Corporate Criminal Liability for Leakage of Personal Data

Muis Ari Guntoro[1], Sanusi[2], Fajar Ari Sudewo[3]
{muisariguntoro@gmail.com}

Magister of Law, Universitas Pancasakti Tegal, Indonesia

Abstract. The type of research used in this thesis is normative juridical (legal research), using a statutory approach, and a conceptual approach. The problems in this thesis are: Regulation of personal data protection in Indonesian legislation and Corporate Criminal Liability for Personal Data Leakage. Personal data is an asset or commodity of high economic value. In addition, there is a correlative relationship between the level of trust and the protection of certain data from personal life. Protection of personal data is currently not regulated in a separate law but is still spread in various laws and regulations. Legal provisions related to the protection of personal data are still partial and sectoral, it seems that they have not been able to provide optimal and effective protection of personal data, as part of privacy. Seeing the victims of corporate crime in the criminal act of leaking personal data, it is very natural that the corporation must be responsible for all of its actions. The forms of losses and also the consequences of corporate crimes cannot be felt immediately (actual victims) but can only be felt and seen at a later time (potential victims). The victims of corporate crime include rival companies (competitors), consumers and the public (public) in general. As in the case of personal data leakage on Tokopedia, the victims are consumers who fall into the category of potential victims.

Keywords: Personal Data, Criminal Liability, Corporate

1. Introduction

The concept of the right to privacy became popular in 1890 when Samuel Warren and Louis Brandeis wrote an essay entitled, "The Right to Privacy," which was published by the Harvard Law Review. They proposed the recognition of individual rights “right to be let alone” and also argued that this right should be protected by existing law as part of the human rights issue. Thus, the concept of the right to privacy has been recognized but is still difficult to define. Privacy, as part of human rights, identifies the protection of personal data as an important right. The right to privacy through data protection is not only important but also a key element for individual freedom and dignity. Data protection is a strong driver for the realization of political, spiritual, religious freedom and even sexual activities[1–3].

In Indonesia, regulations related to personal data and the right to privacy of a person are contained in the Indonesian constitution as previously stated, and also regulated in 1 article in Law Number 19 of 2016 which contains Amendments to Law Number 11 of 2008 concerning Information and Transactions. Electronic information in Article 26. Article 26 of the ITE Law regulates how any electronic information containing personal data may only be used with the permission of that person. There is also Government Regulation (PP) No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. For the specific regulation, it is still up to the Ministerial Regulation, namely the Minister of Communication and Information Regulation Number 20 of 2016 concerning Privacy Data Protection in

MALAPY 2022, May 28, Tegal, Indonesia

DOI 10.4108/eai.28-5-2022.2320539

Electronic Systems. Meanwhile, in Singapore, regarding the Protection of Personal Data, guarantees have been given to the Act, namely the Personal Data Protection Act 2012 which was just amended in 2020, as well as the Public Sector Governance Act 2018. In Indonesia, until now there is no specific law regarding the protection of privacy and data. personal. Therefore, as technology is developing rapidly today, laws for the protection of privacy and personal data are becoming increasingly urgent. The existing law is considered ineffective, especially in following the development of the use of technology itself[4–6].

Recently, the issue of leaking personal data and offering transactions for leaked personal data has resurfaced. The incident hit corporate-managed personal data. Of course the public becomes worried and questions why these incidents often occur and it seems that there is no law enforcement. All incidents of personal data leakage seem to be over with just the news. Corporations and related agencies seem to simply notify the public by issuing statements and clarifications. This causes the perpetrators of personal data theft to walk freely to carry out these actions and feel as if they are free to buy and sell personal data as their livelihood by making offers through darknet sites.

