JARES, Vol.9 No.2 September 2024
p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

REPRESSIVE PROTECTION FOR JOURNALISTS FOR LEAKAGE OF PERSONAL DATA BY TELECOMMUNICATIONS SERVICE PROVIDERS

Diterima:
06 Mei 2024
Revisi:
21 Mei 2024
Terbit:
01 September 2024

[1*]Untari Hesti Ningsih, [2]Eko Wahyudi
[1-2)] Universitas Pembangunan Nasional "Veteran" Jawa Timur

Abstract— Leakage of personal data is the transmission of data via electronic devices including name, place, date of birth, passcode and electronic address which can be accidentally accessed by unauthorized persons. This study aims to understand the legal protection that can be given to journalists for acts against the law by telecommunications service providers for personal data leakage. This study uses normative research methods by analyzing data in a descriptive-qualitative manner. The results of the research show that actions taken by telecommunication service providers are classified as unlawful acts under Article 1365 of the Civil Code. Journalist Akbar Wijaya as the victim suffered material and immaterial losses and disrupted his journalistic activities because he experienced personal data leaks. Thus, based on Article 1365 of the Civil Code, he is obliged to obtain compensation and Telkomsel has not been able to carry out its obligations as a business actor to have good faith in providing its product services. Telecommunications service providers who have a role as personal data controllers commit acts that are not in accordance with the precautionary principle in accordance with Article 3 of Law no. 27 of 2022 concerning personal data protection.

Keywords— *Animation-Based Video Media, Listening*

Penulis Korespondensi:

Untari Hesti Ningsih,
Program Studi Hukum, Fakultas Hukum
Universitas Pembangunan Nasional "Veteran" Jawa Timur
e-mail: untarihesti@gmail.com

JARES, Vol.9 No.2 September 2024
p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

I. INTRODUCTION

Telecommunications service provider is a business actor providing network services in the telecommunications sector. Telecommunications service providers have the task of managing and providing services within the economic scope, the products provided by telecommunications service providers, namely communication and information services in the form of telephone numbers connected to the internet or what can be called provider networks. Examples of using this provider network feature can be done via SMS, Telegram, Line, Twitter, Instagram, and Whatsapp. One of the professions that use this provider network feature is a journalist. As technology advances, journalists also participate in using the features provided by telecommunication service providers, namely cell phone numbers that are connected to the internet or provider networks. The use of this provider's network is still not in accordance with the terms and conditions stated in the product belonging to the telecommunications service. Such as personal data security standards that are still lacking, service error notifications that are still slow, and the absence of compensation and compensation as a result of telecommunication service errors.

Journalists who have ethics in their journalistic activities contained in the Journalistic Code of Ethics, are responsible for respecting the privacy rights of their information sources. If there is a leak of personal data, it will certainly cause losses to the journalist profession, both materially and immaterially. First, material losses in terms of integrity and credibility as a journalist profession. Second, the loss as a user in privacy data that should get a good security system. Third, immaterial losses in the form of fear of spreading personal data because personal data has high economic value. Where this data can be traded and allows for fraud, exploitation of balances through telephone numbers. Losses experienced by journalists if they experience personal data leakage must receive legal protection from the government and society. Laws and regulations relating to the importance of personal data are explained in Article 28 G paragraph (1) of the 1945 Constitution. Indonesia has legal regulations regarding personal data which are contained in Law no. 27 of 2022 concerning personal data protection. Personal data that can be leaked includes names, addresses, telephone numbers, identity numbers, and other information that could endanger the security and privacy of journalists. The emergence of cases of journalists who have not been able to obtain personal data security and responsibility for losses experienced as a journalist, such as in the case of a journalist named Akbar Wijaya.

On September 24, 2022 there was an incident that caused Akbar Wijaya's whatsapp account as a journalist from a mass media platform called Narasi.tv to experience a hack, namely the whatsapp account suddenly exited, every time you want to enter Akbar Wijaya's

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

account you don't receive a one-time-use passcode OTP (One Time Password) which is usually sent by telecommunications service providers via short messages. During the hack, Akbar Wijaya did not receive telephone verification, that Akbar Wijaya also could not access the telephone number which is usually used for daily use. The telephone number can be accessed by users who register by including their KTP and family card numbers. In this case, Akbar Wijaya's number was used by someone else on another device, as a result the data related to that number was discovered without the permission of Akbar Wijaya as the owner of personal data and the original user of Telkomsel's services as a telecommunication service provider. The applications used as communication media, namely whatsapp and telegram, also changed hands because they are directly connected to Akbar Wijaya's telephone number. However, the phone number is already in use by someone else on another device. When changing hands, it requires prior verification, such as sending an OTP (One Time Password) code to a device that uses a telephone number connected to WhatsApp and Telegram communication media.

