Qualitative and Quantitative Research Review, Vol 4, Issue 1, 2019
ISSN No: 2462-1978
eISSN No: 2462-2117

DISCLOSURE OF DATA RELATED TO MONEY LAUNDERING INVESTIGATION FROM DATA PROTECTION PERSPECTIVE

GO LISANAWATI[1]
MOHAMMAD SADEGHI[2]

Faculty of Law, University of Surabaya (UBAYA), Indonesia[1]
Hormoz Research Center, University of Hormozgan, Iran[2]

Date of receipt: 30/05/2018
First Review: 22/07/2018
Second Review: 15/09/2018
Acceptance: 22/11/2018

ABSTRACT

The issue of personal data and its protection is important to be discussed. Data protection has been put as the main mechanism that should be ensured regarding with the using of technology that require data collection, data storage, and data access in all real and virtual activities. More of that, the uses digital signature, digital contract, or any acceptance and verification methods in the activities related to technology uses are need to ensure data protection. The law shall be governed to give the protection in that matter. But the cyber attack appears as serious threat in the context of data protection. All parties who collect data must be respect the disclosure of data and the use of data. Another important criminal cases investigation process and law enforcement that needs data disclosure is money laundering. Money laundering deals with transaction of illicit money, underlying transaction, illicit funds transfer, and other forms of transaction that describe money laundering movement. In case of criminal cases investigation, it is definitely important to the officer to access data to illicit money stored, movement, or transferred that have been conducted

by offender. Investigator needs to access data of offender that using financial provider's service to hide, or to disguise money. This working paper is using qualitative research method that study and analyze the disclosure of data in anti money laundering regime but will be analyzed from data protection regulation perspective. As the result, data protection shall be allowing to be disclosed for money laundering investigation process since money laundering cases is an intelligence investigation. The responsible law agencies and reporting parties shall be handle with very careful and not expose the data beyond the needed. In practice, this paper will give knowledge why does the disclosure of data will remain important for the investigation process of money laundering cases in practice.

Keywords: Anti Money Laundering, Regulation on Data Protection, Data Disclosure, investigation

INTRODUCTION

The development of crime has been touching the vital value of personal data protection. Personal data is related to a scheme of protection, mechanism of acquisition, collection, and any other activities related to individual data protection. In Indonesia, the Ministry of Communication and Informatics has to regulate the Personal Data Protection through the Minister of Communication and Informatics Regulation Number 20 of 2016 concerning Personal Data Protection in the Electronic Systems. It is categorizing personal data into 2 (two) perspectives. One is from general meaning, and other is specific Personal Data. In the general meaning, personal data is related to an individual data that recorded, maintained, its rightness is kept, and the confidentiality is protected. Otherwise, the specific personal data can be understood as accurate and concrete information, directly or indirectly identifiable and attached to each individual. It means that each personal data shall be protected and confidential. Confidentiality is not related only to protection of data, but also the process of transmission and/or dissemination and/or storage. Each data should be treated as a privy. Thus, the scheme of written

consent should be designed to give protection to the owner of the data. However, in the law perspective, consent can be obtained under the law and consent of parties. The consent can only be given after the owner of data confirms regarding the data's precision and confidentiality.

Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) has been a referred regulation to data protection regulation. Article 4 (1) explains: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Thus it means that personal data is including name, identification number, location data, online identifier, etc.

The discussion of personal data is also discussing data privacy. According to the International Covenant on Civil and Political Rights (so-called as ICCPR), data privacy is a part of fundamental rights (among other things General Point No. 16 of Article 17 of ICCPR) but remains possible to be reduced or limited. In other words, data privacy is derogable rights. Point 7 of ICCPR's general comment No. 16 of Article 17 states:

As all persons live in society, the protection of privacy is necessarily relative. However, the competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. Accordingly, the Committee recommends that States should indicate in their reports the laws and regulations that govern authorized interferences with private life.

The law should give limitation and reduction of privacy (in the meaning of derogable rights). Mathovani (2015:46) mention that the limitation and reduction of the protection of privacy rights guarantee is contradiction interest connection between individual interest and public interest. If the limitation and reduction have given by law, then every citizen should obey to it. Thus, in purpose to search and find the real truth, public interest should be placed in the highest position. The law shall give a proper mechanism to create the balance between those two interests, to respect the human rights and in creating proportional fairness of data transmission and any other activities from an intruder and or illegal interception. J. Clough (2010:137) mention: "the interception without right, made by technical means, of no-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data." Further, "Technical means includes technical devices fixed to transmission lines, such as 'packet sniffers' as well as devices to collect and record wireless communication" (J. Clough, 2010:137). Then the law should be ensured the process of data protection will be smoothly exchanged.