Incidents of personal data leakage, of course, do not only occur due to attacks from outside, because they may be an act of disclosure from within the organization or corporation itself. One of the data leak incidents that shocked the public was the widespread circulation of President Jokowi's vaccination certificates on social media due to the leaking of the President's population identification number (NIK), in addition to information regarding the name, date of birth, date of vaccine, and the type of vaccine used by Jokowi. widely circulated on social media where it is very unfortunate. To clarify this, of course, it is necessary to prove that it is impossible to rely solely on the statement of one party, but must also be proven by other parties or related agencies. The government through sectoral agencies in accordance with the authority granted by law, has the duties and functions as well as the authority to supervise the protection of the public's personal data. They are worried that the public will judge as if there is no legal awareness for corporations and related agencies to protect people's personal data. It seems as if there is no effort that can be made by the community to demand better protection, because it seems that corporations and related agencies only look down on this matter, because the incident happened repeatedly without clear law enforcement. Is there really no rule of legal responsibility by the organizer of the electronic system for the data leak? Should the public wait for the Personal Data Protection Bill (RUU PDP) to be ratified first before the action can be held legally responsible.

In general, within the scope of criminal law, data leakage can occur due to intrusion from outside (illegal access) into the system or outside the system (interception or man in the middle attack). But maybe, leakage might also occur from the action leakage from an insider who sends the data outside the system, where the insider should maintain the confidentiality of the user's data. As the controller and data processor, the corporation must be responsible for the security system both physically and logically. At least the act of theft or leakage can basically optimize the provisions of Article 30 and Article 32 of the ITE Law, regarding illegal access and data interference[7–10].

In addition, criminal liability should not release those who are the custodians, including the organizers of darknet sites that become black-market. Offering personal data obtained illegally is like trading stolen goods on the black market as regulated in Article 480 of the Criminal Code. Apart from the main actors, of course, there are accompaniment actions that must be pursued by law enforcers, such as corporations and agencies that intentionally do not own and maintain their electronic security system for proper management of personal data. It should also be said to be responsible for providing the means to commit crimes to the public.

The problems that will be discussed in this research are: How is the regulation of personal data protection in the legislation? What is the corporate criminal responsibility for the leakage of personal data?

2. Method

The research for this paper uses a normative juridical research type (legal research). This type of normative juridical research is carried out by examining various legal rules of a formal nature such as laws, regulations related to the issues discussed. The problem approach method used in the preparation of this thesis is the statute approach, the conceptual approach and the comparative approach[11].

3. Result & Discussion

3.1. Personal Data Protection Regulations in Indonesian Laws

1) Laws and Regulations in Indonesia Regarding Personal Data

So far, Indonesia does not have a policy or regulation regarding the protection of personal data in a special regulation. Regulations regarding this matter are still contained separately in several laws and regulations and only reflect aspects of personal data protection in general. In the existing legislation in Indonesia, there are several laws that pertain to personal data, including :

a) Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration (Population Administration Law)

b) Law Number 7 of 1971 concerning Basic Provisions for Archives (Law on Archives)

c) Law Number 36 of 1999 concerning Telecommunications (Telecommunication Law)

d) Law Number 14 of 2008 concerning Public Information Disclosure (Public Information Disclosure Act)

e) Law Number 10 of 1998 concerning Banking (Banking Law)

f) Law Number 29 of 2004 concerning Medical Practice (Medical Practice Law)

g) Law Number 36 Year 2009 concerning Health (Health Law)

h) Law Number 43 of 2009 concerning Archives (Archives Law)

i) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Transaction Information (UU ITE)

2) The Need for Personal Data Protection Arrangements in Indonesia

The issue of the importance of protecting personal data began to strengthen along with the increasing number of cellular phone and internet users. A number of cases that have emerged, especially those related to the leakage of a person's personal data and lead to acts of fraud or pornography crimes, reinforce the discourse on the importance of making legal rules to protect personal data. Protection of personal data is related to the concept of privacy. The concept of privacy itself is the idea of maintaining personal integrity and dignity.

The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used. The right to privacy through data protection is a key element for individual freedom and dignity. Data protection is a driving force for the realization of political, spiritual, religious freedom and even sexual activities. The right to self-determination, freedom of expression and privacy are rights that are essential to making us human. The collection and dissemination of personal data is a violation of a person's privacy because the right to privacy includes the right to determine whether or not to provide personal data.

Personal data is an asset or commodity of high economic value. In addition, there is a correlative relationship between the level of trust and the protection of certain data from personal life. Unfortunately, the protection of personal data is currently not regulated in a separate law but is still spread across various laws and regulations as reviewed in the previous sub-chapter. Legal provisions related to the protection of personal data are still partial and sectoral, it seems that they have not been able to provide optimal and effective protection of personal data, as part of privacy.