This causes personal data leakage and shows that user security has not been implemented optimally. This incident proves that Telkomsel, as a telecommunications service provider, has failed to safeguard its users' cellular numbers and personal data. Akbar Wijaya said that the hack was a threat to the work of journalists. As a result of this case Akbar Wijaya asked for an explanation from Telkomsel but there was no answer and he transferred the matter to Whatsapp. The case of Journalist Akbar Wijaya shows that telecommunications service providers, namely Telkomsel as a business actor and controller of the telecommunications system, have not been able to provide guarantees for the condition of the products being traded and there is no good will from Telkomsel to correct errors in the security feature of the telephone number service belonging to Journalist Akbar Wijaya. This action shows that Akbar Wijaya as a consumer and responsibility for losses experienced as a journalist, such as in the case of a journalist named Akbar Wijaya.

On September 24, 2022 there was an incident that caused Akbar Wijaya's whatsapp account as a journalist from a mass media platform called Narasi.tv to experience a hack, namely the whatsapp account suddenly exited, every time you want to enter Akbar Wijaya's account you don't receive a one-time-use passcode OTP (One Time Password) which is usually sent by telecommunications service providers via short messages. During the hack, Akbar Wijaya did not receive telephone verification, that Akbar Wijaya also could not access the telephone number which is usually used for daily use. The telephone number can be accessed by users who register by including their KTP and family card numbers. In this case, Akbar

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

Wijaya's number was used by someone else on another device, as a result the data related to that number was discovered without the permission of Akbar Wijaya as the owner of personal data and the original user of Telkomsel's services as a telecommunication service provider. The applications used as communication media, namely whatsapp and telegram, also changed hands because they are directly connected to Akbar Wijaya's telephone number. However, the phone number is already in use by someone else on another device. When changing hands, it requires prior verification, such as sending an OTP (One Time Password) code to a device that uses a telephone number connected to WhatsApp and Telegram communication media.

This causes personal data leakage and shows that user security has not been implemented optimally. This incident proves that Telkomsel, as a telecommunications service provider, has failed to safeguard its users' cellular numbers and personal data. Akbar Wijaya said that the hack was a threat to the work of journalists. As a result of this case Akbar Wijaya asked for an explanation from Telkomsel but there was no answer and he transferred the matter to Whatsapp. The case of Journalist Akbar Wijaya shows that telecommunications service providers, namely Telkomsel as a business actor and controller of the telecommunications system, have not been able to provide guarantees for the condition of the products being traded and there is no good will from Telkomsel to correct errors in the security feature of the telephone number service belonging to Journalist Akbar Wijaya. This action shows that Akbar Wijaya as a consumer and journalist should receive compensation in accordance with Article 7 of Law no. 8 of 1999 concerning consumer protection which states that business actors have an obligation to act in good faith in providing guarantees in their business activities. As a telecommunications service provider, it is the responsibility of protecting the security of its products by providing compensation if the goods or services do not comply.

The purpose of the existence of compensation in civil law is to restore the condition to its original state before the occurrence of an unlawful act. Especially goods and services that do not meet consumer expectations. The explanation for returning to its original state is based on the theory of being properly accounted for (toerrekening naar redelijkheid) presented by Koster. This study will discuss legal protection for journalists in situations related to the responsibility of telecommunications service providers as business actors and controllers of telecommunications systems who have an obligation to provide compensation or compensation for product errors in their business activities. Discussion regarding legal protection for journalists is very important to improve the security of sources of information related to journalistic activities and the privacy of journalists.

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

II. RESEARCH METHODS

The legal research method used is normative by using library materials as a reference in research sources. This research is descriptive analysis in nature by examining problems for journalists who have the right to privacy to be protected, coupled with the existence of a Journalistic Code of Ethics and consumers who should receive compensation responsibility from business actors. The data collection method was carried out by means of a literature study and studying primary, secondary and tertiary legal materials adapted to the research problems. The data obtained was then analyzed using descriptive-qualitative by analyzing through secondary data sources that describe all information in the form of words or sentences. This method collects all information relating to cases of journalists who experience personal data leaks and the responsibility of telecommunications service providers to deal with these problems. The next step is to analyze the laws and regulations relating to the protection of journalists and draw conclusions regarding the analysis in this study.

