International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 09-06-2024, Accepted: 29-06-2024, Published: 23-07-2024
Volume 6, Issue 3, 2024, Page No. 151-157

Concept of legal protection for victims of dissemination personal data in Indonesia

Nur Khalimatus Sa'diyah, Umi Enggarsasi
Faculty of Law, Wijaya Kusuma Surabaya, University Dukuh Kupang, Surabaya, Indonesia

Abstract
The rapid development of information technology causes changes in people's needs and lifestyles, the utilization of information technology can be felt both in the fields of education, economics and others, things related to the development of science, science and so on can be easily accessed, so that a lot of information that we can receive quickly and easily. However, the development of information technology not only provides benefits to society but can also result in various problems that can harm society, such as data misuse, data dissemination, theft of personal data, sale of personal data, fraud and others. With the misuse of personal data, there are weaknesses in the system and lack of supervision, so that personal data can be misused and cause losses to the owner of the data. Legal protection regarding personal data is still lacking in providing protection to owners of personal data who suffer losses due to data theft or criminal acts of dissemination of personal data and so on. Many cases occur regarding the theft of personal data which is often carried out by the perpetrators to gain profit. Victims of cases of personal data theft and dissemination of personal data are clearly affected and severely harmed. Starting from the money in the application that is lost and personal data that can also be traded and even sold on the dark web. Therefore, legal protection for victims of personal data dissemination is needed.

Keywords: Legal protection, personal data, victims, criminal offense

Introduction

The 4.0 to 5.0 Industrial Revolution, which can all be controlled from anywhere through the web and related gadgets, and the current consequences are enormous when technology-based innovations are used by individuals in their daily lives, for example, to improve work efficiency, build financial connections, and help make things easier [1]. The advancement of computer-based data information technology innovations has developed rapidly in the public. These groups of people are then facilitated by technological developments [2]. This reason legitimizes the lack of open attention to security, especially related to the protection of one's own identity. It is very easy for the general public in Indonesia to tell others, their place of residence, date of birth, and all against their connections. In addition, it is customary in Indonesia to show one's identity Card or other individual ID, which includes one's personal information to outsiders, for example when entering a place or building. Online media users in Indonesia generally straightforwardly disclose their unique place of birth (place of residence), date, month and year of birth, phone number, and relationship with guardians or relatives [3]. A consequence of the review also led by the Association of Indonesian Network Access Providers (APJII) of the information over the previous three years starting from 2016-2018 continues to grow, seen in 2016 network access clients were 132.7 million or comparable to 51.7% of the population at 256.2 million individuals, in the following year 2017 increased by 143.26 million clients or equal to 54.68% of the population at 262 million individuals, and in 2018 web access clients have reached 171.17 million clients or an increase of 10.12% from last year's population which is currently 254.16 million. So, it is inevitable that locales that are expected to remember individual information for records will be empowered against things that can harm the information owners of their records. Concerns about the misuse of individual information are likewise seen that a rate of 59% of web clients feel uneasy assuming that their own information is being misused by certain organizations or gatherings with just advantageous thought processes affecting the information proprietors [4]. Meanwhile, in the news from 2019 to May 14, 2024, the Ministry of Communication and Information (KOMINFO) has handled cases of personal data abuse, especially personal data leaks, as many as 111 cases [5].

Indonesia has many regulations regarding the protection of individual data but they are scattered across several regulations. Indonesia does not yet have explicit regulations and guidelines governing the protection of legitimate individual data that can be the answer in many areas of various cases related to the misuse of individual identities. Currently, Indonesia already has a Personal Data Protection Law. This Personal Data Protection Law should also be concentrated on more deeply considering the fact that the Law has weaknesses in its guidelines. Everyone has the choice to protect their own information. Furthermore, assuming that one provides information to others carelessly, this can turn into a law-breaking act that will land one in jail. In the regulations on population organizations, population data can be provided by certain state organizations.

