International Journal of Global Community
Volume IV No. 2 (July), 2021

Legal Protection for Personal Data of Consumers in the Big Data Era Related to Data Breach Activities Based On the Law Concerning Electronic Information and Transaction in Indonesia

Sinta Dewi Rosadi and Hadyan Farizan

Faculty of Law, Padjadjaran University, Bandung

Email: sinta@unpad.ac.id; hadyan.farizan@gmail.com

Abstract

Personal data in the big data era is different from traditional data; such data are specifically based on transactions that are documented, classified, and stored with computer technology. Personal data are inputted into the big data technology system to explain in detail the personality of each individual. This causes concern on the part of the owners of the stored personal data in big data system regarding data breach activities. Data breach is very detrimental to the owners of personal data and the corporate bodies that is responsible for the personal data. The purposes of this study are to formulate the most appropriate steps for legal protection of individuals' personal data against data breach practices and determine the legal liability for data breach by a company that fails to protect the personal data of its customers. The method used is the normative juridical approach. The results of this study indicate that the legal protection of personal data is still insufficiently emphasized by the government to administrators of electronic systems in relation to improving the infrastructure of the company's security system given that the development of big data is rapid. Also, measures to combat data breach has not been implemented properly, as the process is long and involves complaint to the minister before being able to file a civil suit, notwithstanding the fact that personal data is highly sensitivity.

Keywords: Big Data, Data Breach, Data Protection

Introduction

In the current era of globalization, the development of technology, especially information and communication technologies, is very fast. Information technology includes systems that collect, store, process, produce and send information to and from industry or society effectively and quickly. Now, electronic information and communication systems have been implemented in almost all sectors of life in society. Communication technology is everything related to the use of tools to process and transfer data from one device to another. Therefore, information and communication technologies constitute an inseparable equivalent that contains a broad understanding of all activities related to processing, manipulation, management, and transfer of information between media (Syarah, 2009: 1).

Information and communication technology will not function if there is no data to process; therefore, data is also an important component. The data referred to in this paper does not mean the same thing as data in the traditional sense, which is generally defined as the smallest unit embodied in the form of number symbols, letter symbols, or image symbols that describe the value of a certain variable according to data conditions in the field (Kemendikbud, 2017). Rather, this paper refers to data based on objects, events, activities, and transactions that are documented, classified, and stored but not organized to be able to provide a specific meaning (Pawitra, 2016: 2). Examples of the data referred to (Xiaomeng Su, 2016: 3) are web data (level of internet user habits), text data (email, news, Facebook, etc.), time and location data (GPS and mobile phone data along with Wi-Fi connection; time and location information become data sources that continue to grow), smart grid and sensor data, and social network data (social interaction data, which is analyzed to provide advertisements according to user habits; besides this data is used to determine the user's circle of friends or colleagues).

The use of data is already very high because almost everyone has data in their electronic devices (computers/laptops, smartphones, flash drives, etc.); this high level of data usage also has a high-risk factor if we look at using internet technology. With the internet, each individual can connect with people internationally, notwithstanding their jurisdiction. Another development related to data in the current state of the technological era is that the use of data has changed; previously, data could only be owned by a person or subject that is related to the data, but it is now a universal thing that can be accessed by anyone if it is uploaded. The implication of this change is very huge. Data processing is more computerized, so space can be saved in the company’s office by means of softcopy storage. The presence of electronic data has formed a separate world known as the virtual world (cyberspace) or pseudo world, which is a world of computer-based information and communication that offers a new reality in virtual, indirect and unreal forms (Nugraha, 2012: 2). This situation is also known as big data.

Big data can be defined as a data storage medium that offers unlimited space as well as the ability to accommodate and process various types of data very quickly (Bahar, 2017). Initially, big data was a technological system that was introduced to cope with the "information explosion" along with the growing ecosystem of users of mobile phone devices and internet data. Various types of data, ranging from data in the form of text, images or photos, and videos to other forms of data, flood the computing system. The use of big data in today's technological era has many benefits because big data is a combination of old and new technologies that can help companies gain actionable insights. Therefore, big data is the ability to manage large amounts of disparate data at the right speed and in the right time frame to enable real-time analysis and reactions (Hurwitz, et al., 2013: 15).