III. RESULT AND DISCUSSION

1) Legal Protection for Journalists in Personal Data Leakage

Data is information that is processed through recording with tools that can automatically respond to instructions regarding the use of that information. Personal data can be defined as data that contains information from individuals such as date of birth, name, address, religion, and personal information about a person which is generally private. The definition of personal data is based on Article 1 point 1 of Law no. 27 of 2022 concerning the protection of personal data defines personal data as individuals who are identified or can be identified separately or combined with other information, either directly or indirectly through electronic or non-electronic systems. It is important to protect personal information, it is a right to privacy that must be protected and other people must not be involved in this personal data. In various developed countries, the term privacy is used as a right that must be protected, namely the right of a person not to be disturbed by his private life.

The rapid development of technology has an unfavorable impact in terms of personal data security. The responsibility of the electronic administrator is to maintain and keep confidential any important information for each user. Protection of personal data is very important in every electronic transition activity. Regulations regarding the protection of personal data have started to be made by several countries, one of which is Indonesia. Provisions regarding personal data are contained in Law no. 27 of 2022 concerning personal

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

data protection. There are still many digital platforms in Indonesia that are weak in terms of network security systems, especially in the scope of users' personal data. For example, data from digital platform users can be viewed and accessed in online forums. In the scope of technology such as digital platforms, this proves that regulations regarding the protection of personal data in Indonesia are still weak.

Law as a guide and controller of social order must be obeyed by all orders of life to maintain order in society. The relationship between protection and law concerns the fulfillment of community rights and obligations, because law provides rights that must be obtained and obligations that must be carried out by the community. Legal protection is a legal representation to protect legal subjects to get protection for the rights they have as human beings. Basically, people are obliged to get protection to have a sense of security as citizens so that the government is obliged to provide services to protect. Legal protection is the protection of dignity, as well as the recognition of human rights owned by legal subjects based on legal provisions of arbitrariness or as a collection of rules or rules that will be able to protect one thing from another.

As an Indonesian citizen, he is given the right to obtain protection based on Article 28 D paragraph 1 of the 1945 Constitution of the Republic of Indonesia which states that everyone has the right to recognition, guarantees, protection and fair legal certainty and equal treatment before the law. Legal protection for Journalist Akbar Wijaya related to personal data is one of the rights that are owned as individuals and users who can be called consumers of telecommunications service providers. According to Akbar Wijaya, cases of personal data leakage due to hacking experienced by journalists often go unresolved. As the sequence of events experienced by Akbar Wijaya shows the neglect of the apparatus and the state towards the protection of the privacy of its citizens which has been guaranteed and regulated in the constitution and laws

As individuals who work in journalistic activities, of course, incidents like this place a burden on journalist workers. In addition, the incomplete handling of the case against journalists made the victim desperate and made excuses for the incident. Al Ayyubi Harahap Legal Counsel from Akbar Wijaya said the independence of journalistic work should not be disturbed. As journalists also have ethics in maintaining integrity and credibility which are stated in the Journalism code of ethics to respect the right to privacy. If personal data belonging to the journalist profession suffers a data leak, of course, information regarding journalist activities in the form of contacts of the source's cellular numbers, conversations and recordings will also be known without permission. The data was afraid of being misused

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

because it experienced a leak which was previously the responsibility of the journalist. Therefore, it is important to re-enforce legal protection for journalists. In accordance with Article 8 of Law no. 40 of 1999 concerning the press that journalists in carrying out their journalistic activities receive legal protection. This law guarantees journalists to protect their rights, especially in the scope of personal data.

It is important to protect personal data because it relates to access to identity, personal documents, photos, contact lists, and use of social media. That personal data includes privacy that should not be known to other people. If you experience a personal data leak, it certainly has a sizable and detrimental impact. Problems regarding personal data are often ignored and the public does not understand much about the importance of protecting personal data. Based on the Indonesian state constitution regarding the right to protection of personal data contained in Article 28 G paragraph (1) of the 1945 Constitution it states that every individual has the right to protection for himself, his family, honor, dignity and the property he owns. They are also entitled to a sense of security and protection from threats that prevent them from doing or not doing something which is their human right. As a consumer, Akbar should have full control over the various services provided. However, in reality Akbar was logged out of his WhatsApp account and could not log back in with his Telkomsel number.