The legitimate principles of disseminating another person's data or identity are set out in the laws and regulations and subsequently the Electronic Information and Transaction Law. In accordance with managerial regulations, a person can be sentenced to a maximum of 2 years and 8 months in prison for sharing someone's individual information without consent. In this case, the misuse of a person's data dissemination meets the main elements of a criminal offense such as the elements of the crime of theft and the elements of the crime of fraud and other criminal offenses both in terms of objective elements and subjective elements. The crime of dissemination of identity confidentiality, which is a crime that originated from the use of information

technology era that resulted in social media, allows a person's personal information to be opened in cyberspace.

There are several cases related to the criminal act of disseminating identity confidentiality. One of the objects targeted by cybercrime perpetrators is Personal Data [6]." The crime of dissemination of personal data confidentiality that occurred to Andreas who had been presented by the bank demanding to pay off debts as a customer, even though Andreas did not feel that he had borrowed or made debts to the bank at all. However, Andreas said that 2 years ago he used an online KTA from another bank for urgent needs with the lure of various attractive prizes and even a series of very easy and super fast processes. From this, Andreas assumed that the confidentiality of his identity had been disseminated. With the development of technology that has existed, it is misused by people who are only looking for profit but cannot be held accountable for their actions [7].

Adi and Abdul are individual victims of personal identity data misuse. The cases experienced by these two people remind us of the importance of protecting personal identity data [8]." Although personal identity data has been kept confidential, the Marriott Hotel was also victimized. The size of a brand cannot guarantee the confidentiality of its customers' personal data. Like the Marriott Hotel, which could not protect 500 million guests' personal data from hackers who could access guests' names, phone numbers, email addresses, passport numbers, dates of birth, and credit card information that could potentially be misused. In addition, a taxpayer named Adi in Banyuwangi claimed to have been visited by tax officers to pay off arrears of Rp. 32 billion, which previously on May 23, 2018 he received a tax bill. The NPWP and tax were related to the transactions of six bankrupt businesses using his name and identity, but Adi never established a company. The formulation of the problem to be studied is: how is legal protection for victims of personal data dissemination?

Methods

The research method used in this research is Normative Juridical, with field research, namely examining the applicable legal provisions and what happens in reality in society. namely applying a statutory approach (Statue Approach), by understanding the laws relating to the content and regulation of the problem. In addition, using a conceptual approach and case approach.

Discussion

Dissemination of Personal Data

Identity theft or dissemination is an activity of moving or using without permission a person's means of identification with the aim of carrying out unlawful activities. Therefore, all information related to identity is advised not to be shared publicly via any means including social media and chat applications because no matter how small the identity you share, it is vulnerable to being misused by criminals [9]. Advances in digital technology penetrate all sides of people's lives, access to information is quickly easy to receive even in extreme conditions, a fraudster can collect a person's personal identity to be stolen little by little which will be used either to impersonate another person (impersonate) with the aim of benefiting from the victim or used to access your personal account illegally or without permission [10].

1. Definition of Personal Data Dissemination (Doxing)

Doxing is an internet-based action to research and disseminate personal information (including personal data) of individuals or organizations to the public [11]. According to Honan in David M Douglas, the term doxing comes from dropping documents or dropping dox which means dropping dox on someone which was a form of revenge in the 1990s. The Government Regulation of the Republic of Indonesia on the Implementation of Electronic Systems and Transactions explains that personal data is any data that can be identified and/or identified individually or in combination with other information directly or indirectly through electronic and/or non-electronic systems. Meanwhile, the Regulation of the Minister of Communication and Informatics explains personal data as certain individual data that is stored, maintained, and kept correct and protected confidential.

2. Types of Personal Data Dissemination

David M Douglas divides doxing into three types, including the following.

a. Deanonymization Doxing

Deanonymizing doxing means publicly sharing data that explains a person's true identity that was previously known by a pseudonym. This type of doxing involves the public disclosure of a person's identity regardless of whether or not the person intended to hide their identity.

b. Targeting Doxing

Targetting doxing means revealing a person's identity through physical presence whether it is through a phone number or email. Targetting doxing is a type of doxing that increases the physical accessibility of the subject by establishing clarity which includes where a person lives or where a person works. Although it is almost the same as deanonymizing doxing, the difference with targeting doxing is the type of personal data that is spread, targeting doxing spreads personal identity such as home address, campus address, college major, or office address.

c. Delegitimation Doxing

Doxing is sharing personal information that aims to undermine a person's reputation, character, or credibility so as to try to humiliate someone, this type of doxing is often also referred to as violating social norms.