From the above explanation, it is evident that big data technology has many benefits. Big data technology can be utilized by many institutions, including large companies, Small and Medium Enterprises (SMEs), and the government. The benefits of big data have been felt, and they include the following (Kemkominfo, 2015: 9-10):

a. Knowing the public's response to products issued through sentiment analysis on social media.
b. Helping companies make more precise and accurate decisions based on data.
c. Helping to improve a company's image in the eyes of customers.
d. Planning of business by knowing customer behaviour, such as in telecommunication and banking companies.
e. Knowing market trends and consumer desires.
f. Using data on a patient's previous medical history, a hospital provides better and faster services.

The points above are some of the benefits provided by the use of big data. However, the use of big data not only results in positive effects but also negative effects (crimes). Therefore, to avoid these negative impacts, its' use must be accompanied by modern (sophisticated), clear, and strict regulations because the perpetrators of violations in the field of information technology are virtual. Crimes using computers and the internet (as a medium of communication and information) are known as cybercrime. Cybercrime is a crime that includes several types of crimes.

Bernadette Schell and Clemens Martin in the book "Webster New World Hacker Dictionary" (in Anam, 2010: 4) explain:

> "Cybercrime involves such activities as child pornography; credit card fraud; cyber stalking; defaming another online; gaining unauthorized access to computer system; ignoring copyright, software licensing, and trademark protection; overriding encryption to make illegal copies;

> software piracy; and stealing another's information to perform criminal acts…"

From the explanation above, cybercrime includes crimes of various kinds, namely theft, intellectual property violations, piracy, online slander, pornography, intrusion into a computer system through its network without permission for malicious purposes (cracking), overriding encryption to make illegal copies, stealing other people's information to commit criminal acts and others. Of the various types of cybercrimes above, this paper focuses on the crime of stealing other people's personal information (privacy) or breaking into data by damaging other people's computer defense systems to enjoy the results (Juju et al., 201: 77), meaning that the activities of breaking into consumer personal data (data breach) in the current era of big data will be discussed.

This is a challenge in the adoption of big data technology, so the specific challenges regarding data privacy protection will be examined. On one hand, data disclosure is needed, but on the other hand, privacy is a sensitive issue and is often injured through technological advances. Privacy relates to a person's personal data that must be protected. The big data handled by the telecommunication and banking industries, for example, are obtained directly from consumers; most of them are personal data and are very prone to be misused by other parties. The use of a person's personal data must have the consent of the person concerned if it will be used by another party (Kemkominfo, 2015).

The state of data protection in the world is very precarious. Data is still vulnerable to breaches. It is proven based on Cisco's 2017 Annual Cybersecurity Report (ACR) that more than a third of security breaches experienced by companies in 2016 are related to data breaches. When there is a security breach, it is very likely that data leakage will also occur, which results in the loss of at least 20% of the number of subscribers, business opportunities and revenue. The area that is often the focus of hackers is the operating system, and such attacks occurs as much as 36% of times. This is because the operating system carries out the core function, and if it is breached, it will affect the level of productivity, such as in the transportation, healthcare, and manufacturing industries. It may slow down or even stop activities. After the operating system, finance is the most preferred function that is targeted for attacks (Cisco, 2017: 56).

Regarding personal data leakage, an incident was experienced by a company known as Equifax, a consumer credit reporting agency that has the personal data of more than 800 million individual consumers; the personal data of as many as 143 million consumers were stolen. The details of the case are as follows (Naughton, 2017):

> "…It's one of the three largest American credit agencies (the others are Experian and TransUnion) … Equifax was hacked via a security flaw in the Apache Struts software that it used to build its web applications…. As a result, the hackers were able to steal the personal information of 143

> million Americans. It is the most important financial data available on any citizen – names, dates of birth, social security numbers, home addresses and in some instances a lot more, including credit card details of more than 200,000 US consumers. Equifax discovered the breach on 29 July but didn't reveal it publicly until 7 September."

The case above shows that the protection of personal data is very important. Moreover, the leaked data were crucial data of each individual (names, dates of birth, social security numbers, home addresses and in some instances a lot more, including credit card details) entrusted by the them to the company.

