Proceeding of 2nd Malikussaleh Internasional Conference on Law, Legal Studies and Social Science (MICoLLS) 2022

Protection Of Victims Of Personal Data The Through Digital Media

Muhammad Triadi, Sumiadi, Yusrizal

Protection Of Victims Of Personal Data The Through Digital Media

Muhammad Triadi[1*], Sumiadi[2], Yusrizal[3]

[1,2,3]Faculty of Law, Universitas Malikussaleh
[*]Correspondent Author, e-mail: muhammad.180510295@mhs.unimal.ac.id

Abstract

Theft of personal data is a crime that results in many victims experiencing material and psychological losses. However, legal protection for victims has not been clearly regulated in the current law regarding legal protection for victims of personal data theft. This study discusses two important issues, namely how legal protection for victims of personal data theft through digital media and how legal protection policies for victims of personal data theft through digital media. This study uses a normative juridical research method with a statutory and conceptual approach. The nature of this research is descriptive analytical. The collection of legal materials is carried out by literature study and data analysis techniques are carried out qualitatively. Based on the results of this study indicate that the normative legal protection for the criminal act of theft of personal data is not optimal. The policy of protection for victims of personal data theft in terms of the Personal Data Protection Bill (RUU PDP) already contains protection for victims of personal data theft regarding the weaknesses in existing regulations.

Keywords

Protection, Law, Victims, Theft, Personal Data

DOI : 10.29103/micolls.v2i.103

1. Introduction

Currently, information technology is growing rapidly not only in the field of the internet but also in the field of computers. With the development of information technology, it has a positive impact on human life, which makes it easier for humans today to access anything via electronics. Information technology provides several useful things, namely in the fields of business, telecommunications, education, and civilization in society, besides that, with the increase in information technology, it can also provide negative things, namely an effective means of unlawful acts, namely criminal acts. Many forms of crime are committed with information technology so that it is known by the term cybercrime. Various kinds of crimes that can be committed through today's technology such as hacking crimes, phishing crimes,

One of the negative impacts of technological advances is the crime of theft of personal data. Theft of personal data is a very dangerous crime, where this crime is the beginning of other crimes in the cyber world. Cyber crime is also a crime that is difficult to reveal because digital media is global or widespread. This makes it difficult for many victims to report and also get their rights back, the losses suffered by victims are not only in the form of money or wealth but also a violation of privacy.

The regulation of personal data in the legal system in Indonesia is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning

Information and Electronic Transactions (UU ITE) and Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection Personal Data in Electronic Systems (PDPSE). And Law 31 of 2014 concerning the Protection of Witnesses and Victims.

The existence of Law 31 of 2014 concerning the Protection of Witnesses and Victims has benefits for witnesses and victims, but Law 31 of 2014 concerning the Protection of Witnesses and Victims does not specifically explain or guarantee against victims of personal data theft, considering that the Protection Agency Witnesses and Victims (LPSK) are also only in big cities, making people in remote areas unable to report or claim compensation, due to the absence of LPSK in remote areas.

Article 26 paragraph 2 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 has indeed regulated compensation, but it only applies to perpetrators who have been found, but what if the perpetrators are not known to the victim. And in Law Number 31 of 2014 concerning the Protection of Witnesses and Victims, it has not regulated or explained specifically that victims of data theft have the right to compensation, therefore we need to know how far the victim of personal data theft has obtained the legal protection that should be obtained. The problems in this study are how is the legal protection for victims of personal data theft through digital media, how is the legal protection policy for victims of personal data theft through digital media seen from the PDP bill.