Types of Criminal Offenses of Sharing Personal Data Confidentiality

1. Cyberstalking in the Dissemination of Privacy

Cyberstalking is a form of criminal behavior that involves unsolicited threats or excessive attention to the use of the internet and other forms of computer communication that are highly detrimental to the victim. When viewed literally, it can be understood that this action is a model of stalking in cyberspace with the aim of seeking personal information [12]. The motives of the perpetrators of this online stalking action can be various. This is done by the perpetrator starting with digging up the victim's information such as social media, even friends and family on social media in order to get more personal information, such as phone numbers, email addresses, and so on. After getting the victim's information, the perpetrator will usually continue to terrorize or harass the victim. Starting from sending messages, continuous

phone calls and accompanied by threats or unwanted requests.

Cyberstalking as an act followed by other acts such as threatening, harassing, harassing someone, making false accusations (defamation), which is carried out continuously using electronic devices or internet media, by someone who is not or has not been known to the victim or known. Cyberstalking in the dissemination of one's identity confidentiality has the intention that the perpetrator stalks the victim in cyberspace by creating an anonymous social media account or what is commonly called a pseudonym and operating the account to stalk others. Then, the perpetrator sends a message to the victim where the content of the message is in the form of an invitation / trick, or even provides a threat to frighten the victim so that they continue to interact with the perpetrator with the aim of obtaining personal data information. With this without realizing it, the victim has given the confidentiality of her identity to the perpetrator from the attraction of the invitation or threat given by the perpetrator. Based on these elements, it can be said that it can cause the confidentiality of a person's identity to be disseminated. Of the 33 studies examined, 45% specifically defined the minimum number of repetitions of the behavior required to classify the behavior as "cyberstalking", although there were some differences in the number of behaviors defined across studies [13].

2. Data Commercialization in the Dissemination of Personal Data Confidentiality

Data commercialization is the act of using one's personal data in the business world without the consent of the data owner. On the one hand, business owners get economic benefits from a person's personal data, while data owners do not benefit from their personal data. With the misuse or exploitation of personal data, it can be said to be a criminal offense, especially if there is data trading or misuse of data without permission. Practices in the business world do face the protection of one's privacy, on the one hand, business actors get economic benefits from their personal data. economic benefits from other people's personal data, on the other hand, the data owner does not benefit from his personal data [14].

The cormesialization of data in the spread of confidentiality of one's identity is related to the protection of personal data, with the existence of this, it has an impact on us such as offering certain products or getting terrorists such as asking for credit, etc. It is very possible that there are groups or individuals who are interested in the protection of personal data. It is very possible that there are groups or individuals who collect our data on the internet, on social media and then trade it. So that sometimes we do not give or submit to anyone but there are still those who carry out acts of terror, then if it is related to banking matters if there is commercialization of data such as loan offers, gold loan offers, etc. If it is related to company matters, for example consumer data, then the company asks for our data for certain purposes but the company instead commercializes or trades the data, so that previously consumers only provided data for certain purposes but instead it was misused. With the commercialization of data without the consent of the owner, it contains clear elements that this is classified as a criminal offense.

3. Interception or Data Tapping in the Dissemination of Personal Data Confidentiality

Data interception/tapping is the activity of listening to, recording, altering, obstructing, and/or recording the transmission of electronic information and/or electronic documents that are not public by using wired communication networks or wireless networks, such as electromagnetic beams or radio frequencies. What is meant by tapping is the activity of installing additional tools or devices on a telecommunications network for the purpose of obtaining information by unauthorized means. Basically, information owned by a person is a personal right that must be protected so that wiretapping must be prohibited.