The act of gaining access into individuals' personal data by illegal intrusion into the defense system is a violation that is contrary to Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions (EIT Law) as amended by Law No. 19 of 2016. Article 26 states that personal data must be accessed with the consent of the person concerned. In addition, unauthorized access of personal data is also contrary to Article 30 of the EIT Law. The above incident is very regrettable because it is an evidence of the weakness of the company's defense system in safeguarding consumer's crucial personal data and the company's lack of seriousness in taking mandatory actions after knowing that the data defense system has been breached. The responsibility of each party is also an important point that will be studied in this research to find out what actions should be taken by the parties in the event of a data breach.

Problem Statements

a. What is the level of protection of personal data in the big data era against data breach activities based on Law No. 11 of 2008 concerning EIT as amended by Law No 19 of 2016?
b. What is a company's responsibility regarding the personal data of consumers who experience data breach activities?

Research Method

The method used is the normative juridical approach. This research is based on secondary data in the form of primary legal materials from the laws and regulations of the Republic of Indonesia related to the object of research. Secondary data relating to the act of collecting an individual's personal data through data breach activities were analyzed. The laws and regulations used are written or unwritten. In this study, the legal materials used are Law Number 11 of 2008 concerning Electronic Information and Transactions as Amended by Law 19 of 2016 and Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Personal Data in Electronic Systems. Then, legal principles were analyzed and further supported by secondary legal materials

(research results, scientific journals, expert opinions, etc.), which provide an explanation of the primary legal materials.

Discussion

A. Analysis of Personal Data Protection in the Big Data Era against Data Breach Activities Based on Law No. 11 of 2008 concerning EIT as Amended by Law No 19 of 2016

Legal protection is a form of protection for human rights that are harmed by others, and legal protection is given to the society so that they can enjoy all the rights granted by law. In other words, legal protection includes various legal remedies that must be provided by law enforcement officials to ensure a sense of security, both mentally and physically, from disturbances and various threats from any party (Rahardjo, 2000: 55). The legal protection in question here is the protection of personal data.

Law Number 19 of 2016 concerning Information and Electronic Transactions does not define personal data, but the definition of personal data can be found in related regulations, namely Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP) and Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (PM Kominfo). Article 1 point 27 of PP and Article 1 point 1 of PM Kominfo explain that personal data refers to certain individual data that are stored, maintained, and kept confidential.

Personal data contained in a company that implements big data technology is personal information that is very confidential; in other words, personal data is the data of each individual and is only entitled to be owned by the individual entity. The current era of big data has changed the way personal data is collected, processed and utilized. With technology, very large amounts of data are inputted at increased speed with an unlimited storage quota, so it will have a tragic impact if the data storage area is hacked.

Protection of personal data against data breach in Indonesia can be found in Law No. 11 of 2008 concerning EIT as amended by Law No 19 of 2016, Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (PM Kominfo), and Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP). Personal data protection is accommodated in Article 3 of PM Kominfo, which explains that personal data protection in electronic systems is carried out in the processes of acquisition and collection; processing and analysis; storage; appearance, announcement, delivery, dissemination, and/or access opening; and annihilation.

Legal protection for the personal data of individuals who experience data breach activities has been mandated by the EIT Law. Data breach activities can be

categorized into three types, namely malicious or criminal attacks, system glitches, or human errors. The different causes of data theft have been captured in different articles of the various laws. In this paper, the legal protection of personal data against data breach activities for the category of malicious or criminal attacks is the focus. The personal data that is the object of the violation is usually sensitive personal information (for example, social security numbers, driver's license numbers, or financial account numbers), which are sold to the public. The stolen data may be sold to the original owner under certain terms of return or to other people for a quick profit (Identity Theft Resource Center, 2018).

In this paper, the personal data breach at Equifax is analyzed; it is the personal data breach involving the largest amount of sensitive data in history. Equifax uses advanced statistical techniques and software tools to analyze available data, create custom insights, decision making solutions and processing services for clients, i.e. Equifax uses big data technology. Therefore, the data available to the company varies from the simplest to the most sensitive data. The consequence of using big data technology is that it is vulnerable to cyber-attacks.

