IJOBSOR, 11 (2) (2023) pp. 373-383
Published by: TRIGIN Publisher
International Journal of Politics and Sociology Research
Journal homepage: www.ijobsor.pelnus.ac.id

Juridical analysis of personal data protection in the case of BPJS personal data leakage reviewed from a positive legal perspective

Everdina Cathrine Tesaldnika Pattipeilohy
Faculty of Law, Universitas Pelita Harapan Surabaya, Indonesia

ARTICLE INFO

Article history:

Received Jun 16, 2023
Revised Aug 23, 2023
Accepted Sep 28, 2023

Keywords:

BPJS
Information
Law
Personal Data
Security

ABSTRACT

The progress of the Internet today is very rapid, if you need and search for information can be done with the help of modern technology. The basic principle of personal data protection is the principle of restriction of data use which confirms that personal data must not be disclosed, provided or used for purposes other than those prescribed, except with the consent of the data owner or by legal authorities. In addition, there are also Data Protection Principles that emphasize the importance of protecting personal data by maintaining reasonable security against risks such as loss, access, destruction, use, modification, or unauthorized disclosure of data. The case of leakage of BPJS personal data is the responsibility of the BPJS institution (government) as an Electronic System Operator supported by Article 47 of the Personal Data Protection Law. BPJS as a public institution that is an electronic system operator must ensure that in managing personal data must be in accordance with the principles of personal data protection in accordance with the new PDP Law and ensure that even though it cooperates with third parties, it is monitored as well and as much as possible so as not to become a data leak again.

This is an open access article under the CC BY-NC license.

Corresponding Author:

Everdina Cathrine Tesaldnika Pattipeilohy,
Department of Law,
Pelita Harapan University Surabaya,
Jl. Cipta Menanggal 1 blok 16CC2 Menanggal, Gayungan, Surabaya, Jawa Timur 60234, Indonesia.
Email: everdinactp@gmail.com

1. INTRODUCTION

The progress of cyberspace today is very rapid, if you need and search for information can be done with the help of modern technology (Budhijanto, 2023). Access to interconnected networks or the internet can also be accessed anywhere and anytime. This digital age is very helpful in our daily lives. However, according to Brisila Tumalun, some experts criticize technological development because it has brought many changes and affected human progress. The development of information technology has changed the way we think about boundaries, time, values, forms, logic of thinking, work patterns, and limits of social behavior from manual to computerized / digital (Tumalun, 2018).

Technological advances supported by the internet and electronic systems have encouraged information technology personnel, individuals, institutions, and governments to create applications, sites or technology systems where when used people or individuals must enter some personal data into the application, website or technology system as a database (Doa, Laras Nada dan Aufa, 2022). These technological developments encourage Indonesia to make laws, namely Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 concerning Electronic Information and Transactions (hereinafter referred to as

the ITE Law) in Article 2 of the Law it is explained that the ITE Law applies to everyone, both within the jurisdiction of Indonesia and outside the sovereign territory of Indonesia, who commit legal acts based on this law and have legal consequences within the sovereign territory of Indonesia and/or outside the interests of Indonesia (Saleh, 2021). This ITE Law refers to the transmission of personal information via the internet, where some articles affirm that electronic information must be obtained with the consent of the data owner and personal data obtained through the internet will use an electronic system (Rinjani, 2021). Electronic System according to ITE Law Article 1 points 5 and 6 is an electronic system referring to a collection of electronic devices and procedures that aim to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate electronic information (Raineven, 2023). The implementation of electronic systems includes using electronic systems by individuals, business entities, government organizations, and/or communities that offer, manage, and/or operate electronic systems, individually or collectively, for the benefit of themselves and/or others (Haganta, 2020). In Article 15 of the ITE Law, an electronic system implemented by an electronic system operator must be processed reliably and safely, and the electronic system operator is ready to bear responsibility for the proper and correct operation of the electronic system (Sitorus, 2023).

Personal data is regulated in the ITE Law but does not directly define a clear law on personal data, but viewed from the perspective of official interpretation of *privacy rights* in article 26 paragraph 1, personal data includes life affairs including (history) of a person's communications and data about a person personal life affairs including (history) of a person and data about a person in article 26 of the ITE Law also provides legal protection personal data where the use of information concerning a person's personal data through electronic media must obtain consent from the person concerned unless otherwise regulated by laws and regulations, if this is violated then the person has the right to file a lawsuit for losses suffered in accordance with the provisions of this Law (Supriadi, 2019).

In Indonesia, there is the latest regulation that protects personal data, namely Law Number 27 of 2022 concerning Personal Data Protection (abbreviated as PDP Law No 27 of 2022) which was just passed in 2022. PDP Law No. 27 of 2022 provides legal protection related to personal data protection. Article 1 paragraph 1 explains that Personal Data refers to information about a person who can be identified alone or by using other information, whether through electronic or non-electronic systems, directly or indirectly (Arsyah, 2023).