Interception or tapping of data has a very relevant relationship in the spread of confidentiality of a person's identity because wiretapping in the applicable regulations means that the activity of installing additional tools or devices on a telecommunications network for the purpose of obtaining information by unauthorized means [15]. This means that if there is someone who taps on another person's communication device with the aim of obtaining information in an unauthorized manner, intentionally and without the knowledge of the person being tapped in various ways such as installing network equipment on telecommunications and can also use additional devices to obtain information on the telecommunications network. From this, tappers can easily get information and confidentiality of a person's identity. With the existence of tapping outside the authority, it is classified as a criminal offense.

4. Phishing in the Dissemination of Personal Data Confidentiality

Phishing is a form of online identity theft aimed at stealing sensitive information such as online banking passwords or a user's credit card information. This can be done with the help of an application or by sending a link to someone in order to steal that person's information. Phishing can be said to be a form of service that is deceptive by promising the validity and security of data transfer [16]. Phishing has a relationship with the spread of confidentiality of a person's identity which is a method used by hackers to steal passwords by tricking targets using fake login forms on fake sites that resemble the original site. Phishing stages or how it works is by the way a hacker makes us click on their fake site link, as well as with an attractive image, reference to an email and so on. After that, without realizing it, we have entered a username and password which can be said to be a form of identity confidentiality. In this way, the hacker easily takes over our account, then commits criminal acts to misuse it. This can be said to be a form of criminal offense.

5. Doxing in the Dissemination of Personal Data Confidentiality

Doxing comes from the word "dox" which means document which is an internet-based action to research and publicly disseminate personal information (including personal data) against an individual or organization. Doxing is more common in online forums or communities where users mostly use aliases to interact with each other. Unlike, for example, Facebook, users of the social media have generally used their real identities such as photos and names. In essence, publishing other people's personal information in

any form and under any circumstances and by utilizing any platform, falls under the definition of doxing [17].

Doxing in the spreading of identity privacy is very important to concentrate on because doxing is used to victimize others through the internet. The act of doxing reveals a person's identifying information online, such as real name, email address, workplace, telephone, financial, and other personal information. The information is then released to the public without the victim's permission. An example of doxing is a netizen exposing someone's identity. This is a violation of privacy because it shares someone else's personal data. Having someone disseminate someone else's identity without consent is very dangerous and will cause unwanted things in cyberspace.

6. Cyberhacking in the Dissemination of Personal Data Confidentiality

Cyberhacking can be attributed to the fact that the confidentiality of a person's identity needs to be considered. In the explanation of Article 30 paragraph 3 of the Electronic Information and Transaction Law: A security system is a system that limits access to a computer or prohibits access to a computer, namely based on a categorization or classification of users along with the specified level of authority. In paragraph 3, it is stated that someone who deliberately accesses computers and electronic systems by breaking through and/or breaking into the security system owned by the owner or user is a crime mode of a cracker. Hackers do this in order to gain benefits for themselves, namely either by obtaining financial benefits that make a lot of money by breaking passwords belonging to other people related to banking or credit cards, or non-financial to fulfill their own satisfaction by damaging computer networks and the like. With the knowledge of the password and other confidential identities of a person, the cracker can easily commit his crime.

Principles of Personal Data Protection

Confidentiality of identity which is one form of privacy confidentiality of identity is closely related to privacy, regarding the personal identity that a person has, then indirectly we also talk about the privacy of that person which should be protected and respected. in Malaysia compiled their privacy policy notice to comply with the Personal Data Protection Act and organizations differed in terms of the level of compliance and readability of their privacy notice [18]. Privacy is a term of the word that has been used by developed countries that have related to personal identity as a right that must be protected. The right to privacy in identity protection is a key element for individual freedom and dignity [19]. The 1945 Constitution of the Republic of Indonesia, hereinafter referred to as the 1945 Constitution, regulates the protection of personal identity. This becomes a basic rule in Article 28G paragraph (1) which stipulates that:

"Every person shall have the right to the protection of his or her person, family, honor, dignity, and property under his or her control, and shall have the right to security and protection from threats of fear to do or not to do something which is a human right".

In principle, a form of protection of personal identity is divided into two forms, identity protection in the form of security against physical identity, both visible identity and identity that is clearly visible with the formation of a regulated side in the use of identity by other people who are not entitled, misuse of identity for certain interests, and damage to the identity itself.