2. Research Methods

The type of research used by the author is normative research or commonly referred to as doctrinal research. This normative juridical research is a legal research method that is carried out by researching library data. This normative juridical research is also carried out by examining a norm and legislation, and the opinions of legal experts. This research uses a statute approach. And a conceptual approach (conceptual approach). The nature of this research is descriptive analytical, descriptive analytical is a type of research that describes the applicable laws and regulations and is associated with legal theories and legal implementation practices concerning the problems in this research. This study uses library data sources, namely data obtained by the author from various literary sources related to topics/problems raised by legislation, books, print media, journals and various opinions of legal experts, and are divided into 3 (three), namely primary legal materials consisting of laws and regulations relating to the issues discussed, secondary legal materials are materials that provide explanations of primary legal materials such as books, legal dictionaries, and legal journals, and tertiary legal materials are legal materials that provide explanations of primary legal materials and secondary legal materials such as scientific papers, internet, and others. The data analysis of this research was carried out qualitatively by collecting primary, secondary, and legal legal materials. and tertiary materials that are relevant to the problem being studied. After that, sorting the relevant legal materials to suit the problems being discussed by the author.

3. Research Results and Discussion

3.1. Legal Protection Against Victims of Personal Data Theft Through Digital Media

3.1.1 Legal Protection Against Victims of Personal Data Theft Through Digital Media According to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Protection of personal data is one of the personal rights in other words *(privacy rights)*, while personal rights contain the following meanings:

1. Personal rights are the rights to enjoy a private life and be free from all kinds of interference
2. Personal rights are the rights to be able to communicate with other people without being spied on.
3. Privacy rights are the rights to monitor access to information about Personal life.

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions is a law that regulates all crimes committed via digital/internet. Unfortunately, the regulation regarding the theft of personal data is only slightly regulated in Law Number 19 of 2016 (UU ITE), where the regulation is contained in Article 26 Paragraph 1 which contains: "Unless otherwise stipulated by the Legislation, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned."

As for Article 26 Paragraph 2 of Law Number 19 of 2016 (UU ITE) "Everyone whose rights are violated as referred to in Paragraph 1 can file a lawsuit for the losses incurred under this Law." Article 46 Paragraph 2 of Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) also regulates perpetrators who violate data theft, which states "Everyone who fulfills the elements as referred to in Article 30 Paragraph 2 shall be punished with imprisonment of at most 7 (seven) years and/or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiah)." Looking at the provisions of Law Number 19 of 2016 (UU ITE) that explicitly prohibits accessing other people's personal data without the knowledge of the data owner.

Based on the previous description that Law no. 19 of 2016 (UU ITE) has not been able to fulfill the protection of the rights for victims of personal data theft, which results in significant losses for victims which should be prevented and overcome by formulating norms that can punish perpetrators of criminal acts up to the level of punishment (prison) in accordance with his mistake and set the sanctions firmly as required by the norms of criminal law, and because of this case of personal data theft the victim received a lot of material losses, so the need for the formulation of sanctions must also reach the stage where the victim gets compensation as he experienced with the stages as easy as possible.

3.1.2. Legal Protection Against Victims of Personal Data Theft Through Digital Media According to the Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems (PDPSE) is a regulation that can be said to be quite clear in protecting personal data in digital media. Here are some articles that can be said to be important aspects in protecting personal data, namely:

