it is necessary to ask, if it is a threat to the daily lives of the people. What limits should be imposed on its use?

As previously discussed, with the amount of Big Data, Big Data can offer public safety. Officials have an obligation to protect the wider community. Furthermore, when law enforcement agencies and the private sector are working together, it can enable companies, shareholders, customers, and the public to prevent future crime, reduce costs and prosecute criminals. Furthermore, collection and analysis of Big Data are crucial to law enforcement, business and government in order for them to be sustainable and efficient in conducting their tasks. The use of Big Data is beneficial in many respects, but not without some merit. One of the weaknesses is the vulnerability to violate the right of privacy. Principally, any steps to collect, store, analyze, access and share Big Data require certain principles to guarantee protection of the right to privacy. Therefore, the following section discusses certain challenges in the utilization of Big Data under the framework of the right to privacy.

2.2 How Big Data Works and Challenges Privacy

In general, Big Data represents the information assets characterized by its high volume, velocity and variety to require specific technology and analytical methods for its transformation into value (De Mauro, Greco, & Grimaldi, 2016) In order to get advanced analytics of Big Data, there are, at least, some elements to be fulfilled, such as: data management, data mining, software, in-memory analytics, predictive analytics, and text mining (Institute, 2018). Data management represents the capability of an organization or authority to guarantee that the data are well-governed before they can be reliably used, and this should also apply in the maintenance process. Data mining will help the organization to gather and examine large amounts of data; furthermore, this collection data will be analyzed to help answer some apparent patterns. Software will be the main tool to process such data and the issue of the storage process is then examined. In memory analytics, technology has the capability to remove data and undergo n analytical process for a new scenario and also, it is able to make a new model; this may influence the organization to make some business or other decision.

Yet, predictive analytics technology uses data, algorithms, and statistics and machine learning techniques to identify future outcomes based on historical data. This means that the technology provides an assessment of what will happen in the future, so the organization is quite confident in business decision-making. Lastly, text mining is used to analyze data from the web, books, or other text-based sources to uncover insight that the organization had not noticed before. Also, this technology uses a social media platform, feed and an online survey to help the organization to analyze more of large amounts of information and find new topics and discover their relationships.

What we know about Big Data as mentioned above is that Big Data entails three elements: volume, velocity and variety (Laney, 2001). Moreover, Big Data is merely used to describe certain predictive analytics or certain methods to gather the value of data (Boyd & Crawford, 2011). In conclusion, the data gathered, processed and analyzed originate from any data including personal data. Therefore, in its application, Big Data cannot be separated from various issues related to personal data and information as well as the right to privacy.

Big Data works with certain systems that collect various user interaction data and sensor infrastructures, not only generating large amounts of data, but also containing individual information on a person. also known as Personally Identifiable Information (PII) (Aryani, 2017). Specifically, PII is any data that can potentially distinguish one individual from another, so they can be used to reveal the data that should remain anonymous.

Privacy is firstly defined as a legal concept in terms of the right to be left alone (Warren & Brandeis, 1890). It also has been part of a long debate and became broader in interpretation as the right of a person to choose seclusion from the attention of the other, the right to be immune from being watched in a private setting (Solove, 2008). In the context of Big Data, privacy which remains in the private area might be exposed by the nature of data collection and data processing. As a result, there is no more control of the subject in deciding whether their personal data or personal information should remain private.

Furthermore, based on Kurbalija's triangle, the challenge of privacy can be described in relations to states, private sectors and individuals. The relationship between states and individuals occurs when the government collects vast amounts of personal information in national programs such as national identity, e-government services, citizens' administrative services and in the form of social security numbers, tax information and many more. For individuals, there is no choice to opt out of providing their personal information; otherwise, they cannot use the provided government services. In this context, individuals' personal information is voluntarily collected by the government. Meanwhile in the context of crime prevention, personal information on individuals is gathered, processed and analyzed in certain ways without providing an option out due to its utilization. Similarly, in terms of crime prevention, the law enforcement agencies collect vast amounts of personal information through biometric data collection of the citizen. Then, the collection of biometric data is used to identify people and assist criminal profiling.

The relationship between private sector and individuals might challenge privacy when the private sectors should be able to protect their clients, in this regard the individuals, by protecting individuals' confidential information from misuse and theft. In the context of Big Data and crime prevention, as we know that Big Data is also gathered from media social, the media social provider should provide protection for their users, otherwise with the increased information users reveals about themselves, the privacy violation becomes frequent and sophisticated (Marsen, 2012).