The internal government must ensure that the importance of personal identity protection for citizens is institutionalized in a comprehensive law that is equivalent to the principles of personal identity protection. The principles in question are [16].

1. Principle of Use of Restrictions

Regarding the use of other data/identity restrictions, this data should not be disclosed to the public or for purposes other than specific purposes without the permission of the person concerned in the exception of the consent of the data owner or the approval of the legal authority. In this principle, if it is related to the protection of personal data identity, it is privacy in which personal data should not be open in general. There must be a specific purpose and must obtain permission by the person concerned.

2. Principle of Limitation of Collection

In this principle, restrictions on data collection / privacy identity. The data obtained must use legal, fair and necessary means based on the knowledge and consent of the person concerned. In this principle of limiting collection, it explains that the limitation of personal data collection is limited to data collected for necessity only, which is in accordance with the law and the consent of the data owner.

3. Principle of Purpose Specification

To collect data/identity if needed must be a purpose specification, any further use of the data is only limited and in accordance with what is the purpose specification. This means that if you want to use data, there must be a specific reason and a purpose as long as it does not violate the applicable rules. In this principle, what is meant by the existence of purpose specifications in the protection of personal data is that the controller or organizer of the electronic system if it wants to collect data must have a clear and specific purpose related to data/identity collection as long as it is in accordance with the established rules.

4. Security Principles

A procedure with the support of regulations and technology. Every other data/identity must be protected in accordance with safeguards to protect it from loss, damage, use, alteration or dissemination whether intentional or not. The principle of security is very urgent in relation to one of the principles in personal data protection, because it has several procedures for regulations and technology in the event of intentional or unintentional damage, loss, alteration or leakage. In order to protect data to avoid the threat of cybercrime and misuse by irresponsible parties.

5. Principles of Openness

The increasingly strong demands and initiatives for information disclosure have also created new tensions with the protection of the right to privacy, especially personal data and information of citizens. This condition adds to the problem of protecting the right to privacy in Indonesia, which is caused by the lack of public awareness to protect their personal data. The provisions regarding the protection of a person's personal data, especially in electronic form, are only limitedly regulated in Article 26 of the Electronic Information and Transaction Law (ITE). The government,

as the entity that owns the data for data collection and policy making, is vulnerable to personal data leakage, especially under the pretext of public information disclosure. Therefore, the current challenge is how to balance the need to protect privacy and public information disclosure at the same time. In the case of Indonesia, the arrangement adopted is the second model. Whereas information disclosure is currently regulated in the Law on Public Information Disclosure, privacy protection is regulated in the Minister of Communication and Information Technology Regulation on Personal Data Protection in Electronic Systems.

6. Individual Participation Principle

The concept of data protection implies that individuals have the right to determine whether or not to share or exchange their personal data. Thus, individuals also have the right to determine the conditions under which the transfer of personal data will take place. Furthermore, privacy protection. The right to privacy has evolved so that it can be used to formulate the right to protect personal data. Every individual should have the right to obtain information about their personal data/identity and the right to delete or correct any unwanted errors. The principle of individual participation in personal data protection here is that individuals have the right to exercise the right to express opinions in the decision-making process concerning their own interests, either directly or indirectly. In this case, it is the individual who determines the extent to which they will make decisions regarding personal data.

7. Principle of Accountability

The government is obliged to manage population data for development purposes, including to inform public service planning, democracy building, legal protection, and cross-sector and cross-administration system linkages. Thus, the accuracy of population data can only be sustainable if there is a guarantee from the state to respect, protect, and fulfill everyone's right to data protection. Government accountability in personal data protection

a. Ensure universal registration coverage for individuals from birth to death, without discrimination.
b. Removing barriers and disparities in the availability and utilization of information and technology
c. Develop a comprehensive identity system that is unique, secure, and accurate
d. Create the basis for a system that is interoperable and responsive to the needs of diverse users
e. Utilize openly available standards and ensure neutralization of technology vendors and the technology itself
f. Protect personal privacy and user control in system design
g. Planning for financial and operational sustainability without compromising accessibility
h. Maintaining privacy in data, security, and user rights through a comprehensive legal and regulatory framework
i. Establishing comprehensive mandate and accountability
j. Enforce the legal framework and trust through independent oversight and grievance mechanisms [21].