Responsibility stems from Article 1365 *Burgelijk Wetboek* (hereinafter referred to as "BW"). It is stated that unlawful acts that cause harm to another person require that person to compensate for losses caused by errors in determining the original loss manual to computerized/digital, in article 1367 BW which states (Fikri, Muhammad and Rusdiana, 2023):

A person is not only liable for damages caused by his own actions, but also for damages caused by the actions of those for whom he is responsible or caused by goods under his control (Khikam, 2023)."

What can be done when there is a case of personal data leak, if you look at the ITE Law in article 38 of the ITE Law is regulated as follows: a) Any Person may file a lawsuit against the party that organizes the Electronic System and/or uses Information Technology that causes losses; b) The public can file a lawsuit vicariously against parties who organize Electronic Systems and/or use Information Technology that results in harming the community, in accordance with the provisions of the Laws and Regulations"(Putra, Tomi Wicaksono and Abdurrachman, Hamidah and Hamzani, 2023).

For example, one of the electronic systems used by public services is BPJS Kesehatan. The provisions of BPJS are in line with Law No. 24 of 2011 concerning the Social Security Organizing Agency of the Republic of Indonesia (hereinafter referred to as BPJS Law No. 24 of 2011), the definition of BPJS according to Article 1 paragraph (1) of BPJS Law No. 24 of 2011 is a legal entity formed to run social security programs (Saleh, 2021).

BPJS consists of two parts, namely BPJS Employment which guarantees costs due to work accidents for workers and BPJS Health which guarantees costs if the family is sick (Koswara, 2022). To obtain BPJS, we generally have to register personal data by coming directly to the nearest BPJS office, registered by the company if the person registering is a worker, and can also register through the JKN mobile application which can be downloaded on the *appstore* or *google*

play. In accordance with article 10 letter e of BPJS Law No. 24 of 2011 in carrying out its functions, BPJS is tasked with collecting and managing information on Social Security program participants (Mala, 2023).

It is unfortunate that in 2021, BPJS allegedly experienced a data leak of allegedly as many as 279 residents' data (Kautsar, 2022). The data includes data such as ID cards, emails / *emails*, mobile phone numbers, Identity Numbers, and addresses and even data on state officials, TNI, Polri. The police and Kominfo intervened to investigate the data leak incident, whether there were allegations that there were people in BPJS who leaked in order to obtain finances or indeed negligence from BPJS in securing the personal data (Arrasuli, Beni Kharisma and Fahmi, 2023). The results of the personal data leak investigation were sold on the online forum Raid Forums by an account named Kotz, personal data sold including BPJS card numbers, NIK, mobile phone numbers, email addresses and salaries, this data included data about deceased citizens (Bukit, Abigail Natalia and Ayunda, 2022). BPJS data breaches have disturbed the public because they are vulnerable to cybercrime related to data storage of government and private institutions.

This research is of a Normative Juridical nature, using deductive methods and conducted through the analysis or examination of relevant laws and documents related to the research topic, while also considering literary sources. Its objective is to assess the compliance of the Information and Electronic Transactions (ITE) Law regulations pertaining to Personal Data as positive law, as well as to identify the responsible parties in the event of a personal data breach in similar cases.

2. RESULTS AND DISCUSSIONS

The basic principle of personal data protection is the principle of restriction of data use which confirms that personal data must not be disclosed, provided or used for purposes other than those prescribed, except with the consent of the data owner or by legal authorities. In addition, there are also Data Protection Principles that emphasize the importance of protecting personal data by maintaining reasonable security against risks such as loss, access, destruction, use, modification, or unauthorized disclosure of data (Fikri, Muhammad and Alhakim, 2022).

According to Article 1 paragraph 6a of the ITE Law, electronic system operators are individuals, government institutions, companies, and communities that produce, manage, and/or run electronic systems for personal interests or the interests of others, so government institutions or public institutions are allowed to organize electronic systems by taking into account laws and regulations and BPJS is one of the public institutions (Redi, Ahmad and Ramadhan, 2023).

As operators of electronic systems, public institutions have the responsibility of ensuring that the electronic systems they manage meet reliable, secure, and controlled requirements and comply with data protection principles (Firdaus, 2022). This aims to prevent leakage or legitimate use of data, as well as ensure that the system can function stably and reliably by users. Some of the conditions that must be met by a reliable, safe, and controlled electronic system include: a) Data security: The system must be equipped with adequate security protections, such as firewalls, passwords, and data encryption technologies. b) Defense systems: Systems must be designed to be able to survive unexpected situations, such as hacker attacks or natural disasters. c) System availability: The system must be accessed quickly and not interrupted by technical glitches or outside attacks. d) Privacy protection: The system must ensure that the user's personal data is protected from other parties. e) Monitoring and control: The system should be equipped with sufficient monitoring and control mechanisms to prevent theft or security intrusions (Greenler, Robert. Rainbows, Halos, 2020).