a) Article 2 paragraph 2 Regarding Personal Data Protection, which contains 10 Points, namely:
   1. Respect for Personal Data as privacy
   2. Personal Data is confidential in accordance with the Approval and/or based on the provisions of laws and regulations
   3. Based on Approval
   4. Relevance to the objectives of acquisition, collection, processing, analysis, storage, display, announcement, delivery and dissemination
   5. Eligibility of the Electronic System used
   6. Good faith to immediately notify the Personal Data Owner in writing of any failure to protect Personal Data
   7. Availability of internal rules for the management of Personal Data protection
   8. Responsibility for Personal Data that is in the control of the User
   9. Ease of access and correction of Personal Data by the Personal Data Owner
   10. Integrity, accuracy and validity and up-to-date of Personal Data.
b) Article 26 Regarding the Rights of the Personal Data Owner, that the data owner has the right to:
   1. For the confidentiality of his Personal Data
   2. File a complaint in the context of resolving personal data disputes over the failure to protect the confidentiality of personal data by the Electronic System Operator to the Minister
   3. Gain access or opportunity to change or update their personal data without disturbing the Personal Data management system, unless otherwise stipulated by the provisions of laws and regulations
   4. Gain access or opportunity to obtain historical Personal Data that has been submitted to the Electronic System Operator as long as it is still in accordance with the provisions of the laws and regulations
   5. Request the destruction of his/her Certain Individual Data in the Electronic System managed by the Electronic System Operator, unless otherwise stipulated by the provisions of the laws and regulations.
c) Article 28 Regarding the Obligations of the Electronic System Operator, that the operator is obliged to:
   1. Performing Electronic System certification which it manages in accordance with the provisions of laws and regulations;
   2. Maintain the truth, validity, confidentiality, accuracy and relevance and suitability

for the purpose of obtaining, collecting, processing, analyzing, storing, displaying, publishing, transmitting, disseminating, and destroying Personal Data

3. Notify in writing to the Personal Data Owner if there is a failure to protect the confidentiality of the Personal Data in the Electronic System it manages, with the following notification conditions:
   a) Must be accompanied by reasons or causes for failure of confidential protection of Personal Data;
   b) It can be done electronically if the Personal Data Owner has given Consent for that which was stated at the time of the acquisition and collection of his Personal Data;
   c) It must be ensured that it has been received by the Personal Data Owner if the failure contains a potential loss for the person concerned
   d) Written notification is sent to the Personal Data Owner no later than 14 (fourteen) days after the failure is known
4. Have internal rules related to the protection of Personal Data in accordance with the provisions of laws and regulations
5. Provide an audit track record of all Electronic System implementation activities it manages
6. Provide options to the Personal Data Owner regarding the Personal Data that he manages can/or cannot be used and/or displayed by/to third parties upon approval as long as it is still related to the purpose of obtaining and collecting Personal Data
7. Provide access or opportunity for Personal Data Owners to change or update their Personal Data without disturbing the Personal Data management system, unless otherwise stipulated by the provisions of laws and regulations
8. Destroying Personal Data in accordance with the provisions in this Ministerial Regulation or other laws and regulations that specifically regulate the respective Supervisory and Regulatory Agencies for this purpose
9. Provide a contact person who is easily contacted by the Personal Data Owner regarding the management of his Personal Data.

d) Article 29 Regarding Dispute Settlement, namely:
   1. Every Personal Data Owner and Electronic System Operator may file a complaint to the Minister for the failure to protect the confidentiality of Personal Data.
   2. The complaint as referred to in paragraph (1) is intended as an effort to resolve the dispute by deliberation or through other alternative settlement efforts.
   3. The complaint as referred to in paragraph (1) is made based on the following reasons:
      a) There is no written notification of the failure of the confidential protection of Personal Data by the Electronic System Operator to the Personal Data Owner or other Electronic System Operators related to the Personal Data, whether or not it has the potential to cause harm.
      b) There has been a loss for the Personal Data Owner or other Electronic System Operators related to the failure of the confidential protection of the Personal Data, even though a written notification has been made of the failure to protect the confidentiality of the Personal Data, but the notification time is too late.

4. The Minister can coordinate with the leadership of the Sector Supervisory and Regulatory Agencies to follow up on the complaints as referred to in paragraph (1).

e) Article 36 Regarding Administrative Sanctions Given To Actors Who Violate the Regulations in Article 36, namely:
   1. Everyone who obtains, collects, processes, analyzes, stores, displays, announces, sends, or disseminates personal data without rights or not in accordance with the provisions in this Ministerial Regulation or other laws and regulations is subject to administrative sanctions in accordance with the provisions of the legislation. in the form of:
      a) Verbal warning
      b) Written warning
      c) Temporary suspension of activities
      d) Announcements on online sites (websites online).

The Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems has already regulated in detail regarding the protection of personal data, starting from the definition, limitations, responsibilities of the organizer, the protection process and sanctions. Looking at Regulation No. 20 of 2016 (PDP SE) unfortunately it still has weaknesses in which there is no legal protection for victims to get compensation carried out by the organizers who fail to protect the victim's personal data, as well as the absence of criminal sanctions given to the behavior of theft of personal data. only administrative sanctions.

3.1.3. Legal Protection Against Victims of Personal Data Theft Through Digital Media According to Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Protection of Witnesses and Victims

Victims of theft of personal data who basically have a need to fulfill the material losses they have experienced, in Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Protection of Witnesses and Victims, it is stated that there is protection for victims and witnesses of criminal acts, namely in forms of Compensation, Restitution and Assistance.

Material losses for victims of this criminal act of theft of personal data, Restitution is the right method. As in Article 1 Paragraph 11 which states that "Restitution is compensation given to the victim or her family by the perpetrator or a third party." To obtain protection for victims of criminal acts through the LPSK, must go through the stage of submitting an application submitted by the LPSK, taking into account the requirements stated in Article 21 of Government Regulation no. 7 of 2018 concerning the Provision of Compensation, Restitution and Assistance to Witnesses and Victims.

Basically, the application for restitution to the LPSK can be submitted before the case is indicted, and after the case has received a court decision. Handled by LPSK, to apply for Restitution from the applicant to the related parties. For cases that have not been indicted, the application is submitted to the public prosecutor so that the application can be included in his claim at once, and for cases that have obtained a court decision, it is submitted to the

court so that a determination can be given.

In Article 7A paragraph 1 of Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning the Protection of Witnesses and Victims, it is stated that victims of criminal acts are entitled to Restitution, in the form of:

a. Compensation for loss of property or income;
b. Compensation for losses caused by suffering directly related as a result of a crime
c. Reimbursement of medical and/or psychological treatment costs.

In the Regulation of the Chairperson of LPSK Number 6 of 2010 concerning Procedures for Providing Witness and Victim Protection, Article 16 Paragraph 1 states that, the Decision of the Plenary Meeting of LPSK members as referred to in Article 15 Paragraph 4 contains:

a. Classification of cases or cases: severe, moderate, or mild faced by the applicant
b. The form of protection provided to the applicant
c. Providing assistance to fulfill procedural rights.

Thus, the continuation to the next stage only depends on the results of the Plenary Meeting of LPSK Members, then further if it is declared accepted it can be delegated to the protection sector to enter the stage of providing protection as referred to in the application. If the application is rejected, LPSK will continue to deliver the notification to the applicant in writing. However, the legal protection referred to according to Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning the Protection of Witnesses and Victims is anyone who applies for protection that can be protected in terms of the losses actually experienced by the victim. victim.

For compensation, compensation according to Article 1 Paragraph 10 of Law No 31 of 2014 concerning the Protection of Witnesses and Victims, "Compensation is compensation provided by the state because the perpetrator is unable to provide full compensation which is his responsibility to the victim or his family". Compensation is only given to victims of serious human rights violations and terrorism, there is no compensation for victims of data theft.

Legal protection for victims of crime is contained in Law Number 31 of 2014 concerning the Protection of Witnesses and Victims, this law explains the rights of victims and the protection provided to victims, but in Law Number 31 of 2014 concerning Protection Witnesses and Victims do not include all the victims of the crime who received them.

It can be understood from what has been explained above that there are several regulations governing the protection of personal data theft but there is no law that specifically discusses the protection of personal data. The existence of clear legal certainty against the theft of personal data will have an impact on the welfare of privacy for the victims in particular and society in general because all citizens have the potential for their personal data to be stolen and misused, therefore the need for the government to immediately provide clear and specific legal certainty regarding data by prioritizing and following international legal standards.