The potential for violation of privacy rights over personal data does not only exist in on-line activities but also off-line activities. The potential for privacy violations of personal data on-line, for example, occurs in mass personal data collection activities (digital dossier), e-commerce transactions, direct marketing (direct selling), social media, implementation of the e-KTP program, implementation of e-health programs and cloud computing activities.

The arrangements that will be drawn up in the Personal Data Protection Bill are expected to place Indonesia on a par with developed countries that have implemented laws regarding personal data protection. This will further encourage and strengthen Indonesia's position as a trusted business center, which is a key strategy in Indonesia's national economy. In addition, the regulation regarding the protection of personal data will minimize the threat of misuse of personal data in the e-commerce industry, banking, online friendship sites (eg Facebook, My Space, Twitter, Path, Google Plus), electronic ID cards (e-KTP), e-health. . The potential for crime stems from searching for someone's personal data, removing the identity of data from criminals, search engines (eg google.com and bing.com), and cloud computing. Taking into account all the threats and potential violations above, personal data protection arrangements are intended to protect the interests of consumers and provide economic benefits for Indonesia.

Seeing the developments that have occurred, informatics law experts try to develop the principles of how this personal information should be managed is known as fair information practices. These principles are standard principles used in practice (standard practice) by the public and private sectors so that consumer privacy is protected. This principle was first used by the Department of Health, United States in 1973 because at that time the use of computers to process and store population data had been misused by certain parties so that a lot of population health data fell into the hands of manufacturers of drugs and related health products. others for marketing purposes. Fair Information Principles are as follows :

1. Principle of limitation (collection limitation): The collection of public personal information should be limited to its original purpose.
2. Disclosure: Individuals must be informed about the purposes for which their personal information is collected and disseminated.
3. Secondary usage: Individuals can refuse other parties to collect their personal information without asking for prior consent.
4. Correcting data (record correction): there must be a mechanism that allows someone to be able to correct their personal information.
5. Security: Government agencies that manage and collect a person's personal information are obliged to ensure the security of the information they manage to avoid the misuse of information by others.

In fact, then these principles are widely used by government and private agencies in managing public information in the United States and then encourage the United States government to make laws on the protection of privacy, namely the Privacy Act, 1974 and internationally has inspired to To be able to apply Fair Information Principles internationally, finally in 1980 the OECD developed Guidelines which normally accommodate Fair Information Principles derived from practice in the United States.

In addition, the FTC (Federal Trade Commission), which is a federal agency that handles business competition in the United States, also issues the principles of fair information practices, namely :

1. The principle of notification (Notice/Awareness)

This principle is the most basic and important principle because consumers must be informed in advance that their personal information will be accessed. Although the contents of the notification are submitted to each institution, in practice it must include:

1) the identity of the institution that will collect the information;
2) identification of the company that will store the information;
3) identification of other parties who will use the information;
4) the purpose of data collection; and
5) what steps will be taken to secure the information.

In addition, there are also institutions that list other consumer rights, such as the right of consumers to be able to access their information, the right to correct information that is no longer accurate. In e-commerce transactions, the notification must be included and the way it is presented must be clear and not confusing to consumers.

2. The principle of choice or consent (choice/consent)

This principle gives consumers the choice to approve or reject the use of their personal information by third parties. This process is very important with regard to the use of their information by third parties or called secondary uses or the use of information for purposes other than the agreed transaction, for example the use of information to be stored in consumer data, or for marketing purposes for other products, or the information is transferred to third parties. third. Currently, there are two kinds of notification (consent), namely the first is called opt-in, the consumer must give express approval before the information is collected/used by other parties. Second, opt-out, consumers are asked for consent when the information will be transferred.

3. The principle of access (access / participation)

This principle provides an opportunity for consumers to be able to access their personal information which is in the hands of certain companies and are given the opportunity to check the accuracy of their information and the process must be designed as easy as possible and consumers should not be charged.

4. Information integrity and security principles

This principle is very important, namely that the second party must maintain the integrity and security of information both technically, for example through encryption technology, passwords and good corporate management such as company internal security, especially preventing the data it manages from being used by irresponsible parties.