By meeting these requirements, public institutions can ensure that the electronic systems they manage can run properly, and provide safe and reliable services to users. Personal data relating to individuals that can be used to identify or connect an individual is directly or indirectly called personal data. Personal data may include various types of information, such as name, address, telephone number, email address, date of birth, identification number, and financial or health information (Doa, Laras Nada dan Aufa, 2022).

This information plays a very important role in everyday life from filling out registration forms, accessing online shopping sites, to other things, protecting personal information is very important to minimize the risk of misuse or data harvesting by unauthorized parties, cybercriminals can use personal information for criminal activities such as identity theft or financial fraud. In

addition, irresponsible parties may use personal information to send spam or phishing messages to email addresses or phone numbers. Personal information is indeed the most important factor for BPJS participants because BPJS needs participants' personal information to manage and manage the BPJS program (Lubis, 2022).

BPJS has a privacy policy that explains how the data and information provided by Users when registering and using the Application are protected and used. BPJS may amend this Privacy Policy in accordance with changes in law, collection and practice of using Personal Data, application features, or technological advances (Mirna, 2023). The privacy policy of BPJS is divided into two, namely for BPJS Kesehatan and BPJS Ketenagakerjaan (Firdaus, 2022).

BPJS Kesehatan collects user data to facilitate application usage. User data collected includes healthy Indonesia card numbers, KTP / NIK numbers, dates of birth, names of biological mothers, mobile phone numbers of participants and registered family members, electronic mail addresses (e-mail) of participants and registered family members, as well as correspondence addresses of participants and registered family members (Rianarizkiwati, 2022). In addition, there is a collection of information data provided voluntarily when users register as participants or Mobile users, update the data of registered participants and family members, conduct medical history screening, or file complaints through the features provided. Information data recorded when users use the application includes real and approximate location data such as IP address, Wi-Fi, cocation, time of each user activity, type of device used, operating system and version, software, file name and version, language selection, unique device identifier, serial number, device movement information, and/or cellular network information. In addition, logs are also recorded on servers that receive data such as the device's IP address, date and time of access, application features or pages viewed, application work processes, and other system activities.

BPJS Kesehatan guarantees that there will be no sale, transfer, distribution, or loan of users' personal data to third parties without permission from the user. However, BPJS Kesehatan may disclose user data to partners or other third parties who assist BPJS Kesehatan in providing services on the application. BPJS Kesehatan can also provide relevant information to business partners in accordance with user consent to use business partner services and can disclose user data in an effort to comply with legal obligations and/or legitimate requests from law enforcement officials.

As for BPJS Ketenagakerjaan, BPJS Ketenagakerjaan has the right to use user data and information to improve quality and service in the Jamsostek *Mobile* application. However, BPJS Ketenagakerjaan is not responsible for the self-exchange of data among Jamsostek *Mobile* users. BPJS Ketenagakerjaan will only disclose the data and/or information it has if required by laws and regulations, requested by an authorized institution based on applicable legal provisions, and/or obtain an official order from the Court. During the process of providing services. BPJS Ketenagakerjaan is committed to providing the best protection in storing users' personal data.

In the third-party platform service policy, BPJS Ketenagakerjaan can cooperate with biometric service provider partners recognized by the Ministry of Communication and Information Technology as Electronic Certification Providers. The third party will verify the identity in the implementation of the data update, and the user's personal data will be checked for suitability. The personal information collected will be stored and used by biometric service provider partners for the purpose of providing BPJS Employment Services, diagnosing, fixing problems, and improving Services, as well as evaluating and developing new Services. In addition, users' personal data may also be used to fulfill legal and law enforcement obligations, process payments, support business functions, marketing, and other uses. The third party will issue an electronic certificate as proof that the user's personal data has been verified and in accordance with the data recorded in the system of the agency entitled to issue the identity[1].

Responsibility for BPJS Data Breach

Legally, responsibility is a consequence or consequence of freedom of action alone related to ethics or morality (Notoatmodjo, 2010). In the vocabulary of law, obligation is a necessity for an individual to fulfill the duties that have been required of him (Hamzah, 2009). Accountability must have a basis, namely a cause for the creation of a legal right for a person to sue others at the same

time and also give rise to the legal obligation of others to liability (Febrian, 2010). Liability means the obligation to provide answers that are an explanation of all things that happened and the responsibility to provide compensation for losses that may be incurred (Soegeng Istanto, 1994).