The government, in terms of protecting one's personal data, is fully responsible for one's personal data. In the event of a leak, such as some time ago, government agencies and related state institutions actually have legal responsibilities, which at least have been regulated in the above laws and regulations. There are at least three things that need attention in relation to the various cases of personal data leaks that have occurred. First, regarding the alertness of the relevant agencies or institutions. The relevant agencies must basically be alert and take the necessary security measures as soon as possible to ensure that the allegedly leaked personal data is not further spread. Although it may seem quite technical, it is in principle a manifestation of the principle of integrity and confidentiality.

Concept of Legal Protection for Victims of Personal Data Dissemination

1. Preventive Protection Efforts Against Victims of Personal Data Dissemination

Preventive means prevention, one of the functions of prevention is to prevent or avoid a problem that will occur. With this preventive effort, it aims to direct the anticipation of problems from general to specific in the hope that these problems will not occur which have fatal consequences [22]. In the dissemination of identity confidentiality, preventive efforts are needed to prevent data leaks that harm the parties. One of the government's efforts to protect people's personal data and encourage awareness of the protection of personal data and or identity is by providing guidelines and regulations. Currently, in the PPD Law as a preventive effort, there is Article 17 Paragraph 2 which reads:

"Processing of Personal Data as referred to in paragraph (1) shall be carried out in accordance with the principles of protection of Personal Data, including

a. the collection of Personal Data is limited and specific, legally valid, appropriate, and transparent.
b. the processing of Personal Data is conducted in accordance with the purpose;
c. the processing of Personal Data is conducted by guaranteeing the rights of the Personal Data Owner
d. the processing of Personal Data is accurate, complete, non-misleading, up-to-date and accountable;
e. the processing of Personal Data is conducted by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction and/or loss of Personal Data;
f. the processing of Personal Data is conducted by informing the purpose and activities of processing, as well as the failure of protection of Personal Data;
g. Personal data is destroyed and/or erased after the retention period expires or based on the request of the Personal Data Owner unless otherwise provided by laws and regulations; and
h. Personal Data processing is carried out responsibly by fulfilling the implementation of the principles of Personal Data protection and can be clearly proven.

The processing of personal data aims to prevent the leakage of personal data; thus, the collection of personal data is limited and specific, lawful, proper and transparent. Data processing is carried out by guaranteeing the rights of the owner of personal data, carried out accurately and accountably, the processing of personal data is carried out by protecting the security of personal data from unauthorized access, unauthorized disclosure, misuse,

destruction and or loss of personal data. Then, the processing of personal data is carried out to inform the purpose and activities of the processing and the failure of personal data protection.

It can be said that this is listed in 28 letter c of the Ministerial Regulation on Personal Data Protection for Electronic Systems as a form of preventive effort, but in this case the author has assessed that the aspect of preventive protection provided by the Ministerial Regulation on Personal Data Protection for Electronic Systems is still premature, which is considering that currently there are still many data leaks and crimes that evolve in the cyber realm [23]. In addition, Article 28 letter c reads as follows:

Notify in writing to the Personal Data Owner if there is a failure to protect the confidentiality of Personal Data in the Electronic System it manages, namely with the following notification provisions

a. Must be accompanied by the reason or cause of the failure to protect the confidentiality of Personal Data;
b. Can be done electronically if the Personal Data Owner has given consent for it which is stated at the time of acquisition and collection. his/her Personal Data;
c. Must be confirmed to have been received by the Personal Data Owner if the failure results in potential harm to the person concerned; and
d. Written notification shall be sent to the Personal Data Owner no later than 14 (fourteen) days since the failure is known.