The third side of the privacy challenge is the relationship between law enforcement agencies and the private sector. This relationship is considered to be the most significant issue since both states (law enforcement agencies) and private sectors collect massive amounts of data on individuals. Some of the data are exchanged with other states in the context of preventing and combating trans-national crimes. As mentioned previously, data exchange is an important element in preventing foreign terrorist fighters (FTFs). Meanwhile, in the process of data sharing, the absence of individual control over personal information is likely to happen. Moreover, the accuracy of data analysis is affected because of the vulnerability of errors in the systems provided by the private sector. In other words, there is a danger of inaccurate personalization over certain data caused by the system, and this can allow images to be displayed to identify certain person such as fugitives, missing persons and persons of interest. Yet, there are always changes in the physical appearances of individuals (Paripurna, Indriani, & Widiati, 2018).

The last challenge for privacy is person to person (individuals to individuals). As technology development increases, any person with sufficient models might own surveillance tools. As a result, the invasion of privacy is becoming more sophisticated, while, in the context of crime prevention, the capability of such individuals might harm society which means that privacy is an important issue. Although there is also less concern for privacy in certain cultures.

2.3 Indonesian Government's Responses on the Right to Privacy

As the right to privacy is the main element related to data protection, we found a study that has recorded that there are at least 32 regulations that contain material related to personal data. Most of these regulations provide the authority to collect and process personal data, including intruding with some exceptions (ELSAM, 2018). The study also found overlapping between: 1) the purpose of processing personal data; 2) notification or consent of the subject data; 3) data retention; 4) the destruction, removal or alteration of personal data; 5) the purposes of data disclosure for third parties; 6) data disclosure processes for third parties; 7) the period of data disclosure for third parties; 8) sanctions; and 9) recovery mechanisms for the subject data whose privacy are violated (ELSAM, 2018).

Yet, the discussion of the legal basis for the protection of the right to privacy does exist. Although the right to privacy itself is not explicitly mentioned in the 1945 Constitution, the basic concept of privacy protection can be found in Article 28F and 28G of the Amendment to the 1945 Constitution. In addition, the protection also can be found in Human Rights Law in Article 13 and Article14 that guarantee every person can be protected in terms of self-development in science and technology, also in communicating and gathering information. To be more specific, there are some regulations containing protection for privacy such as Consumer Protection Law, Banking Law, National Health Law, Hospital Law, and Telecommunication Law and Information and Electronic Transaction (ITE) Law.

In the context of crime prevention, based on Article 26 of ITE Law, it is highlighted that the use of any information through electronic media concerning the personal data of a person shall be made with the consent of the person concerned and whoever's rights are violated may file a lawsuit for damages incurred. However, as argued by Kurbalija, data protection would be the legal mechanism to ensure privacy (Kurbalija, 2014). Hence, data protection law that contains the principles of data protection would help detail the protection and maintenance of citizens' basic rights.

Following on from this, in responding to data protection and the right to privacy, the Indonesian Government enacted Regulation of Ministry of Information and Communication No. 20 of 2016 on Personal Data Protection in Electronic Systems (PDP regulation). Privacy in the PDP regulation is described as the freedom of personal data's owner to disclose or not to disclose his/her personal data, unless otherwise stipulated by the law. In addition, the approval of the disclosure process is given after the owner confirms it in terms of appropriate confidentiality and the purpose for which it is being used. Following the approval, the process, is the collection process, analyzing, storage, and data exchange and the retention process. On the other side, the electronic system provider is obliged to: a) provide an internal procedure to protect such data in terms of its collection and maintenance processes; b) provide access to a subject's data in the context of data modification. In addition, to guarantee the readiness system, the system used by the provider for the process should be certified. Another issue to be highlighted in this regulation concerns data centers. The provider is also obliged to assign a data center and disaster recovery center within Indonesian jurisdiction for the prevention of data-leaking abroad.