The concept of responsibility was conveyed by Hans Kelsen, the originator of pure law theory, Hans said that obligation and responsibility are closely related, but not the same. Responsibility arises because there are legal rules that regulate and give obligations to legal subjects. Legal subjects who have obligations must carry them out according to the dictates of the rule of law. If the obligation is not implemented, then there will be sanctions. This sanction is a forced act of the rule of law to ensure that obligations are properly carried out by legal subjects. According to Hans, the legal subjects subject to such sanctions are considered "responsible" or legally liable for violations (Hans, 2008).

Liability under Indonesian law refers to the obligation of a person or legal entity to be held accountable for his or her actions or deeds, this liability can be criminal or civil depending on the type of offense committed. In the context of criminal law, a person or legal entity can be held accountable if proven to have committed a criminal act, criminal liability can be in the form of criminal sanctions such as imprisonment, fines or other punishments.

On the other hand, civil law liability refers to the responsibility of a person or legal entity (such as a company or organization) to bear the legal consequences of an act or omission that causes loss or damage to another party within the scope of civil law, in civil law obligations can be divided into two types, namely firstly obligations arising from agreements or contracts (contractual obligations) that occur when a person or party makes a promise or agreement with other parties to do or not do a certain thing. This obligation arises because of an agreement between the parties involved, and is usually stipulated in a contract or written agreement, the second is a legally arising obligation (legal obligation) that occurs due to a legal provision that requires a person or party to do or not do a certain thing, this obligation does not require an agreement or agreement between the parties involved, But arising from the existence of governing legal provisions, examples of legal obligations are the obligation to pay taxes, the obligation to avoid actions that harm others, and so on. Meanwhile, civil law obligations in connection with unlawful acts depend on the existence of legal relations, rights, and responsibilities derived from legal regulations (M.A Moegni Djojodirdjo, 1982). According to R. Subekti, civil legal liability arises because of an Engagement or Contract arising from an action that can cause harm to others because it is done incorrectly in civil law, which is referred to as an Unlawful Act and contains elements of error resulting in civil liability, the step of occurrence of civil legal liability due to an unlawful act where the obligation of liability begins with an engagement. According to Article 1233 of the Civil Code, the source of engagement consists of agreement and law, the meaning of engagement is a legal relationship in matters of property, where one party is entitled to an achievement while the other party is obliged to carry out the achievement. Meanwhile, Article 1313 of the Civil Code defines an agreement as an act in which one or more persons bind themselves to one or more other persons. However, this definition was criticized by R. Subekti because it only includes unilateral agreements, while agreements are generally reciprocal such as sale and purchase agreements, leases, exchanges, and so on. Engagements arising from the Act consist of engagements derived from the Law and engagements derived from the Act relating to human actions. Engagements derived from laws related to human actions can be divided into legal engagements and unlawful engagements, i.e. unlawful engagements (Subekti, 2008). If an agreement is not fulfilled as it should, it is referred to as default, default refers to the debtor's non-compliance with the agreement, in which case the affected party can take some civil action[2].

In the event of a breach of civil obligations, the injured party may file a claim for compensation against the responsible party. Such claims may include financial damages, restoration of circumstances as before, or other actions deemed necessary to address losses arising from such violations. In addition, in some cases, individuals or legal entities may be held liable, such as violations of government regulations or applicable regulations. This administrative responsibility can be in the form of reprimands, warnings, or administrative sanctions such as

revocation of business licenses. In general, legal accountability in Indonesia is based on the principles of justice, equality and protection of human rights.

Electronic System according to ITE Law Article 1 points 5 and 6 is an electronic system referring to a collection of electronic devices and procedures that aim to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate electronic information. The implementation of electronic systems includes the use of electronic systems by individuals, business entities, government organizations, and/or communities that offer, manage, and/or operate electronic systems, either individually or collectively, for the benefit of themselves and/or others. In Article 15 of the ITE Law, an electronic system implemented by an electronic system operator must be processed reliably and safely, and the electronic system operator is ready to bear responsibility for the proper and correct operation of the electronic system. In the case of BPJS personal data leak, BPJS is the organizer of the electrobic system.

In 2021, BPJS Indonesia as an electronic organizer, faced a massive data leak that revealed the personal information of millions of BPJS participants. The breach resulted in the loss of sensitive information such as name, address, date of birth, ID number and other personal information. BPJS Kesehatan stated that the data leak occurred due to hacking or hacking on the BPJS information system. In addition, BPJS also said that they had coordinated with the police to handle the case and had made improvements to their information security system. The result of the investigation of this personal data leak is that the personal data was sold on the online forum Raid Forums by an account named Kotz, the data sold includes BPJS card numbers, NIK, mobile phone numbers, email addresses and salaries, this data includes data about deceased citizens. Due to the results of the investigation that this personal data leak was hacked by a third party and sold on the online forum Raid Forums, BPJS (Social Security Organizing Agency) should have a legal responsibility to protect the personal data of its members.