3.2. Legal Protection Against Victims of Personal Data Theft Through Digital Media According to International Legal Instruments

Seeing that the protection of victims of data theft in Indonesia still does not have a separate or special law regarding the protection of personal data, this makes it difficult for the public to get protection. Due to data theft cases being a big problem and the perpetrators are also difficult to detect, so that international law also discusses and regulates the structure of international organizations, one of which is regulated, namely the protection of personal data. There are several international legal instruments that regulate the protection of personal data, namely:

3.2.1. *Organization for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 1980*

The OECD (The Organization for Economic and Cooperation Development) participates by issuing guidelines/guidelines on basic principles in the protection of personal data that can be used as a reference in making a rule. As for the basic principles these are:

a. The principle of collection limitation is to collect personal data legally and fairly, and to be followed by the consent of the data subject and with his knowledge.
b. Principle of Quality (Data Quality Principle), the collection of personal data must be in accordance with the purpose of the user and the personal data must be complete, accurate and if there is a change, it must be immediately updated.
c. The Purpose Specification Principle, the purpose for which personal data is collected must be determined no later than the time the personal data is collected
d. Use Limitation Principle, the consent of the data owner is required to disclose, provide or use the data for purposes other than the original purpose for which the data was collected.
e. Security Safeguard Principle, personal data must be protected from the risk of data loss, data destruction, unauthorized use, data disclosure or unauthorized access.
f. The principle of openness (Openness Principle) The main purpose of data use, identity and data controller must be established, prior to which a policy on openness related to the development or management of personal data must be established.
g. Principle of Individual Participation (Individual Participation Principle) The purpose of this principle is to control data or confirm data related to it by providing access to be deleted, changed or corrected.
h. The Accountability Principle It is the responsibility of the data controller to comply with the measures that have an impact on the principles mentioned above.

The OECD has regulated the basic principles of personal data protection and then also stipulates related guidelines regarding the protection of personal data, but the OECD in terms of legal protection for victims has not at all regulated the legal rules regarding compensation that must be given to victims of personal data theft so as to create a Legal Instrument Internationally contained in the OECD is not so optimal. The OECD should also be able to focus on victims of personal data theft who have been harmed so that victims can

get their rights that have been taken away by perpetrators of personal data theft.

3.2.2. *European Union Data Protection Directive 1995*

Regarding the general rules on the principles of member countries in Article 6 of the Data Protection Directive 1995 stipulates that personal data must:

i. Processed fairly and legally
j. Collected clearly and legally in accordance with the intended purpose, and will not be processed further in a way that is not in accordance with the purpose
k. Relevant and not redundant for the purpose of collection and processing
l. Data must be accurate, any inaccurate or incomplete data must be deleted or corrected
m. Stored in a form that allows for identification of the data subject. And countries should establish appropriate safeguards for personal data to be stored for long periods.
n. Processed for personal data security by ensuring protection against processing, and not violating the law.

Legal remedies regarding responsibilities and sanctions, which state obligations are regulated in Article 23 paragraphs 1 and 2 of the Data Protection Directive 1995, namely:

1. Member States should provide that any person who has suffered harm is entitled to compensation for unlawful processing.
2. The controller can be released from this obligation if it is proven that he is not responsible for the damage that occurs

Furthermore, regarding the supervisory authority and individual protection in the management of personal data, it is regulated in Article 28 of the Data Protection Directive 1995 where the supervisory authorities are:

1. Each Member State shall determine that one or more public authorities shall be responsible for assisting the application within the territory of the provisions held by the Member States.
2. Each member state should provide that supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individual rights and freedoms in relation to the processing of personal data.
3. Each authority will specifically be given investigative powers such as the authority to access data, effective intervention powers such as giving opinions before processing operations are carried out, and finally the power to be involved in legal proceedings.
4. Every supervisory authority must listen to the claims made by each person
5. Each supervisory authority must make periodic reports on its activities, and these reports will be made public
6. Each supervisory authority has the authority, regardless of the national law applicable to processing which is concerned to carry out in the territory of its own member country
7. Each member and staff of the authority after their term of office has ended, they are subject to confidentiality obligations with respect to the confidential information they have accessed.