5. Implementation of the above principles (enforcement/redress)

The above principles can be applied effectively if there is an enforcement mechanism. when not these principles are only in the form of recommendations so that their compliance depends on the good faith of each party. For the effectiveness of this principle, it is necessary to use a mechanism or use a self-regulatory model implemented by the industry or use laws that impose sanctions on parties who violate the principles above.

1) Self-regulation (self-regulation)

To be effective, self-regulatory arrangements must also regulate the sanctions that will be applied to those who violate. For example: being expelled from the association or not being given a certificate showing the company's compliance. In the event of a violation, the consumer must receive compensation.

2) Through government regulation (government enforcement)

The government issued a law that would provide compensation and criminal penalties. In addition to the principles above, the FTC also requires the industry to apply the Fair Information Principles, especially children's personal information. This principle is applied because children often search for data through the internet and in practice they are often asked to fill in their personal information so that in many cases their personal information is used to sell toys, games, or to send pornographic content. This principle requires parental consent in advance, namely :

(1) Parental notice/awareness and parental choice/consent

Parents must receive notification and consent in advance that children's personal information will be collected by certain industries. To facilitate the mechanism must be made easy and simple. In addition, it must provide opportunities for parents to supervise it. Basically, the industry should not ask children directly for their personal information such as email numbers, addresses and telephone numbers.

(2) Access/participation, integrity and security

This principle requires the industry to provide opportunities for parents to access information and also to correct the accuracy of children's personal information. In addition, the industry is also required to secure the personal data it manages.

In addition, the need for a Personal Data Protection Law, it is also necessary to pay attention to relevant principles to serve as the basis for formulating norms in the Personal Data Protection Bill, including :

1) Protection Principle

The principle of protection is very relevant to the Personal Data Protection Bill because basically the existence of this law is intended to provide protection to data owners regarding their privacy, regarding their personal data, regarding their rights to data so that the data is not misused to the detriment of the interests of the data owner.

2) Principle of Public Interest

The principle of public interest is very important to be one of the principles of the Personal Data Protection Bill, because it is the public interest that can be used as a valid reason, according to the formulation of the law, as a reason to break through or as an exception to privacy protection for personal data. These public interests include, among others: state security, state sovereignty, eradicating corruption and other criminal acts.

3) Balance Principle

The principle of balance is also an important principle that needs to be considered as the basis for the formulation of norms in the Personal Data Protection Bill, because the arrangements in this law actually reflect efforts to balance privacy rights on the one hand with legitimate state rights based on interests. general.

4) Principle of Accountability

The principle of responsibility provides a basis for all parties related to the processing, dissemination, management and supervision of personal data to act responsibly so as to ensure the balance of rights and obligations of the parties involved, including the data owner.

Taking into account all the threats and potential violations described above, the personal data protection arrangements are intended to protect the interests of consumers and provide economic benefits for Indonesia. This arrangement will protect the personal data of each individual against misuse when the data has a high value for business purposes, whose collection and processing has become easier with the development of information and communication technology. The development of regulations on the protection of personal data in general will place Indonesia on a par with countries with advanced economic levels, which have implemented laws regarding the protection of personal data. This will strengthen and

strengthen Indonesia's position as a trusted business and investment center, which is a key strategy in Indonesia's economic development.

For the benefit of consumers, the need for the protection of consumer personal data, especially in an era where personal data is very important valuable for business purposes, raises concerns that consumer personal data is sold or used without the consumer's consent as examples of violations described previously. Therefore, the protection of personal data that is specific in a law is very necessary to ensure that consumer personal data is properly protected. For economic development, the protection of personal data of a special nature will strengthen Indonesia's position as a trusted business and investment center and create a conducive environment for the growth of global data management and data processing industries such as cloud computing to thrive in Indonesia.