In the case of BPJS data leakage, BPJS violates several obligations stipulated in laws and regulations in Indonesia, including:

1. Article 26 of the ITE Law regulates the obligations of electronic system operators, which include: a) Guarantee the confidentiality and security of information received, stored, or processed in electronic systems. b) Provide complete, accurate, clear, and non-misleading information about identity, services, products, and prices. c) Provide proof of transaction to electronic system users. d) Guarantee the availability and completeness of information and documents related to electronic transactions. e) Provide adequate facilities and infrastructure for users of electronic systems. f) Respond to complaints or complaints of electronic system users in a timely manner and in accordance with applicable regulations.

If a violation is committed against one of the above obligations by the BPJS organizer, it can be considered a violation of the ITE Law.

2. PP No. 71 of 2019 concerning the Implementation of Electronic Information Security Article 8 Paragraphs (1) and (2) stipulates that information owners must secure the information they have, including identifying information security risks and making applicable information security policies within the organization. BPJS data leakage cases show that the information security policies implemented by BPJS are inadequate so that users' personal information is exposed and can be accessed unlawfully.
3. Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning Personal Data Protection in Electronic Systems is as follows: a) Obligation to implement adequate technical and organizational measures to protect personal data, such as data encryption, data backup, access rights settings, and information security policies. b) Obligation to maintain the confidentiality of personal data, including preventing unauthorized access to or disclosure of personal data. c) Obligation to provide clear and complete information to the owner of personal data, including about the use of personal data, the rights of the owner of personal data, and how to access and correct personal data. d) Obligation to respond quickly and effectively to personal data owner's complaints and requests.

In the case of BPJS 2021 data leakage, third parties cooperating with BPJS are suspected of violating these obligations, causing data leakage that endangers the privacy and security of BPJS participants' data.

1. Obligation to maintain personal data protection in accordance with the principles of personal data protection, third parties who cooperate with BPJS have the obligation to maintain the confidentiality of BPJS participant data they handle in accordance with the ITE Law and PDP Law. The obligation to maintain the confidentiality of personal data of BPJS Kesehatan participants, in accordance with Article 26 Paragraph (1) and (2) of the ITE Law as well as Article 28 Paragraphs (1) and (2), and article 30. and Perkeminfo 20 Year 2016 Article 4,5,7,8.
2. Obligation to protect personal data, third parties also have an obligation to protect the personal data of BPJS participants they handle. This is in accordance with the provisions of Law Number 11 of 2020 concerning Job Creation Article 51 paragraph (1) which states that "Everyone who processes personal data must ensure that the personal data processed is guaranteed confidentiality and not misused."

In 2021, there was a large case of leakage of personal data of BPJS Kesehatan participants and raised concerns about data privacy and security. As the institution responsible for the data, BPJS Kesehatan is subject to several sanctions in the prevailing laws and regulations in Indonesia, including: a) Violations of the BPJS Kesehatan ITE Law may be subject to administrative sanctions in the form of reprimands, access blocks, or revocation of electronic system operating permits, if proven to violate the provisions regarding the management of participants' personal data. b) Violations of Law No. 36 of 2009 concerning Health BPJS Kesehatan may be subject to administrative sanctions in the form of warnings, written reprimands, temporary suspension of activities, or revocation of licenses to operate health insurance programs, if proven to violate the provisions regarding the management of participants' health data. c) Violation of Minister of Communication and Information Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems: BPJS Kesehatan may be subject to administrative sanctions in the form of written reprimands, activity restrictions, or revocation of licenses to operate electronic systems, if proven to violate the provisions regarding the protection of participants' personal data.

Indonesia has a new law for personal data protection, PDP Law No. 27 of 2022 requires the data controller, in this case BPJS, to process personal data responsibly and show responsibility in fulfilling the principles of personal data protection is an important task. One of the important principles in the processing of personal data is to protect the security of personal data from unauthorized access, disclosure, misuse, destruction and loss of personal data. In other words, the loss of personal data of BPJS participants is not in accordance with the principles of personal data protection. If the personal data controller is not responsible for carrying out the protection of personal data, administrative sanctions may be imposed, such administrative sanctions in the form of: a) Written reprimand, b) Permission freeze, c) Destruction of personal data, d) Administrative penalty of 2% of annual income.