The perpetrators that hacked into Equifax database exploited a security vulnerability in the Apache Struts software used to build its web application. The loophole gave the hackers a way to control the company's crucial sites. The hackers deliberately entered the big data system to break into the personal data of 147.9 million people, and it can be assumed that the leaked personal would be used for the personal interests of the perpetrators. The legal protection of personal data against data breach activities as stated in Article 15 of PP indicates that if a company has failed to maintain the personal data of its clients, the electronic system operator is obliged to notify the owner of the personal data in writing. Furthermore, the notification is regulated in PM Kominfo. Article 28 letter c of PM Kominfo explains the provision regarding notification by the electronic system operator to the owner of personal data if there is a failure to protect the confidentiality of the personal data in the electronic system it manages. It states that the notification:

1. must be accompanied by reasons or causes for the failure of confidential protection of personal data;
2. can be done electronically if the owner of the personal data has given his/her consent which was stated at the time of the acquisition and collection of his/her personal data;
3. it must be ensured that it has been received by the owner of the personal data if the failure contains a potential loss for the person concerned; and
4. written notification is sent to the owner of the personal data no later than 14 (fourteen) days after the failure is known.

In PM Kominfo, Chapter VI Article 29 - 30 explains that the owner of the personal data can submit a complaint to the Minister for the failure to protect the confidentiality of the personal data. The complaint is intended as an effort to

resolve disputes by deliberation or through other alternative settlement efforts. The complaint can also be made based on failure by the company to meet its obligations stipulated by law regarding the loss of personal data, as follows:

a. Failure to provide written notification of the failure to protect the confidentiality of personal data by the Electronic System Operator to the owner of personal data or other Electronic System Operators related to the personal data, whether or not it has the potential to cause harm; or
b. There has been a loss for the owner of personal data or other Electronic System Operators related to the failure to protect the confidentiality of the personal data, even though written notification has been made of the failure to protect the confidentiality of personal data, but the notification time is too late.

In PM Kominfo, there is a further explanation of the complaint process, which is contained in Article 32; it asserts that if efforts to amicably resolve disputes regarding personal data breach are unsuccessful, the owner of the personal data in question can file a lawsuit for the failure to protect the confidentiality of the personal data. Article 32 of PM Kominfo means that parties who own personal data are given the opportunity to sue a company that fails to protect their personal data, such as Equifax, since the rights of the owners of personal data have been violated because personal data that should be protected.

This step to file a lawsuit is also in line with the measures to ensure legal protection of personal data as stipulated in Article 26 paragraphs (1) and (2) of the EIT Law. The personal data of individuals in general have been protected by Article 26 of the EIT Law. According to the article, personal data, which is only fully owned by each individual, cannot be processed (used, distributed, etc.) and must be kept confidential as long as the individual's consent has not been received. In other words, the individual will always be aware of any actions taken regarding his personal data.

There is another form of legal protection provided by the EIT Law for the owner of personal data whose rights have been violated because the company failed to keep his personal data confidential, which is liability in the form of punishment to the company, as contained in Article 32 of the EIT Law. The regulation explains that legal protection for data owners' personal rights do not only come in the form of a civil lawsuit but can also take the form of a criminal lawsuit. The articles above provide an opportunity for redress for clients whose personal data were breached due to failure by the company managing them to be protect the data, such as in the Equifax case. Individuals can request for compensation due to the violation of their personal rights by filing a lawsuit to recover the losses incurred. Also, a criminal lawsuit can be filed to hold the company to account for its failure to protect individuals' personal data.

Based on the explanation above and in relation to the Equifax case, which has the possibility of happening in Indonesia, the company where the data breach occurred must notify all those whose personal data have been breached.

The notification must be made in writing or electronically; it can be done electronically if the owner of the personal data has given consent to receive it in that form. The notification must be accompanied by the reasons or causes for the failure to protect the confidentiality of personal data, and if the failure to protect the personal data has the potential to cause harm to the person concerned, it must be ensured that it has been received by the owner of the personal data. The most important thing is that a written notification is sent to the owner of the personal data not later than 14 days after the failure is known.