As a preventive measure, if there is a failure to protect the personal data it manages, it must be notified in writing to the data owner, must be accompanied by a reason that is clear enough for the cause of the failure, then the notification will be sent to the owner and / or identity user which is usually sent via email. After that, it must be confirmed again to the owner of the personal data if the failure contains potential losses for the person concerned, written notification will be sent to the owner of the personal data no later than 14 (fourteen) days from the time the failure is known. In addition, other effective preventive efforts in the Personal Data Protection Law provide protection and ensure the security of the data it processes, by carrying out the preparation and implementation of operational technical measures to protect personal data from interference with personal data processing that is contrary to the provisions of laws and regulations and the determination of the level of security of personal data by taking into account the nature and risks of personal data that must be protected in personal data processing.

2. Repressive Protection Efforts Against Victims of Personal Data Dissemination

Repressive action is action that is curbing, restraining, and oppressive. This repressive action aims to restore harmony that has been disturbed due to an offense by imposing sanctions in accordance with the offense committed. This repressive action aims to take preventive action against possible violations of social norms. As, there are regulations that provide repressive efforts regarding the form of protection of the confidentiality of personal data, but with the ratification of the Personal Data Protection Law there is a dispute resolution and procedural law, as in Article 56 which reads

1. Dispute settlement for the protection of Personal Data shall be conducted through arbitration, court, or other alternative dispute resolution institutions in accordance with the provisions of laws and regulations.
2. Procedural law applicable in dispute settlement and/or court process of Personal Data protection as referred to in paragraph (1) shall be implemented based on applicable procedural law in accordance with statutory provisions.
3. Valid evidence in this Law are:

a. evidence as referred to in procedural law; and
b. other evidence in the form of electronic information and/or electronic documents in accordance with laws and regulations. in accordance with statutory regulations.

4. In the event that it is necessary to protect Personal Data, the trial process shall be conducted in a closed manner.

It is explained that dispute resolution regarding the protection of Personal Data can be carried out through arbitration, court, or other alternative dispute resolution institutions in accordance with statutory provisions and in the event that it is necessary to protect Personal Data, equipped with valid evidence and other evidence in the form of electronic information and / or documents and the trial process is carried out in a closed manner.

For this reason, it is further emphasized that the Permen PDPSE provides a form of protection in the form of dispute resolution through complaints to the Minister of Communication, as explained in Article 29 regarding dispute resolution paragraph 3 that:

The complaint as referred to in paragraph (1) is made based on the following reasons

a. No written notification of failure to protect the confidentiality of Personal Data by the Electronic System Operator of the Data Owner to the Personal or other Electronic System Operator related to the Personal Data, either potentially or not potentially causing harm; or
b. There has been a loss to the Personal Data Owner or other Electronic System Operator related to the failure of the confidential protection of Personal Data, even though a written notification of the failure of the confidential protection of Personal Data has been made but the notification time is late.

Complaints can be made to the Minister for failure to protect the confidentiality of personal data based on the failure to notify in writing the failure to protect the confidentiality of personal data by the electronic system organizer to the data owner or other electronic system organizer related to the personal data, both potentially or not potentially causing harm or if there has been a loss for the owner of personal data or other electronic system organizer related to the failure to protect the confidentiality of personal data, even though a written notification of the failure to protect data confidentiality has been made but the notification time is late.

If there is a data leak due to the fault of the government, the first data controller will be held accountable if it concerns the government, the liability covers both the private and public sectors. After that, the supervisor authority must be competent independent to be able to prove the fault of the

public and private sectors, ideally it must be explained directly to the data owner if there is a data leak.

Conclusion

Legal protection against victims of personal data dissemination there are efforts that can be used to protect victims against the dissemination of identity confidentiality, namely by using preventive and repressive efforts. In preventive efforts, victims get protection from the Personal Data Protection Law regarding victim protection to prevent by using the rights and authorities that the owner of personal data can access his personal data if there is inaccuracy. In addition, there are repressive efforts in protecting victims against the dissemination of identity confidentiality that the owner has the right to receive written notification from the electronic system organizer. Preventively, the government must provide stricter supervision of the dissemination of personal data, such supervision can be in the form of supervision of the security of the system used for electronic system users in order to avoid data leakage. Other actions that must be provided by the government in protecting people's personal data and encouraging awareness of Personal Data Protection by providing guidelines and derivative regulations. Then provide education and raise awareness of Personal Data Protection properly through electronic media, print media, or online media, as well as national and international cooperation.