Administrative sanctions may be imposed if BPJS does not report a personal data breach. In addition to administrative sanctions, participants who become victims can file civil lawsuits for BPJS participant data breaches. This is regulated in Article 12 paragraph 1 of PDP Law No. 27 of 2022, which states that the owner of personal data has the right to file a complaint for violations of personal data processing in accordance with Article 1365 BW.

Sanctions obtained by third parties who cooperate with BPJS in cases of BPJS data leakage, here are some sanctions that may be applied: a) Administrative Sanctions, third parties who violate the provisions in laws and regulations may be subject to administrative sanctions. These sanctions can be in the form of reprimands, warnings, or administrative fines. b) Criminal Sanctions, if proven to have committed a criminal act, third parties who cooperate with BPJS may be subject to criminal sanctions in accordance with applicable laws and regulations. For example, Article 32 of the ITE Law, which regulates computer crimes. c) Civil Sanctions, third parties who cooperate with BPJS can also be subject to civil sanctions if proven to have violated the agreement that has been agreed with BPJS. This civil sanction can be in the form of compensation for losses suffered by BPJS. d) Suspension of Cooperation, BPJS can also freeze cooperation with third parties who are proven to have violated data security. This can have an impact on the reputation and business of those third parties.

BPJS Responsibilities

BPJS (Social Security Organizing Agency) data leakage can cause significant losses to participants and these organizations. In the event of a personal data breach, the aggrieved owner of the personal data may file a claim for compensation against the party responsible for the breach. The amount of compensation that can be received by the owner of personal data will be determined based on the losses suffered by the owner of personal data as a result of the personal data breach that occurs. However, to determine the amount of compensation that can be received by the owner of personal data, it must go through a court process and must first be proven that there is a violation of the personal data owned by the owner of the personal data.

If there is a data leak, an investigation must be carried out first, because this personal data leakage is caused by a third party who cooperates with BPJS, the third party must be tried in accordance with applicable laws, but BPJS as a public institution that collects the data, BPJS must be responsible for providing compensation to participants affected by the data leak because in doing Data protection is incompatible with the principles of personal data protection.

Based on the author's explanation above, what are the compensations provided by BPJS to BPJS participants whose personal data is leaked, Article 26 paragraph (1) in the ITE Law states that any individual who suffers losses due to violations of the provisions as referred to in Article 30 paragraph (2) can claim civil compensation. In this case, Article 30 paragraph (2) in the ITE Law states that every individual is prohibited from taking actions that directly or indirectly harm others. In Law Number 19 of 2016 Article 26 paragraph (1) it is stipulated that every individual who suffers losses due to violations of the Electronic System Operator's obligation to protect Personal Data has the right to seek compensation, and based on PDP Law Number 27 of 2022, the owner of personal data has the right to sue and ask for compensation for violations of his personal information in accordance with applicable laws and regulations. What about the form of compensation will be explained as follows.

As a social insurance institution, BPJS Kesehatan is responsible for protecting participants' personal data. However, in the event of a data leak, BPJS Kesehatan must provide compensation to the affected participants. Here are some types of compensation that can be provided by BPJS Kesehatan along with examples in the case of BPJS data leakage: a) Material compensation is a form of compensation given in the form of money or goods. An example of material compensation is BPJS Kesehatan providing funds to reimburse participants for the costs incurred to replace stolen identities or the cost of repairing financial losses incurred due to data leakage. b) Immaterial damages are forms of compensation provided in non-material forms, such as apologies, restoration of good names, or compensation for emotional stress caused by data leaks. An example of immaterial compensation is BPJS Kesehatan apologizing publicly to participants and providing free psychological counseling for participants who are disturbed by data leaks. c) Preventive compensation is a form of compensation that aims to prevent the recurrence of similar events in the future. An example of preventive compensation is BPJS Kesehatan improving the security of participants' personal data and providing training and education on data security to BPJS Kesehatan employees and participants. d) Compensatory compensation is a form of compensation that aims to compensate for losses suffered by participants due to data leakage. An example of compensatory compensation is BPJS Kesehatan providing compensation for financial losses incurred due to participants' identities being stolen and misused by irresponsible parties. e) Compensation in the future, for example the leaked personal data may not be used by hackers or hackers *at that time it may be years after the data is just used, for example* hackers *use our* personal data to make online *loans and are not paid then bills come to the home of one of the BPJS participants whose personal data was leaked* even though the participant never made a loan *Another* example is that the leaked personal data is used to register credit cards even though we do not register directly but the bill comes to the BPJS participant whose data is leaked, this kind of thing whose losses can arise in the future, participants still have to have evidence in court for this future loss. f) Compensation related to psychological pressure is a form of compensation which is generally in the form of giving money to victims from unlawful acts that cause victims to experience psychological distress, for example, it could be because the personal data of BPJS participants is leaked making one of the BPJS participants feel emotional suffering because there are certain data that they do not want people to know for example on the Indonesian KTP still includes marital

status and there are several If the divorce case occurred while still alive, the status on the ID card is a living divorce, this may cause embarrassment, stress, mental stress because the status will be known to many people if the data is disseminated. Another example is as follows: it could be that from the leakage of personal data, there are certain parties who know the address of one of the BPJS participants, then that party can *stalk* and supervise the house of one of the BPJS participants which can cause the BPJS participant to have excessive fear.