Looking at some of the existing regulations in the European Union Data Protection Directive, we can conclude that these instructions from the European Union Data Protection Directive are considered the strongest regulations regarding personal data protection.

Although this instruction only applies to countries in Europe, of course this instruction can be a reference or guideline for other countries, including Indonesia itself, in making regulations regarding the protection of personal data through digital media so that it is much safer in protecting the public from cases of theft. personal data.

3.2.3. United Nations General Assembly Resolution on Privacy Rights in the Digital Age or the so-called (The Rights of Privacy in Digital Age)

This resolution is also one of the responses to the movement of the states of Germany and Brazil, so that this resolution is also supported by thirty-five countries including Indonesia, as for the things that contain the UN General Assembly Resolution on Privacy Rights in the Digital Era, namely:

a. This resolution increases the capacity of governments or companies to monitor data collection that violates privacy rights
b. Affirming the human right to privacy so as not to be subjected to arbitrary interference
c. Emphasize actions that violate the right to privacy, are acts that violate the rights of freedom and are contrary to the principles of a democratic society
d. This resolution pays attention to the negative impact on interception of communications and the collection of personal data, especially on a mass scale
e. Affirming that the rights owned by someone offline must also be protected online, including the right to privacy
f. Notify all countries to:
    1. Respect and protect the right to privacy, including digital communication
    2. Take action to end violations of privacy rights in order to create conditions to prevent infringement
    3. Reviewing procedures, practices, and legislation regarding the control of communications, and data collection, with a view to upholding the right to privacy and exercising them under human rights and international law
    4. Establishing independent supervision that is able to guarantee for the supervision of communications, interception and collection of personal data
    5. Provide commensurate compensation to individuals whose rights to privacy are violated, in accordance with international human rights obligations.

Several international legal instruments that have been described previously prove that it is very important to protect the personal data of citizens, seeing that the majority of the Indonesian population is currently using a lot of technology, it is appropriate for the Indonesian state to protect its citizens so that their privacy is safe. We can see that currently Indonesia does not have a special law that regulates the protection of personal data, Indonesia itself only has special regulations regarding the protection of personal data in digital media which is in the form of Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Digital Media. Electronic System.

3.3 Legal Protection Policy Against Victims of Personal Data Theft Through Digital Media Judging from the Personal Data Protection Bill

The Personal Data Protection Bill defines personal data as “any data about a person,

either identified or individually identifiable or combined with other information, either directly or indirectly through electronic and/or non-electronic systems." As well as in the Personal Data Protection Bill, it also explains which data includes general and specific data. The general personal data are full name, gender, nationality, religion, and finally personal data combined to identify a person, while the specific personal data are health information data, biometric data, genetic data, sexual orientation data, views politics, crime records, child data, personal financial data.

The Personal Data Protection Bill regulates the parties involved in processing personal data, namely personal data owners, personal data controllers, and personal data processors. The owner of personal data as the data subject has rights, including the right to request information, the right to complete, access, update, and/or correct errors and/or inaccuracies in his personal data, the right to end processing, delete, and/or destroy personal data. his rights (right to erasure), the right to withdraw consent to processing, the right to object to the profiling action, the right to delay or limit the processing, the right to claim and receive compensation.

Personal data controller is a party whose purpose is to process personal data. Thus, the personal data controller must be responsible for all processing of personal data. While the personal data processor is the party that performs the processing of personal data on behalf of the personal data controller. although personal data controllers and personal data processors are different but still have the same basic obligations, here are 7 basic scopes of the same basic obligations between personal data controllers and personal data processors, namely, maintaining the confidentiality of personal data, protecting and ensuring the security of personal data, including safeguarding personal data. accessed illegally, supervise all personal data processing activities, record personal data processing activities, ensure accuracy, completeness.