References

1. Syaifudin A. Perlindungan Hukum Terhadap Para Pihak Di Dalam Layanan Financial Technology Berbasis Peer to Peer (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta). Dinamika,2020:26(4):408-421.
2. Aswandi R, Putri R, Muhammad S. Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS). Legislatif,2020:3(2):167-190.
3. Kusnadi, Sekaring Ayumeida, Wijaya, Andy Usmina. Perlindungn Hukum Data Pribadi Sebagai Hak Privasi. Jurnal Ilmu Hukum, Universitas Wijaya Putra, 2021, 2(1).
4. Ramadha, Bagus Satriyo. Kemampuan Hukum Pidana terhadap Kejahatan Siber Terkait Perlindungan Data Pribadi di Indonesia. Tesis. Magister Hukum Universitas Islam Indonesia, 2021.
5. https://www.kompas.id/baca/ekonomi/2024/06/03/111-kasus-kebocoran-data-pribadi-ditangani-kemenkominfo-pada-2019-14-mei-2024?open_from=Tagar_Page
6. Paulus J Karu, *et al*. Legal responsibility towards personal data controller due to dissemination of personal data. Law Science, 2024, 6(1). Available from: https://doi.org/10.35335/jls.v6i1.4581
7. Michael Agustinus. tiba-tiba ditagih pajak Rp.32 Miliar. Kumparan (online), 2022.
8. Agustin Setyo. 500 juta data pribai tamu hotel marriots bocor. Desember, 2022, 1.
9. Ahmad Sodiki. Kejahatan Mayantara. Bandung: Refika Aditama, 2010, 103.
10. Raharjo, Agus. Cyber Crime dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: Citra Aditya Bakti, 2022, 102.
11. Dewi Septiani. Apa itu doxxing dan dampaknya pada privasi online, 2021. Available from: https://bpptik.kominfo.go.id/2021/06/21/8958/apa-itu-doxxingdan-dampaknya-pada-privasi-online/. Accessed 2024 Jun 25.
12. M. Redha Azhari. Aspek Pidana Mayantara (Cyberstalking). Badamai Law Journal, 2019, 4(1).
13. Chanelle Wilson, *et al*. What is Cyberstalking? A Review of Measurements. Journal of Interpersonal Violence, 2021, 37(11-12). Available from: https://doi.org/10.1177/0886260520985
14. Bambang Pratama. Data Pribadi, Data Privasi Dan Komersialisasinya. BINUS University, 2019.
15. Aggraini. Pemberlakuan Ketentuan Pidana Akibat Melakukan Tindak Pidana Intersepsi atau Penyadapan atas Informasi Elektronik atau dokumen elektronik. ejournal.unsrat.ac.id, 2021, 10(3).
16. Dian Rachmawati. Phising sebagai salah satu bentuk ancaman dalam dunia cyber. jurnalSAINTIKOM, 2014, 13(3).
17. Angga Prastiyo. Pemaknaan Objektifikasi Perempuan sebagai Hasil Doxing pada Akun Instagram Undip Cantik. Tesis. Magister Hukum, Fakultas Ilmu Sosial dan Politik Universitas Diponegoro, Semarang, 2018, 50.
18. Hui Na Chua, *et al*. Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. Telematics and Informatics,2017:34(4):157-170.
19. Saeful Bahri SH. Cyber Crime Dalam Sorotan Hukum Pidana. Jakarta: Bahasa Rakyat, 2020, 30.
20. Nurhamdiah Nadya. Perlindungan Hukum Terhadap Data Pribadi Pengguna Marketplace. Makassar, 2021. Available from: reporsitory.unhas.ac.id
21. Anonim. Tanggungjawab Negara Dalam Mengelola Data Penduduk. Puskapa, 2019.
22. Achmad Juntika Nurihsan. Bimbingan dan Konseling. PT Revika Utama, 2009, 21.
23. Maichle Delpiero, *et al*. Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. Padjajaran Law Review, 2021, 17.