LITERATURE REVIEW

Financial crime is increasing more and more in line with the process of development of nation. There is an adagium said when a country is developing then there will remain an economic crime. Thus, it means also the financial crime will remain exist when the country is developing. Financial crime in its development has been manifested into many forms. One of them is money laundering. Money laundering in its characteristic has interacted with the aspects of a life of every field including technology, and other security things. Chandna (2017:11) explains that "Money laundering simply means conversion of black money (Dirty Money) into white money (clean money) where the black money may not become white legally but appear to have become so." Thus offender of predicate crime will try to do anything to hide,

disguise, or conceal their assets of crime's sources in a money laundering scheme. More complex its predicate crime, it is the most challenging money laundering scheme will be conducted. In this matter, an offender who gain money from illegal activity (in a relationship with the economic crime) which they could not freely and openly (disclose) sources of assets, and create many ways to hide its source of funds, it should be categorized as conduct money laundering. The methods to do money laundering is sophisticated, and in some cases it can be so complicated because the offender do more than 1 (one) predicate crime and complex methods.

In theory, money laundering can be conducted through 3 (three) methods. It called as:

- Placement. It is a method where the offender places the illicit money into a bank account. The offender will deposit black money in banking and/or other services provider, tunneling and smoothly channelized the further utility. The offender frequently will efficiently use the money or assets without attracting suspicious attention.
- Layering. It is a method to disguising the transaction using various ways. The purpose of this method is actually to let the law officer finds difficulty to disclose the source of funds. Generally, in a layering method, the offender will divide the funds into a small transaction and make it complicated by transferring from one bank account into others, and conducted smurfing method to hide the source of money.
- Integration. It is a method whereby offender of predicate crime who gain illicit money demonstrating the justification of the funds' holder into a "seemly legitimate" ownership such as buy luxury apartment, luxury cars, islands, and many more even though using other's assistance to hide the real source of funds holder.

Through the theory, it can be understood that money laundering will create more opportunity by the offender to combined and make more complex the methods by using many ways. In this sense, the offender itself wishes to hide the personal information. Money laundering process needs the underlying transaction. It can be a trail to be traced. In this regards, all the tracing process will use financial tracking. It needs more effort to elaborate information.

In the money laundering process, a country uses Financial Intelligent Unit that will work through gather information from any reporting parties, financial account, and compliance of profession party who has been appointed by the law to be the reporting parties. Alldridge, in Greed, Corruption, and the Modern State book, explains that: "The AML (Anti Money Laundering, red) is now in play, carrying with it greater investigatory powers, greater potential sentences reporting requirements, attenuated professional privileges and so on..." (Alldridge, 2015: 331). Thus, the investigation process will need more than a power to reveal, but also information including what is called as personal information regarding with the personal data related to crime conducted by the offender and the environment that may involved in the criminal activity.

METHODOLOGY

This is an explanatory article. It is a qualitative legal research that gives an understanding on the importance of data disclosure in the money laundering criminal cases investigation process. As it is understood, money laundering is always related to a financial tracing because money laundering is one of proceeds of crime that using money and/or property as the object of crime.

Money laundering investigation is financial transaction intelligence. The collection of data's technique is using observation and text reviewing.

Qualitative and Quantitative Research Review, Vol 4, Issue 1, 2019
ISSN No: 2462-1978
eISSN No: 2462-2117

RESULT AND ANALYSIS

As it is mention above, the existence of anti-money laundering regime is actually to cut the benefit acquired from illicit activities or called as a crime. From the perspective of public, it is essential to save the state treasury from the potential crime that may destruct the economic life of a nation. In the money laundering process, there are several risks and mitigation risk that should be well and earlier recognized. Since money laundering is usually using multi-layering and/or vehicle, it is essential to know where illicit money will be placed.

Council Resolution on Lawful Interception of Telecommunication 196/1329/01 as followed by many countries implemented the Privacy International principles as:

1. Legality principle
2. Legitimate aims, necessity, and proportionality
3. Safeguards against Illegitimate Access. In this principle, the privacy of citizen shall be meet one of the requirements such as conducted by the legal authority. It will limit the possibility of illegitimate access by creating a mechanism of proper monitoring and evaluation both internal and external.
4. Due process. In this context, to get personal information as the evidence of a crime, it should be meet the proper effort.