Compared to the Organization for Economic Co-operation and Development (OECD)'s Privacy Framework, as the data collected is personal information, there are a number of requirements from the subject in terms of certain principles. Those principles are: 1) The Collection Limitation Principle: it should be clear whether the collection of personal data should be obtained by fair means and lawfully and with the consent and knowledge of the subject data; 2) Data Quality Principle: the data collected should be relevant, accurate, complete and up to date; 3) Purpose Specification principle: the purpose of the collected data shall be subject to data collection and the subsequent use of the subject of the data collection and the subsequent use; 4) Use Limitation Principle: any personal data should not be disclosed, and should be available except when stated otherwise with the consent of the data subject; or by the authority of law; 5) Security Safeguard Principle: personal data should be protected by the company with any reasonable security safeguards against risks of unauthorized access or loss, destruction, modification or disclosure of data; 6) Openness Principle: there should be a general policy of openness about developments, practices and policies with respect to personal data; 7) Individual Participation: the subject data should have some rights to obtain information including communication from the data controller, when given a reasonable reason by the subject; also it should be possible to challenge data relating to the subject data in terms of data retention, and rectification and amendment; 8) Accountability Principle: the data controller should be accountable for complying with the principles mentioned above (OECD, 2013).

Even though the PDP regulation has accommodated certain principles above, the PDP regulation is still considered insufficient since it is only regulated at ministry level. As a result, the regulation might cause technical challenges in bureaucracy.

3 CONCLUSIONS

The utilization of Big Data in the area of crime prevention throws up several issues, particularly the right to privacy. Big Data is shaped by personal information collected and analyzed in a certain manner. Therefore, privacy might be invaded in the context of the relationships of states with individuals, states with the private sector, the private sector with individuals, and individuals with individuals as presented by Kurbalija. These relationships show that the violation of privacy in terms of crime prevention is mostly caused by the absence of data protection principles.

Responding to those threats, in the context of Indonesia, the protection of the right to privacy is guaranteed by the 1945 Constitution; however, at the implementation level, the PDP regulation is still considered insufficient since it is only regulated at ministry level. As a result, the regulation might cause technical barriers in bureaucracy.

REFERENCES

Aryani, T. R. (2017, 09 11). *Bigdata Sharing Vision*. Retrieved from Bigdata Sharing Vision: http://www.bigdatasharingvision.com/articles/isu-big-data-data-privacy-dan-compliance

Babuta, A. (2017). *BIg Data and Policing.* London: Royal United Service Institute for Defence and Security Studies.

Boyd, D., & Crawford, K. (2011). Six Provocations for Big Data. *A Deacade in Internet Time: Symposium on the Dynamics of the Internet and Society.* Oxford.

Davenport, T. H. (2013). *Big Data in BIg Companies.* International Institute for Analytics.

De Mauro, A., Greco, M., & Grimaldi, M. (2016). A Formal definition of Big Data based on its essential Features. *Library Review*, 122–135.

Dearden, L. (2017, October 7). *The Independent*. Retrieved from www.independent.co.uk: https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html

ELSAM. (2018, March 7). UU Perlindungan Data Pribadi Penting Segera Diwujudkan. *UU Perlindungan Data Pribadi Penting Segera Diwujudkan*. Jakarta.

Institute, S. (2018). *https://www.sas.com*. Retrieved from https://www.sas.com/en_id/insights/analytics/big-data-analytics.html

Kurbalija, J. (2014). *An Introduction to Internet Governance.* Diplo Foundation.

Laney, D. (2001). 3D Data Management: Controlling Data Volume, Velocity and Variety. *META Group Research Note*, 70.

Marsen, C. (2012, January 26). *15 Worst Internet Privacy Scandals of All Time*. Retrieved from Network World: https://www.networkworld.com/news/2012/012612-privacy-scandals-255357.html?page=1

OECD. (2013). the OECD Privacy Framework. OECD.

Paripurna, A., Indriani, M., & Widiati, E. P. (2018). Imlementation of Resolution no.4/2016 of the ICPO-INTERPOL Concerning Biometric Data Sharing: Between Countermeasures Against Terrorist Foreign Fighters (FTFs) and Protection of the Privacy of Indonesian Citizens. *Brawijaya Law Journal*.

Shimbun, T. A. (2018, July 13). *Editorial: Privacy Under AI surveillance: China's extreme use raises alarm*. Retrieved from The Asahi Shimbun: http://www.asahi.com/ajw/articles/AJ201807130017.html

Solove, D. (2008). *Understanding Privacy*. Cambridge, Massachusetts: Harvard University Press.

Warren, S. D., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law*.