Since the enactment of the GDPR (General Data Protection Regulation) regulations regarding provisions for personal data protection from a business perspective concerning the processing and processing of personal data has been implemented throughout the world, one of which is Indonesia through the Personal Data Protection Act. The goal of the GDPR is that personal data obtained by employers is not misused by irresponsible parties. Within the GDPR itself there are many individual rights which include the scope of personal data protection that must not be violated, such as the right to request the deletion of personal data (right to be forgotten) and the right to receive information that a person's personal data has been transferred to another party (right to data portability). Literally right to be forgotten means the right to be forgotten. The official interpretation of this principle is the right to delete personal information that has been misused in acts of misuse of personal data.

In Law no. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions explained that every electronic system operator is required to delete irrelevant Electronic Information and/or Electronic Documents under his control at the request of the person concerned based on a court order and must provide a mechanism for deleting Electronic Information and/or Documents Electronics that are no

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

longer relevant in accordance with statutory provisions (Indonesia, 2016).

The application of the GDPR provisions also applies to telecommunications service providers, namely Telkomsel, in making cellular number business services to provide information or prior notification in the event of a network interruption. Journalist Akbar Wijaya as a user can anticipate so that he does not experience losses that impact both materially and immaterially. Enforcement of the provisions of Law no. 27 of 2022 concerning personal data protection allows telecommunication service providers to provide better services according to this law. Article 1 paragraph (2) in Law no. 27 of 2022 explains that the protection of personal data is all data about individuals who are identified or can be identified with other information, either directly or indirectly through electronic or non-electronic systems.

Telecommunications service providers have control over every network activity that concerns both IP addresses, records of telecommunications network activities and service usage. In the incident experienced by Journalist Akbar Wijaya, it is necessary to increase security and caution for any processing related to the network regarding personal data. Article 3 of Law no. 27 of 2022 states that every party related to personal data applies caution in every processing and monitoring of personal data. Telecommunications service providers as controllers of personal data based on Law no. 27 of 2022 concerning the protection of personal data, it is obligatory to be responsible for the security and protection of personal data. In accordance with Article 35 which states that personal data controllers are obliged to protect and ensure the security of the personal data they process, by doing:

a. Preparation and implementation of operational technical steps to protect personal data from interference with the processing of personal data that is contrary to the provisions of laws and regulations; And
b. 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 processing personal data.
c. Article 36 states that personal data controllers are responsible for maintaining the confidentiality of personal data when they process it, and Article 38 states that personal data controllers are responsible for preventing unauthorized processing of personal data. This article explicitly states legal protection of personal data from unauthorized processes or transactions.

2) Legal Settlements for Journalists for Leakage of Personal Data

In telecommunications networks, telephone numbers are used as intermediaries for

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

communicating in the form of text messages, telephone and the internet connected to telecommunications networks. In addition, if the security of the telephone number is not maintained, irresponsible people can use it to find out sensitive things that should not be known, such as knowing telephone contacts, data related to telephone numbers and telephone history. Telecommunications service providers such as Telkomsel, which provide cellular number services, apply terms and conditions for using their products. Several provisions contain security, safety and comfort in the use of goods and or services. Telkomsel also provides guarantees with responsibility if there is damage and loss incurred when using its products. Privacy protection is an obligation for everyone that must be maintained. This is one of the inherent rights of every individual related to self-identity. Protecting privacy means protecting freedom of expression. In other words, the right to privacy guarantees protection against the fear of doing or not doing something that is a human right (HAM).

This means that the responsibility carried out by telecommunications service providers is an obligation carried out by business actors in the technology sector to provide safe telecommunications by utilizing digital technology. However, the fact is that Telkomsel in the case of Journalist Akbar Wijaya has not been able to carry out its obligations properly. It is proven by the lack of caution in the telecommunications network security system which results in unusable telephone numbers and the transfer of numbers to other people without verification of the original owner of the number. This results in losses to users both in terms of material and immaterial. Personal data breaches in Indonesia are increasingly common, in the case of someone whose personal data is used by another person without permission for a specific purpose and seeking profit

Civil law regulates the protection of certain rights, both regarding personal rights and property rights and the law will protect with strict sanctions both for those who violate these rights, namely the responsibility to pay compensation to those whose rights are violated. Thus any action that causes harm to other people creates accountability. The principle of responsibility is a very important matter that telecommunications provider product providers must pay attention to in terms of compensation, because it requires carefulness and analysis of who should be responsible and how far the responsibility can be borne by related parties, namely product provider providers. telecommunications as a business actor. Product liability is the responsibility of producers or providers of telecommunication provider products as business actors for losses caused by their services.