Thus the process of personal data as information shall be treated well, but it does not mean that the data is secret under enclosed protection. In the context of a crime such as money laundering, corruption, and other financial crime, information shall be put as a public good. From perspective of the ultimate goal, Nation is actually to realize the social welfare. It means the interest of public is the priority. M. Goodman (2015:116) strengthening that: "the explosion of data has led to the creation of a brand-new industry for transnational organized crime groups, and mass identity theft is the result." M. Goodman is shared

how the data (including personal data) needs a protection scheme also. The illegal access of data will bring negative result as well.

According to The General Data Protection Regulation, there are 6 (six) principle of data protection processing as explained in the Article 5 (1). It is that Personal Data shall be:

a. Lawfulness, Fairness, and Transparency
b. Purpose limitation
c. Data minimization
d. Accuracy
e. Storage limitation
f. Integrity and confidentiality

Regarding to the principle of integrity and confidentiality, the officer shall be process personal data with appropriate security manners. Personal data shall be avoided from unlawfulness or unauthorized data processing. Personal Data breach as mentioned in the Article 4 (12) means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Money laundering will need information regarding with the due diligence regime. Esoimeme (2015:27) reminds: "Any type of account is potentially vulnerable to money laundering or terrorist financing. By the nature of their business, occupation or anticipated transaction activity, certain customers and entities may pose specific risks..., it is essential that the financial institution/DNFBP exercise judgment and neither define nor treat all members of a specific category of a customer as posing the same level of risk". From that explanation, it can be understood that since the customers carry out of the level of risks, then it is essential to know how is the information of customers can be assisted to reduce money laundering.

It is essential to get the customer's information due to the response regarding of due diligence (both customer's due diligence and/or

enhance due diligence). There is standard due diligence's degree. It should be applied to all customers. The profiling that conducted by the financial institutions, and/or professionals, and/or other goods and services providers, correspondent banking, beneficial owner, and other reporting parties. The risk is also attached to the position of Politically Exposed Persons as recognized by the FATF as a risky people. FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (2012) explained that: "PEPs are individuals who are or have been entrusted with prominent public functions and an immediate family member or a known close associate of such a person."

Esoimeme (2015:205) then add information that: "the amount of corruption and abuse of public funds by some government leaders and public officials over recent years have given great cause for concern both internationally as well as in countries involved. Those people are collectively known as politically exposed persons (PEPs)". Thus, the risk of specific customers so called as PEPs put difficulties to a state body to know the PEPs if the reporting parties did not comply with the law and international standards to give any report regarding with the illicit funds and did not work under the name of data protection.

In this sense, all the information will bring benefit to country to reveal the crime related to sophisticated and challenging crime through many schemes. The International society standardize the using of Enhance Due Diligence (deeper than customer due diligence) to treat PEPs. Due diligence should include the information concerning:

- Legal Name and any other name
- Address (permanent and mailing address)
- Telephone number, fax number, email address
- Date and place of birth
- Nationality
- Occupation, a public position held (designation), the name of employer

- Unexpired verification and other clarification tools such as passport, or social number card, driving license, identity card, and many more.
- Source of funds and wealth
- The purpose of the transaction
- The last connection of transaction
- Relationship with the party who will get the benefit from that fund. In this perspective, it should be identified the complete profile of the beneficiary, the relationship with the person who gives the benefit.
- The transactions using suspected illicit funds and/other unclear sources of funds.

In this context, data (even though some of them are personal) but it is important to disclose.

As the Financial Action Task Force recommendation mention that each of financial institutions, the directors, officers, and employees should not or where appropriate, should not be allowed to, warn their customers when information relating to them is being reported to the competent authorities. In this context, the report is containing any information (including personal data). Data in Anti Money laundering will contain valuable information for a process of enforcement. Thus, data shall not be a limitation for a work of law enforcement in considering the nature of the crime itself. As mentioned before, money laundering is very dangerous and sophisticated. It is threatening for the economic and financial life of Nation. Thus, it shall be treated as an essential data that will contribute to Nation.

In this term, there are several mechanisms should be given to ensuring the importance of the data protection aspects in the anti money laundering regime. Preziosi (2017) said that:

AML obligations have tended to take precedence, even if this meant trumping on data protection principles. This is even true from a regulators' perspective, who appeared to promote the countering of money laundering as far more important than protecting an individual's privacy... In turn, obliged entities have been left with little option but to do what they can to meet regulators' expectations, even if this meant throwing data protection principles out of the window, thus safeguarding themselves against the risk of reputational damage and other regulatory sanctions.