To ensure the effectiveness of law enforcement on the protection of personal data, this Draft Law also stipulates administrative sanctions, criminal sanctions, compensation and criminal sanctions aimed at misuse of personal data. Administrative sanctions can be in the form of written warnings, temporary cessation of processing activities, deletion or destruction of personal data, compensation, and administrative fines. In the PDP Bill against the organizers (Corporations) who cannot protect the personal data of their users, they can be subject to fines in accordance with Article 66 paragraphs 2 to 4 of this Bill, namely: (3) The fine imposed to the Corporation a maximum of 3 (three) times the maximum penalty imposed. (4) In addition to being sentenced to a fine as referred to in paragraph (2), the Corporation may be subject to additional penalties in the form of:

a) confiscation of profits and/or assets obtained or proceeds from criminal acts;
b) freezing of all or part of the Corporation's business;
c) permanent prohibition from performing certain actions;
d) closing all or part of the place of business and/or activities of the Corporation;
e) carry out obligations that have been neglected; and
f) payment of compensation and the absence of criminal sanctions given to the organizer of the personal data that violates.

The bill on the protection of personal data also stipulates compensation for victims by submitting a dispute resolution through a civil lawsuit. Regarding the claim for compensation for the victims, it will be easier if it is directly included in the indictment in

the criminal case concerned, because if the victims have to file a claim for compensation in a civil case it will be very difficult for the victims. Victims who have been harmed and have their rights taken away by perpetrators should be given an easy way by the government to obtain material and immaterial damages caused by criminals, especially the theft of personal data.

The provisions that violate Article 51 Paragraph 1 of the Personal Data Protection Bill are "Everyone is prohibited from obtaining or collecting Personal Data that is not theirs with the intention of unlawfully benefiting themselves or others or may result in losses to the Personal Data Owner". Sanctions will be imposed in Article 61 Paragraph 1 of the Bill on the Protection of Personal Data, namely "Anyone who knowingly obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person against the law or may result in the loss of the Personal Data Owner. as referred to in Article 51 paragraph 1 shall be sentenced to a maximum imprisonment of 5 (five) years or a maximum fine of Rp. 50,000,000,000.00 (fifty billion rupiah)". Article 65 of the PDP Bill states that in addition to being sentenced to five (5) years in prison and a maximum fine of Rp. 50,000,000,000.00 (fifty billion rupiah) the defendant may also be sentenced to additional punishment in the form of confiscation of profits or assets obtained and proceeds from criminal acts and payment of compensation.

Looking at some of the regulations regulated in the Personal Data Protection Bill, of course, there are shortcomings, such as in the processing of personal data, where the Personal Data Protection Bill does not clearly state the duties and responsibilities of Kominfo in its role as an authority. protection of personal data. As well as the absence of a special independent commission to oversee the management of personal data, Ardi Khwatir as the impartial research coordinator said "if the management of personal data is completely left to the government, say Kominfo, then the vulnerability the occurrence of misuse of personal data is getting bigger". Therefore, it is fitting for Indonesia to have a special agency that oversees the management of personal data. While inGeneral Data Protection Regulation (GDPR)his personal data protection authority hasindependent and have a clear scope of responsibilities to ensure the agency can enforce the law and sanction stakeholders such as governments and companies.

Furthermore, the weakness in the Personal Data Protection Bill (RUU PDP), namely, the absence of criminal sanctions against the organizers of personal data, if they commit a violation, only administrative sanctions are imposed, this is deemed insufficient in providing a deterrent effect on the organizers who violate the victim's personal data.