In addition, in 2019, the Indonesian government again proposed the Personal Data Protection Bill as a form of refinement of various existing laws and regulations. This Personal Data Protection Bill consists of 72 articles, and has gone through various stages of discussion. The provisions for criminal sanctions are regulated in the 2019 Personal Data Protection Bill. The criminal provisions in the 2019 Personal Data Protection Bill are quite detailed, namely those related to the acquisition and collection of personal data, disclosure of personal data, use of personal data, installation and use of on-site visual processing devices. public or public service facilities, falsification of personal data for the benefit of oneself or others or causing harm to others, as well as the sale or purchase of personal data. There are several differences that are refinements to the Personal Data Protection Bill, including:

What needs to be appreciated is that punishment can not only be imposed on individuals, but also on corporations, which means that punishments can also be imposed individually on administrators, controllers, order givers, and even beneficial owners. Electronic System Operators in this case must be more careful because it means they are included in this Corporate category. In addition to crime, other sanctions that may be received by the Electronic System Operator are confiscation of profits from a criminal act, freezing of all or part of its business, permanent prohibition from carrying out certain actions, closing all or part of the place of business and/or activities of the Corporation, carrying out obligations that have been neglected, to the payment of compensation. These are all regulated in Articles 61 to 64 of the 2019 Personal Data Protection Bill.

2. Corporate Criminal Liability Against Personal Data Leaks

The term liability or commonly known as liability in terms of legal philosophy, Roscoe Pound states that: "I..use simple word liability for the situation whereby one may exact legaly and other is legally subject to the excaxtion". an obligation to pay the retaliation that the perpetrator will receive from someone who has been harmed. In corporate criminal liability, there are several theories that can be used as the basis for corporate punishment, as for these theories, including :

a. Direct Corporate Criminal Liability Theory

In countries that adhere to the Anglo-Saxon legal system, such as England and America, the theory of direct corporate criminal liability is known. According to this theory, corporations can commit a number of offenses directly through agents who are closely related to the corporation, acting for and or on behalf of the corporation. They are not substitutes and therefore, corporate liability is not personal. The requirement for direct corporate criminal liability is that the actions of these agents are still within the scope of the corporation's work.

The existence of a corporation, according to the theory of direct corporate criminal liability, is independent in terms of its criminal liability. Therefore, it cannot be equated with

the vicarious liability model. Thus, the actions or activities carried out by individuals do not represent the corporation, but are considered the actions of the corporation itself. When the individual makes a mistake, by itself the mistake is basically the fault of the corporation. In short, individual error is synonymous with corporate error.

b. Strict liability theory

Strict liability is defined as a criminal act by not requiring any fault on the part of the perpetrator against one or more of the actus reus. This strict liability is a liability without fault. With the same substance, the concept of strict liability is formulated as the nature of strict liability offences is that they are crimes which do not regulate any mens rea with regard to at least one element of their "actus reus". Absolute responsibility is a form of violation or crime in which it does not require an element of error, but only requires the existence of an act).

Another opinion regarding strict liability is expressed by Roeslan pious as follows : In practice, criminal liability disappears, if one of the circumstances forgives. The practice also gives birth to various levels of mental conditions that can be a condition for the abolition of the imposition of a crime, so that in its development a crime group is born which is sufficient for handling the crime with strict liability. In a criminal act that is strict liability, all that is needed is the suspicion or knowledge of the perpetrator (the defendant), and that is enough to demand criminal responsibility. So, there is no question about the existence of mens rea because the main element of strict liability is actus reus (actions), so that what must be proven is actus reus (deeds), not mens rea (errors).

According to Romli Atmasasmita, the legislators have determined that the rules regarding strict liability crimes can be enforced as follows :

a) The crime committed is not a serious crime;
b) The applicable penalty is light;
c) The requirement for the existence of mens rea will hinder the purpose of the legislation;
d) Crimes committed directly constitute coercion on the rights of others;
e) According to the applicable law, mens rea is not necessary.

Barda Nawani Arief argues that the strict liability theory, according to English criminal law, is only applied to cases of minor violations, such as violations of public order or public welfare. Included in the categories of violations mentioned above are:

a) Violation of court order;
b) Defamation of a person;
c) Disturbing public order.