Regarding the data breach at Equifax, it is known that it occurred in mid-May 2017 and was discovered by the company on July 29 2017. However, the company did not act in good faith as it did not immediately notify the owners of the personal data regarding the breach, either in writing or electronically. Equifax only notified the owners on September 7, 2017. If we relate this scenario to Indonesian regulations related to personal data protection, then the owners of the personal data can file a complaint to the Minister for the failure to ensure the confidentiality of their personal data. This is because Equifax meets the criteria for being held responsible for unlawful acts, namely the company did not provide notification when it became aware of its failure to protect the personal data of its clients in writing or electronically. Equifax exceeded the notification limit set in PM Kominfo, which is "not later than 14 days after the failure is known". The company waited until 40 days after the failure was known.

The above legal protection measures are legal protection efforts by deliberations or through other alternative settlement efforts. Besides, the owner of the personal data is entitled to file a criminal threat suit based on Article 32 paragraph (3), as the elements of confidential electronic information becoming accessible by unauthorized persons (hackers) has been fulfilled, and the penalty is a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah). This effort is the last step for consumers or owners of personal data to obtain accountability from companies such as Equifax, in accordance with the regulations of the EIT Law and the PM Kominfo.

B. The Company's Responsibility as Electronic System Operators regarding Personal Data of Consumers Who Have Conceded Data (Data Breach)

Accountability is the consequences of a person's freedom regarding his actions in relation to ethics or morals in doing an act (Notoatmojo, 2010: 38). Accountability in any case must have a basis, namely things that give rise to legal rights for a person to sue others as well as things that give rise to other people's legal obligations to provide accountability (Triwulan et al., 2010: 48).

In the case of Equifax, the most effective way to determine accountability is by looking at the impact of the data breach on individuals. The impact experienced by individuals is mainly material losses, because consumers

will directly be harmed by the sale of their personal information without their consent after the data breach.

To provide the most effective view of liability for the losses obtained by the owner of personal data or the profits of the person/hacker who carried out the activity of breaking into consumer personal data, the following should be considered (The Editor, 2017):

1. Inventory of stolen data

   Hackers will look at the stolen data files for authentication; personal information, such as name, address and phone number; and financial information such as credit card details.

2. Selling personal information

   Hackers will package personal information, such as name, address, phone number and email address. The information will be sold; the personal information will be more valuable if the data is recent. According to Quartz (in Collins, 2018), a complete set of a person's personal information, including identification number, address, date of birth, and possibly credit card information costs between $1 and $450, with an average cost of $21.35.

3. Save important data information

   Hackers will store authentication credentials and look for potentially profitable accounts. If the information obtained is the personal data of important people, then the data will be specifically stored to be targeted for sale in the future to parties who offer higher prices.

4. Sell in bulk

   After a few months, hackers will collect authentication credentials and sell them massively at discounted prices. At that time, most of the credentials are worthless as the company has most likely discovered the breach and taken steps to fix it.

The impact of the loss above is an affirmation that a further lawsuit is needed in accordance with the regulations contained in the EIT Law and the PM Kominfo, as a form of accountability. Based on the explanation above, the case of Equifax can be categorized as an unlawful act, which leads to liability based on fault, in general, because the personal rights of consumers or the owner of personal data have been violated.

Specifically, Article 1365 of the Civil Code explains that every unlawful act, which brings harm to another person, obliges the person who, because of his

fault, published the loss, compensates for the loss. Article 1365 of the Civil Code requires the existence of certain basic elements for someone to be held legally responsible for acts against the law as follows (Fuady, 2002: 10-14):

a. The existence of an action;
b. The act is against the law;
c. There is an error on the part of the perpetrator;
d. There is a loss for the victim; and
e. There is a causal relationship between actions and losses.

In the case of the data breach at Equifax, there was failure on the part of the company to maintain the confidentiality of personal information of individuals, and there was no notification of the failure to the affected individuals. So, the first element in an unlawful act, namely "the existence of an act", has been fulfilled in this case.