The Personal Data Protection Bill (RUU PDP) does not yet cover international standards, with this, it is hoped that the Indonesian state should immediately revise the PDP Bill to comply with international standards in protecting the personal data of all its citizens, and ratify it as soon as possible so that the public can be protected from harm. the crime of theft of personal data and get maximum legal certainty. The presence of the PDP Bill is expected to provide protection for electronic systems from cybersecurity attacks, and the protection of people's personal data on digital platforms. The government continues to make efforts to protect people's personal data, in order to avoid misuse or data leakage by irresponsible parties. In tackling the problem of private data leakage, the government through the Ministry of Communication and Informatics intervened to strengthen regulations and invite the whole community to continue to improve literacy, especially

regarding the protection of personal data. This includes participating in various digital literacy trainings provided, in which the Ministry of Communication and Informatics targets 12.5 million people to be digitally literate per year.

Seeing that the government in tackling victims of personal data theft only provides socialization and digital literacy training (appeals) it is deemed insufficient in protecting victims, the government should guarantee protection for victims who have suffered losses by providing or updating the PSK Law so that compensation can be added. victims of personal data theft due to the protection of victims of personal data theft is one of the state's responsibilities to protect every citizen, it can be seen in Article 28 G paragraph 1 of the 1945 Constitution which states that "everyone has the right to personal protection, family , honor, dignity, and property under his control,and has the right to a sense of security and protection from the threat of fear to do or not do something which is a human right".

4. Conclusion

Regulations regarding the protection of personal data in Indonesian law are regulated in Article 26 Paragraph 1 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. However, this law does not regulate the legal protection of data owners by related parties such as personal data organizers. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems but this Ministerial Regulation does not regulate the form of compensation for victims that must be borne by third parties. Law Number 14 of 2016 concerning the Protection of Witnesses and Victims only regulates the provision of restitution and compensation for victims of gross human rights violations. Arrangements regarding the protection of personal data in international legal instruments are regulated in the Organization for Economic Co-operation and Development (OECCD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 19880,

The policy of the Personal Data Protection Bill has been said to be optimal in protecting victims from personal data theft, the PDP Bill has regulated the definition of personal data, types, ownership rights, processing, exceptions, controllers and processors, delivery, authorized institutions that regulate personal data, and dispute resolution. In addition, the PDP Bill will also regulate international cooperation to sanctions imposed for misuse of personal data. The PDP Bill has focused more on discussing and specifically regulating legal protection for victims who are harmed and also on protecting the privacy of personal data. The PDP Bill also has a weakness in that it does not clearly state the duties and responsibilities of Kominfo in its role as the authority for protecting personal data.

5. Reference

Abdul Salam Siku. (2016). Protection of the Human Rights of Witnesses and Victims in the Criminal Court Process, *Indonesia Prime*, Indonesia.

Amira Paripurna, et al. (2021). *Victimology and the Criminal Justice System*. Depublish: Yogyakarta.

Joshefin Mareta. "Witness and Victim Protection Policy Analysis."

Balitbangham.Go.Id Vol 10, No. 1, (2016), pp.1–29.https://www.balitbangham.go.id/po-content/po-upload/jikh_volume_10_No_1_tahun_2016.

Kominfo. "Ministry of Communication and Informatics." Kominfo.Go.Id. Last modified 2020. AccessedJanuary28,2022.https://www.kominfo.go.id/content/detail/28343/bersama-protect-private-data-on-digital-platform/0/article.

M. Arief Mansur and Elistaris Gultom. (2005). *Cyber Law Legal Aspects of Information Technology*. Refika Aditama: Bandung.

Marli Candra and Imron Rosyadi.(2020). *Victim Precipitation in the Crime of Theft (An Approach to Victimology), Duta Media Publishing, Indonesia.*

Muhadar. Protection of Witnesses and Victims in the Criminal Justice System, Putra Media Nusantara: Surabaya, 2010.

Republic of Indonesia "Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Protection of Witnesses and Victims,".Republic of Indonesia, "Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions".

Republic of Indonesia. "Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 5 of 2015 concerning Protection of Personal Data in Electronic Systems,".