Activities in electronic and telecommunication networks on digital platforms make

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

personal data a requirement to be able to carry out activities in the digital world. Personal data which is essentially private and confidential and may not be known to other people. Often a security system that is lacking in digital networks is used by irresponsible people to make personal data a loophole for carrying out prohibited actions. According to the UpGuard website, data in 2021 regarding the causes of personal data leakage include software configuration errors, fraud through social engineering, passwords or passwords that are used repeatedly, theft of items containing sensitive data, software vulnerabilities, and the use of passwords. default password. If personal data is leaked, of course it will have a detrimental impact on the owner of the data.

Civil law regulates the protection of certain rights, both regarding personal rights and property rights and the law will protect with strict sanctions both for those who violate these rights, namely the responsibility to pay compensation to those whose rights are violated. Thus any action that causes harm to other people creates accountability. The principle of responsibility is a very important matter that telecommunications provider product providers must pay attention to in terms of compensation, because it requires carefulness and analysis of who should be responsible and how far the responsibility can be borne by related parties, namely product provider providers. telecommunications as a business actor. Product liability is the responsibility of producers or providers of telecommunication provider products as business actors for losses caused by their services.

Activities in electronic and telecommunication networks on digital platforms make personal data a requirement to be able to carry out activities in the digital world. Personal data which is essentially private and confidential and may not be known to other people. Often a security system that is lacking in digital networks is used by irresponsible people to make personal data a loophole for carrying out prohibited actions. According to the UpGuard website, data in 2021 regarding the causes of personal data leakage include software configuration errors, fraud through social engineering, passwords or passwords that are used repeatedly, theft of items containing sensitive data, software vulnerabilities, and the use of passwords. default password. If personal data is leaked, of course it will have a detrimental impact on the owner of the data.

Disadvantages of personal data leaks include:

a. Receiving Lots of Spam

Sending spam is in the form of continuous messages in electronic devices which results in hoarding of important messages, taking up memory storage on the device and making the device susceptible to malware. Messages are sent via email, whatsapp, or advertisements

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

on the website. This action is detrimental to the privacy of the actual data owner.

b. Identity Abuse

Leaked personal data provides an opportunity for irresponsible people to use this identity. The use of this identity is done to deceive or phishing by convincing someone using a false identity. Second, the leaked data can be used as data for making online loans. As a result, the owner of the original data is involved in online loans from identity abuse by irresponsible people. Sometimes the owner of the data is suddenly called by an online lending company because of the use of data from irresponsible people.

c. Withdrawing Money from a Bank Account

Personal data is not only related to name, address, place and date of birth. Important data such as bank account numbers are also included in the scope of personal data which in essence should not be publicly known. Irresponsible people often carry out hacking actions through electronic devices by sending spam in the form of links to gain access to withdraw money without the knowledge of the owner of the account number. This action is certainly detrimental to the owner of the data and feels uncomfortable when using electronic devices.

Basically every individual has the right to obtain legal protection for personal data. In accordance with the provisions stated in Article 28 G Paragraph 1 of the 1945 Constitution. Every user complaint on a telecommunications network can be sent through Customer Service, as well as Telkomsel in carrying out telecommunications activities providing services in the form of fixing any user problems. However, after submitting complaints and conducting mediation with Telkomsel, no results have been obtained and no information has been provided by Telkomsel.

With regard to these problems, the need for a legal process to provide a settlement regarding cases of leakage of personal data. The legal process that can be taken is settlement through litigation (court) and efforts to resolve through non-litigation or outside the court. There are several ways that can be done when using non-litigation settlements, namely arbitration, negotiation, consultation, and mediation. As Article 64 paragraph (1) of Law no. 27 of 2022 concerning protection of personal data explains that personal data dispute resolution is carried out through arbitration, courts, or other alternative dispute resolution institutions in accordance with statutory provisions.