This will now have to change. The GDPR imposes harsher penalties and transparency requirements, and more importantly, introduces the concept of individual accountability. Collectively, these factors suggest that obliged entities must up their game when it comes to compliance with data protection requirements.... It also imposes data retention limits and forces human intervention in automated alert systems, thereby impressing upon obliged entities the need to consider AML and data protection requirements as complementary to each other rather than being mutually exclusive.

Thus the problem appears here are not about the use of personal data, but all the access to the personal data and the process of its protection needs a certain mechanism and guarantee of the data uses from destruction, damaging, or alternation. The data shall be treated as public goods, in a term of the user of data is for the public (mean as the society). Thus, in anti-money laundering, several mechanisms should be implemented by Government, for example, the implementation of "Professions Secrecy" principle. The principle is prohibiting any law enforcement agent, reporting parties, and also Financial Intelligence Units that have already gain documents or information regarding with the customer who is suspected to be involved in the money laundering scheme. They should obey the obligation to keep that document or the information according to their professionals' obligation. However, as long as the law orders it, then the data shall be revealed.

Herewith personal data should keep in disclose in the specific terms and through a proper mechanism under the law, and it should not contra to

the money laundering law enforcement process. The function of law here is to give certainty and then create justice. Gardner (2012:233), based on the Hart, mentions that: "law is conceptually connected to legality, and that legality is conceptually connected to justice." In considering the utility based on the happiness of the society in the enforcement against money laundering, we need more the flexibility to diminish the possibility of the abuse against personal data. Thus, personal data will not be a limitation for the process of enforcement in the anti-money laundering regime.

RECOMMENDATION AND CONCLUSION

The aspect of data protection is remaining important to avoid abuse of powers of the law enforcement agents (including Financial Intelligence Units and reporting parties). The uses of article on "Professions Secrecy" is important to give protection in the context of personal data will be professionally treated through a specific needed and proper mechanism. It is guaranteed by the law to access and a responsibility to keep it as its way. The law should be ensuring its protection.

REFERENCE

Alldridge P. (2015). Tax Avoidance, Tax Evasion, money laundering and the problem of 'offshore', Article, in *Greed, Corruption, and the Modern State: Essay in Political Economy*, edited by Susan Rose-Ackerman and Paul Lagunes.2015. UK - USA: EE Elgar

Esoimeme, E.E. (2015). *The Risk-Based Approach to Combating Money Laundering and Terrorist Financing*. United State of America: Eric Press

Gardner, J. (2012). *Law as a Leap of Faith*. UK: Oxford University Press

Goodman, M. (2015). Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. USA: Anchor Canada

Manthovani. R. (2015). *Penyadapan vs. Privasi*. Jakarta: Bhuana Ilmu Populer

Preziosi, C. (2017). Finding the balance between data protection and AML requirements". Article, Retrieved from: https://www.lexology.com/library/ detail.aspx?g=8aabfbf8-33c1-456d-869b-ef1f56ec0e08, June 23. (accessed on 23rd August 2018).

Paper for Issue

Volume:4 Issue:1

Sr No.	Article Information
1	SERVICE QUALITY AND CUSTOMER LOYALTY: MEDIATED BY CUSTOMER SATISFACTION IN THE TELECOMMUNICATION INDUSTRY Author(s): VIKINESWARAN A MANIAM, VISWANATHAN ANNAMALAI. View Abstract Page No : 1-24 Download pdf
2	ORGANISATIONAL CLIMATE AND COMMITMENT: A SARAWAK VOCATIONAL COLLEGES' TEACHERS PERSPECTIVE Author(s): CHUNG JEE FENN. View Abstract Page No : 25-47 Download pdf
3	INDEPENDENCE, CORPORATE GOVERNANCE AND AUDIT QUALITY ON THE INTEGRITY OF FINANCIAL STATEMENTS Author(s): SAHIDAH. View Abstract Page No : 48-76 Download pdf
4	EXTERNAL AND INTERNAL FACTORS AFFECTING THE PROGRESS OF EVENT INDUSTRY IN MALAYSIA Author(s): ABDULLAH-AL-HASAN, ONG SIEW HAR, CHRIS. View Abstract Page No : 77-112 Download pdf
5	INTERNAL DEMOCRACY AND NIGERIAN POLITICAL PARTIES: THE CASE OF ALL PROGRESS CONGRESS (APC) Author(s): BABAYO SULE, MUHAMMAD AMINU YAHAYA. View Abstract Page No : 113-142 Download pdf
6	EXPERIENCE, COMMITMENT AND SENSITIVITY AUDITORS OF ETHICS REPRESENTATIVES Author(s): ANWAR. View Abstract Page No : 143-159 Download pdf