The next element according to Article 1365 of the Civil Code is that the act committed must be against the law. Since 1919, this unlawful element has been defined in the broadest sense, which includes the following (Fuady, ibid):

a. Acts that violate applicable laws;
b. Who violates the rights of others guaranteed by the law;
c. Actions that are contrary to the legal obligations of the perpetrator;
d. Actions that are contrary to decency *(geode zeden*); or
e. Acts that are contrary to good attitudes in society to pay attention to the interests of others *(indruist tegen de zorgvuldigheid, welke in het maatschappelijk verkeer betaamt ten aanzein van ander person of goed)*.

Regarding the Equifax case, as previously explained, there is a violation of the provisions in Article 28 point C of the PM Kominfo regarding the obligation of the electronic system operator (Equifax) to notify the owners of personal data in writing about the beach in the electronic system it manages. Also, the company has violated the principle of good data protection. Thus, the second element ("the act is against the law") has been fulfilled.

Further, Article 1365 of the Civil Code also requires an error on the part of the perpetrator. Errors have two meanings, namely errors in a broad sense (there is negligence and intention) and errors in a narrow sense (only intentional). If a person at the time of committing an unlawful act knows very well that his actions will result in a certain condition that is detrimental to another party, that person can be held accountable and vice versa. In this case, there was an error on the part of the perpetrator, Equifax. They should have provided a notification within a predetermined timeframe (14 days) with the necessary components after the data breach. Moreover, the company knows that the impact of the data breach due to its actions or inactions will result in certain circumstances that are detrimental to the owners of the personal data. So, the element of error in the unlawful act has been fulfilled.

The 4th element is the existence of a loss (*schade*) for the victim. It is also a condition for an act to be categorized as an unlawful act. Material losses

can consist of losses that are actually suffered or profits that will be obtained by the party committing the violation. In this case, there is a loss in the form of loss of consumer's personal rights due to the leak of the information. Besides, if Equifax had notified the owners of the personal data of the breach, they could have taken quick action to reduce the losses that will be suffered. Losses due to delay in notification can be fatal, because the data that have been compromised comprise sensitive information. For example, if the credit card serial number of an individual is compromised, early notification could prevent or reduce losses as the individual can take action to freeze the card. Affected individuals suffer material losses when the card is used by another person. Thus, the element of loss regarding unlawful acts has also been fulfilled.

The last element is that there must be a causal relationship between the act committed and the loss incurred. In the adequate theory *(Adequate Veroorzaking),* Von Kries teaches that actions that must be considered as the cause of the resulting effects are actions that are balanced with the consequences (Setiawan, 1999: 87). The basis for determining a balanced action is a proper calculation. In the case of personal data theft at Equifax, the fact that the company did not notify the affected individuals within the specified grace period indicates that there is a clear cause-and-effect relationship, since data breaches that are not accompanied by direct notification to those affected (cause) will result in direct losses to them (consequences). So, it is clear that the losses suffered by the affected individuals are a direct result of the actions taken by Equifax. From the foregoing, it is evident that the data breach at Equifax fulfils all elements of an unlawful act. Therefore, Equifax can be held legally responsible for the breach, based on Article 1365 of the Civil Code.

According to Munir Faudy, unlawful acts are a collection of legal principles that aim to control or regulate dangerous behaviour, which in this case is detrimental to consumers or owners of personal data. Responsibility must be borne for a loss that arises from social interaction and compensation provided to the victims with an appropriate lawsuit (Djojodirdjo, 1982: 25-26). Regarding the nominal amount and the method of calculating the compensation, it is not explicitly regulated by the EIT Law and the PM Kominfo, but the regulations only explain that the lawsuit is a civil lawsuit and is filed in accordance with the provisions of the legislation. Therefore, the rules used for compensation refer to Article 1243-1252 of the Civil Code. Compensation according to Article 1246 of the Civil Code is broken down into 3 categories, namely (Fuady, 1999: 137):

1. Costs: Any costs that must be incurred in real terms by the aggrieved party; in this case, it is the result of an act of default;
2. Losses: The decline (decrease) in the value of the Creditor's assets as a result of default on the part of the Debtor; and/or
3. Interest is profit that should be obtained but not obtained by the Creditor, due to a default action on the part of the Creditor.