But for civil sanctions, compensation must be in accordance with the elements of article 1365 BW and the causality relationship that as long as this personal data leakage incident does not cause losses, the owner of personal data cannot ask for compensation, all must be proven through clear evidence in court later, in other words, the determination of compensation in BPJS data leakage cases usually involves a legal process and strict examination to determine the level of responsibility from the parties involved. Therefore, it is necessary to conduct a comprehensive investigation and audit to determine the exact amount of compensation in this case.

3. CONCLUSION

The conclusions that can be drawn from writing this thesis are as follows:

1. Those responsible for the breach of personal data of BPJS participants are Electronic System Operators, namely BPJS, a government institution that handles social security for the Indonesian people with legal foundations, namely: Article 1 points 5 and 6, Article 3, especially the word "good faith", Article 9, Article 15 paragraphs 1 and 2, Article 26 of the ITE Law as the basic basis for implementing the implementation of electronic systems. The breach of BPJS personal data is the responsibility of the BPJS institution (government) as an Electronic System Operator supported by Article 47 of the PDP Law
2. It does not necessarily appear if the BPJS electronic system breaks, considering the elements of article 1365 are. As follows: a) Unlawful acts: acts that are contrary to the law or applicable legal norms. In the case of BPJS personal data leakage, if a certain person or party obtains access and misuses the personal data unlawfully, it can be considered that the elements of unlawful acts are fulfilled. b) Loss: the existence of material or immaterial losses experienced by the victim. Losses can occur if the personal data is used for interests that harm the data owner, in this case it is a BPJS participant or the public who registers themselves to get BPJS, such as identity misuse or fraud. c) Mistakes: Perpetrators of unlawful acts must be held accountable for their actions. To be held responsible, the perpetrator must have fault either in the form of negligence (culpa) or malicious intent (dolus). d) Indemnity: For the party who suffered losses due to unlawful acts to claim compensation from the responsible party.

There must be causality on element number 2 of loss and element number 4 of compensation then compensation appears can be filed a lawsuit. For administrative sanctions to arise immediately because the BPJS electronic system operator is negligent so that the data is breached, laws and regulations require that every electronic system operator must carry it out safely, reliably, and be ready to bear responsibility for the operation of the electronic system properly and correctly.

BPJS as a public institution that is an electronic system operator must ensure that managing personal data must be in accordance with the principles of personal data protection in accordance with the new PDP Law and ensure that even though it cooperates with third parties, it is monitored as well and as much as possible so as not to become a data leak again. If the data owner suffers losses due to data hacking, it is recommended to contact the relevant institution or company to find out the procedures for claiming compensation that must be undertaken.

In the pursuit of understanding the complexities surrounding data breaches within the context of BPJS, we must acknowledge certain research limitations that guide our future explorations. The current discourse largely gravitates toward the legal and regulatory facets of data breaches. However, it is evident that the comprehensive grasp of this issue necessitates a broader perspective. To effectively prevent data breaches, we must delve into the intricate technical and cybersecurity aspects, which are instrumental in fortifying our defense mechanisms. While the existing body of research draws heavily from legal provisions and theoretical analyses, a more practical dimension remains underrepresented. Future investigations should be grounded in

empirical data, incorporating case studies and real-world examples of BPJS data breaches. This shift would offer invaluable insights into the pragmatic implications of data breaches.

Prospective research endeavors should embark on an exploration of the specific cybersecurity measures that organizations like BPJS can adopt to safeguard personal data more effectively. This might encompass a meticulous study of technical solutions, encryption practices, and security audits. Conducting in-depth case studies of actual data breach incidents involving BPJS or similar entities can provide a treasure trove of insights. These case studies can unravel the root causes, repercussions, and best practices for mitigation.

The cultivation of awareness and education regarding data security practices is paramount. Governments and Private endeavors should aim to discern effective strategies for raising awareness and educating not only BPJS participants but also the general public. In the Future Governments and Privates can contribute significantly by formulating policy recommendations. These recommendations should aim to enhance data protection laws, regulations, and advocate for increased government involvement in data security efforts. In the face of global data security challenges, international collaboration and agreements on data protection warrant exploration. Such collaborations can fortify our collective ability to tackle data security issues effectively.