However, most of the strict liability is found in offenses regulated in law (statutory offenses regulatory offenses, mala probhitia) which are generally offenses for public welfare. Including regulatory offenses are the sale of harmful food and drink or drugs, the use of misleading trade images, and traffic violations.

c. Vicarious Liability Theory

Vicarious Liability, commonly referred to as substitute liability, is defined as a person's legal liability for wrongdoing committed by another person. Barda Nawawi argues that vicarious liability is a concept of a person's responsibility for mistakes made by others, such as actions taken that are still within the scope of his work (the legal responsibility of one person for wrongful acts for another, as for example, when the acts are done within the scope of employment).

The principle of working relations in vicarious liability is called the principle of delegation, which is related to granting permission to someone to manage a business. The

license holder does not run the business directly, but he gives full trust (delegates) to a manager to manage the corporation. If the manager commits an unlawful act, then the permit holder (delegator) is responsible for the manager's actions. On the other hand, if there is no delegation, the delegate will not be responsible for the manager's crime. An interesting example of this lack of delegation is presented as follows:

A permit to open a restaurant that serves alcoholic beverages can only be sold and granted to someone who orders food. The waiter sold the drink to someone who didn't order food. The license holder was charged with violating Article 22 (1) of the Licensing Act 1961, on the basis of knowledge of selling alcoholic beverages. The license holder is not aware of the servant's actions. Prosecutors ignored the defense. The Supreme Court accepted the permit holder's defense so that the employer was not penalized.

Meanwhile, according to Marcus Flatcher, in a criminal case, there are two important conditions that must be met to apply a criminal act with substitute liability, these conditions are as follows:

a) There must be an employment relationship, such as that between an employer and an employee or worker;
b) The criminal act or crime committed by the employee or worker is related to or still within the scope of his work.

According to statute law, vicarious liability or substitute liability can occur in the following cases:

a) A person can be charged with criminal responsibility for actions committed by other people, if there is a delegation (the delegation principle).
b) A person can be charged or the employer can be held accountable for his actions which is physically carried out by the employee if according to the law, the act is seen as the employer's act.

4. Conclusion

Personal data is an asset or commodity of high economic value. In addition, there is a correlative relationship between the level of trust and the protection of certain data from personal life. Protection of personal data is currently not regulated in a separate law but is still spread in various laws and regulations. Legal provisions related to the protection of personal data are still partial and sectoral, it seems that they have not been able to provide optimal and effective protection of personal data, as part of privacy.

Seeing the victims of corporate crime in the criminal act of leaking personal data that is so widespread, it is very natural that the corporation must be responsible for all its actions. The forms of losses and also the consequences of corporate crimes cannot be felt immediately (actual victims) but can only be felt and seen at a later time (potential victims). The victims of corporate crime include rival companies (competitors), consumers and the public (public) in general. As in the case of personal data leakage on Tokopedia, the victims are consumers who fall into the category of potential victims.

References

[1] Wahyudi Djafar dan Asep Komarudin, Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci. Jakarta: Elsam; 2014.

[2] Freeman M, Ert G. International Human Rights Law. Canada: Irwin Law Inc; 2004.

[3] Huda C. Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan, Cet. Kedua, Jakarta: Prenada Kencan; 2006.

[4] Saleh R. Tindak Pidana dan Pertanggungjawaban Pidana". Jakarta: Aksara Baru; 1983.

[5] Marpaung L. Proses Penanganan Perkara Pidana. Jakarta: Sinar Grafika; 2011.

[6] Jayawickrama N. The Judical Application of Human Rights Law, National. United Kingdom: Regional and International Jurisprudence; 2006.

[7] Suheryadi B. Penanggulangan Kejahatan Korporasi Dalam Perspektif Kebijakan Hukum Pidana. Yuridika n.d.;18:79–98,.

[8] Adriano KPPK, Disertasi. Fakultas Hukum Universitas Airlangga. Jurnal Hukum Dan Peradilan n.d.;5.

[9] Reid ST. Criminal Law. Third. New Jersey: Prentice Hall; 1995.

[10] Sudarto HPI. Badan Penyedia Bahan-Bahan Kuliah. Semarang: FH UNDIP; 1988.

[11] Hamzani I. Achmad "Pendekatan-pendekatan dalam Penelitian Hukum", Bahan Kuliah Metodologi Penelitian Hukum. Fakultas Hukum Universitas Pancasakti Tegal; n.d.