The above categories cannot simply be applied to acts that qualify as unlawful acts. This is because the assessment of the replacement size is difficult to determine. In connection with this, the provisions for compensation due to default also cannot be applied to compensation due to unlawful acts, namely those contained in Article 1247 – Article 1250 of the Civil Code. In terms of compensation due to unlawful acts, Article 1365 of the Civil Code cannot quantify the amount of loss, but it will be determined by the judge with reference to previous decisions (jurisprudence). Losses that arise due to unlawful acts cause the imposition of an obligation on the perpetrator to provide compensation to the sufferer, as far as possible, to restore the situation back to its original state, namely before the unlawful act occurred.

Based on the law and jurisprudence, there are various kinds of compensation that can be sought for under Article 1365 of the Civil Code by sufferers, as an effort to compensate for losses and restore honour. The forms of liability for such losses are:

1. Compensation in the form of money for the losses incurred;
2. Compensation in kind;
3. A statement that the act committed is against Law;
4. An act is prohibited; and/or
5. Announcement of judge's decision.

The forms of liability stated above can be applied in the case of Equifax. The most appropriate is compensation in the form of money for the losses caused, along with other compensation costs, as the data is not ordinary data that can be easily accounted for, considering that the data will be used illegally or traded. Personal data contains very sensitive information, ranging from full names, addresses, credit card serial numbers, driving license numbers, to the health records of each individual.

Conclusion

a. The legal protection of personal data provided by the EIT Law in the big data era against data breach activities is the provision of the opportunity for the owner of the personal data that have been breached to be able to file a civil lawsuit to seek redress for the loss. Meanwhile, the derivative regulation of the EIT Law, namely PM KOMINFO provides legal protection by stating that a notification of failure to protect personal data containing the reasons underlying the personal data breach should be sent to the owner of the personal data that were breached not later than 14 days from the discovery of the breach. Also, affected individuals can submit a complaint to the minister before filing a civil lawsuit against the company regarding the failure to safeguard consumer personal data.
b. The most effective liability for a company that fails to protect personal data of consumers, leading to data theft, is to pay compensation in the

form of money for the impact of losses caused to consumers, along with other compensation costs because the data is not ordinary data that can be easily accounted for, namely data with very sensitive types, ranging from full names, addresses, credit card serial numbers, driver's license numbers, to the health records of each individual. Compensation in the form of money also comes from unlawful acts committed by the company by not providing notification in accordance with the predetermined grace period.

Recommendation

a. The Government through the Ministry of Communications and Information Technology should immediately implement laws that specifically regulate the protection of personal data. Regulations related to personal data are separated into several laws and regulations, namely Law No. 11 of 2008 concerning Electronic Information and Transactions as amended by Law No. 19 of 2016, Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, and Regulation of the Minister of Communication and Information No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems. Moreover, in terms of data breach activities in the big data era, it is requested that a specific category of violation activities be compiled, considering that, currently, data breach activities are increasing in ASEAN, including Indonesia, and the origin is not only cyber attacks, but there are human errors and system glitches. This will ensure that there will be no legal vacuum. And lastly, to ensure the protection of personal data, the government needs to oblige every company that uses big data technology to improve the monitoring function of cyber security to the maximum by using legal instruments in the form of a Ministerial Decree or Ministerial Regulation related to security systems.

b. Criminal law sanctions are required for electronic system operators who do not provide notifications to owners of personal data who are victims of data breaches, and the grace period given in the regulation needs to be reviewed effectively, considering that within 14 days, personal data containing important and sensitive information would already have been used by individuals in terms of utilization and buying and selling for personal benefit. Therefore, there is no reason for companies that fail to protect personal data not to provide notifications or to provide them after the grace period.***

References

Anam, Khairul. 2010. *Hacking VS Hukum Positif & Islam* (Hacking VS Positive & Islamic Law). Yogyakarta: Sunan Kalijaga Press.

Bahar, Emirul. *Big Data*, Source: dari http://emirul.staff.gunadarma.ac.id/ Downloads/folder/0.4 Accessed: 19 Oct. 2017.

Cisco, 2017. *Cisco Annual Cybersecurity Report*.

Collins, Keith. *Here's what your stolen identity goes for on the internet's black market*. Source: https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/. Accessed: 7 July 2018.