REFERENCES

Arrasuli, Beni Kharisma and Fahmi, K. (2023). Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi. *UNES Journal of Swara Justisia*, *7*(2), 369-392aa.

Arsyah, M. F. (2023). *Perspektif Hukum Hak Asasi Manusia terhadap Jaminan Perlindungan Data Pribadi di Indonesia*. Universitas Islam Indonesia.

Budhijanto, D. (2023). *Hukum Perlindungan Data Pribadi di Indonesia Cyberlaw & Cybersecurity*. Refika Aditama.

Bukit, Abigail Natalia and Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20.

Doa, Laras Nada dan Aufa, M. F. (2022). *Pengertian Kausalitas dan Teori Kausalitas*. Universitas Sebelas Maret Surakarta.

Febrian, T. T. dan S. (2010). *Perlindungan Hukum bagi Pasien*. Prestasi Pustaka.

Fikri, Muhammad and Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *YUSTISI*, *9*(1).

Fikri, Muhammad and Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia. *Ganesha Law Review*, *5*(1), 39–57.

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23–31.

Greenler, Robert. Rainbows, Halos, and G. (2020). Society of Photo-Optical Instrumentation Engineers (SPIE). *Pres. Washington-USA*.

Haganta, R. (2020). Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic. *Lex Scientia Law Review*, *4*(2).

Hamzah, A. (2009). *Kamus Hukum*. Yayasan Obor.

Hans, K. (2008). *Pure Theory of Law, Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif* (Keenam). Penerbit Nusa Media.

Kautsar, T. R. (2022). *Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi dan Regulasi Perlindungan Data Pribadi*. UIN Ar-Raniry.

Khikam, D. (2023). *Kajian Hukum Perlindungan Data Pribadi Dalam Peraturan Perundang-undangan di Indonesia*. Universitas Islam Sultan Agung Semarang.

Koswara, W. (2022). Implementasi Aturan Perlindungan Data Pribadi Oleh Penyelenggara Sistem Elektronik Dikaitkan Dengan Teori Keadilan dan Kepastian Hukum. *Jurnal Paradigma Hukum Pembangunan2*, *7*(2), 86–103.

Lubis, P. R. F. (2022). *Perlindungan Hak Asasi Manusia Atas Data Pribadi DI Era Digital dalam Prinsip Negara Hukum Berdasarkan Pancasila*.

M.A Moegni Djojodirdjo. (1982). *Perbuatan Melawan Hukum* (Kedua). Pradnya Paramita.

Mala, D. (2023). *Pertanggung Jawaban Hukum atas Kebocoran Data Pribadi Pengguna BPJS Kesehatan*. Universitas Medan Area.

Mirna, M. (2023). Analisis Pengaturan Keamanan Data Pribadi Di Indonesia. *JURNAL ILMIAH LIVING LAW*, *15*(1), 16–30.

Notoatmodjo, S. (2010). *Ilmu perilaku kesehatan* (Vol. 200, pp. 26–35). rineka cipta.

Putra, Tomi Wicaksono and Abdurrachman, Hamidah and Hamzani, A. I. (2023). *Pertanggungjawaban Pidana terhadap Kejahatan Hacking*. Penerbit NEM.

Raineven, S. V. C. (2023). *Perlindungan Hukum Bagi Konsumen yang Mengalami Kebocoran Data*

Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Indonesia. Fakultas Hukum.

Redi, Ahmad and Ramadhan, D. A. (2023). *Komisi Independen Perlindungan Data Pribadi: Quasi Peradilan dan Upaya Terciptanya Right To Be Forgotten di Indonesia*.

Rianarizkiwati, N. (2022). Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia. *Jurnal Hukum Sasana*, *8*(2), 324–341.

Rinjani, H. S. (2021). *Menjaga datamu, data kita bersama*. Fakultas Sains and Teknologi Universitas Sari Mulia.

Saleh, A. R. (2021). Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana. *HUKMY: Jurnal Hukum*, *1*(1), 91–108.

Sitorus, S. Y. H. (2023). *Perlindungan Hukum Data Pribadi Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi Ditinjau dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Universitas Kristen Indonesia.

Soegeng Istanto, F. (1994). *Hukum Internasional*. UAJ.

Subekti, R. (2008). *Hukum Perjanjian*. PT Intermassa.

Supriadi, D. (2019). Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya. *Hukum Online*.

Tumalun, B. (2018). Upaya Penanggulangan Kejahatan Komputer Dalam Sistem Elektronik Menurut Pasal 30 Undang-Undang Nomor 11 Tahun 2008. *Lex Et Societatis*, *6*(2), 2018.