Dewi, Sinta. 2016. *Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia (The Concept of Legal Protection for Privacy and Personal Data Associated With the Use of Cloud Computing in Indonesia*). Jurnal Yustisia, Vol. 5 Nomor 1, Januari- April 2016.

Djojodirdjo, M.A. Moegni. 1982. *Perbuatan Melawan Hukum* (Unlawful Action) 2nd Edition. Jakarta: Pradanya Paramita.

Fuady, Munir. 1999. *Hukum Kontrak Dari Sudut Pandang Bisnis* (Contract Law From the Business Perspective). Bandung: Citra Aditya Bakti.

Fuady, Munir. 2002. *Perbuatan Melawan Hukum: Pendekatan Kontemporer* (Unlawful Actions: A Contemporary Approach). Bandung: PT Citra Aditya Bakti.

Hurwitz, Judith et.al. 2013. *Big Data for Dummies*, Canada: John Wiley & Sons.

Identity Theft Resource Centre, *What Do Hackers Do With Corporate Security Breaches?*, Source: https://www.idtheftcenter.org/what-do-hackers-do-with-corporate-security-breaches/. Accessed: 28 June 2018.

Juju, Dominikus and Feri Sulianta, 2010. *Hitam Putih Facebook* (Black and White Facebook), Jakarta: PT Elex Media Komputindo.

Kementerian Komunikasi dan Informatika (Kemkominfo). 2015. *Buku Saku Big Data* (Big Data Pocket Book) Jakarta: Kementerian Komunikasi dan Informatika.

Kementrian Pendidikan dan Kebudayaan, *Bahan Sajian Penyusunan Arus Siswa*, (Student Flow Preparation Materials) diakses di http://sdm.data.kemdikbud.go.id/upload/files/15Arus%20Siswa%20Revisi.pdf. Accessed: 7 Oct. 2017.

Naughton, John. 2017. *It's one rule for big data, another for its 143 million victims*, Source: https://www.theguardian.com/commentisfree/2017/sep/17/equifax-data-breach-one-rule-for-credit-agency-another-for-143-million-victims. Accessed: 19 Oct. 2017.

Notoatmojo, Soekidjo. 2010. *Etika dan Hukum Kesehatan* (Health Ethics and Law), Jakarta: Rineka Cipta.

Nugraha, Radian Adi. 2012. *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-undang Informasi Dan Transaksi Elektronik* (Juridical Analysis Regarding the Protection of Personal Data in the Cloud Computing System in terms of the Information and Electronic Transaction Law). Skripsi, Depok: Fakultas Hukum Universitas Indonesia.

Pawitra, Puruhita Mega. 2016. *Big Data*, Surakarta: Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sebelas Maret.

Rahardjo, Satjipto. 2000. *Ilmu Hukum* (Legal Science), Bandung: PT. Citra Aditya Bakti.

Syarah, 2009. *Perkembangan Teknologi Informasi dan Komunikasi; Faktor-faktor yang Mempengaruhi Serta Pemetaan Kondisi TIK*, (Development of Information and Communication Technology; Influencing Factors and Mapping of ICT Conditions). Skripsi, Depok: Fakultas Matematika Dan Ilmu Pengetahuan Alam Departemen Matematika Universitas Indonesia.

Setiawan, Rachmat. 1999. *Pokok-Pokok Hukum Perikatan* (Principles of the Law of Agreement). Bandung: Putra Abardin.

Triwulan, Titik and Shinta Febrian, 2010. *Perlindungan Hukum Bagi Pasien* (Legal Protection for Patients), Jakarta: Prestasi Pustaka.

The Editor (Security Simplified), *Once Stolen, What Do Hackers Do With Your Data?*, Source: https://www.secplicity.org/2017/05/18/stolen-hackers-data/. Accessed: 28 June 2018.

United States Securities and Exchange Commission, *Equifax Inc. Annual Report* (*Form 10-K*), 31 Desember 2017. Source: https://www.sec.gov/Archives/edgar/data/33185/000003318518000011/efx10k20171231.htm#s24891C96B2CB5057988EF8DF94F2F40B. Accessed: 23 June 2018.

Xiaomeng Su. 2016. Introduction to Big Data, Norway: Norwegian University of Science and Technology.