Akbar Wijaya has carried out the mediation process but there has been no resolution of the case. As a result, choosing the litigation route to provide efforts to resolve the sequence of

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

incidents of personal data leakage. The process of resolving disputes through the courts (litigation) is a dispute settlement carried out by proceedings in court where the authority to regulate, examine and decide on cases is carried out by judges. In the litigation process, the parties are placed against each other to defend their rights before the court. The end result of litigation is a win-lose decision in this case, one party loses and one party wins. It is hoped that the submission of a lawsuit against the law at the South Jakarta District Court will provide protection for journalists. This lawsuit serves as a security boost for other Journalists. The Personal Data Protection Act provides administrative sanctions if the party controlling personal data does not want to be responsible, these sanctions can be in the form of:

a. written warning;

b. Temporary suspension of Personal data processing activities;

c. Deletion or destruction of Personal Data; and/or

d. Administrative fine.

Legal efforts need to be made to protect the personal data of the journalist profession and the public. So that every telecommunications operator can make a communication system that has security and comfort in technological networks. The importance of protecting victims, considering that the losses suffered by consumers due to leakage of personal data can be felt both in terms of material and non-material, the value of the loss cannot be measured. In principle, legal protection in Indonesia consists of 2 (two) forms, namely preventive as a precautionary measure and also repressive as a handling measure.

Legal protection in Indonesia as a form of the state guarantees the security and peace of its citizens as contained in the values of Pancasila. With the existence of a preventive form, the goal is not to become a victim of a crime guaranteed by legal protection. Meanwhile, repressive includes protection for victims to compensate for the suffering or loss experienced by someone who is a victim of crime by obtaining compensation or guarantees. Broadly speaking, in principle protection for victims of crime must be seen or identified the type of loss or suffering experienced by the victim. So that if you already know the type of loss or suffering the victim can then provide appropriate protection regarding what victims of crime need.

IV. CONCLUSION

1) The acts of negligence and mistakes committed by telecommunications service providers, namely Telkomsel, can be categorized as unlawful acts because they have fulfilled the elements of unlawful acts in accordance with Article 1365 of the Civil Code. Where this

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572

causes losses to Journalist Akbar Wijaya from a material and immaterial perspective, especially the disruption of journalistic activities. Telkomsel as a business actor does not carry out its obligations in good faith, namely to provide compensation to Akbar Wijaya as a consumer for the incompatibility of Telkomsel's products. This is based on Article 7 of Law no. 8 of 1999 concerning consumer protection which states that business actors have an obligation to act in good faith in providing guarantees in their business activities.

2) Settlement of the personal data leakage case experienced by Journalist Akbar Wijaya initially started with mediation to obtain an explanation regarding the incident and as an effort to get Telkomsel responsible for errors in the telecommunication network. But Telkomsel did not make any effort and ignored the problems in this case. Akbar Wijaya's legal efforts are through litigation by filing lawsuits against the law in court to reveal the facts of what happened to journalist Akbar Wijaya and as a form of encouragement for the security of other journalists in telecommunications networks.

REFERENCES

[1] Abner, Winfritz Jeremia dan Christian Andersen. 2023. The Responsibility Telecommunication Service Providers Against Recycled Telephone Numbers from Consumer Protection Law. *Journal of Humanities and Social Sciences Innovation,* Vol No. 1.

[2] Ali, Zainuddin. 2021. *Metode Penelitian Hukum*. Jakarta: Sinar Grafika.

[3] Fadli, Andi. 2018. Etika dan Tanggung Jawab Jurnalis (Studi Pemberitaan Hoax mela Media Online di Kota Makassar). *Jurnalisa*, Vol. 04, No. 2.

[4] Ishaq, H. 2018. *Dasar-Dasar Ilmu Hukum*. Jakarta: Sinar Grafika.

[5] Makmur, Erick. 2021. *Sanksi Pelaku Wanprestasi*. Bandung: LBH Pengayoman Unpar.

[6] Manurung, Evelyn Angelita Pinondang, Emmy Febriani Thalib. 2022. Tinjauan Yuri Perlindungan Data Pribadi Berdasarkan UU Nomor 27 Tahun 2022. *Jurnal Huk Saraswati (JHS),* Vol. 04, No. 02.

[7] R., Muhamad Hasan dan Hartadi, Hanif. 2020. Kebijakan Penanggulangan Pencurian D Pribadi dalam Media Elektronik. *Jurnal HAM*, Vol. 11, No. 2.

[8] S. A., Kusnadi. 2021. Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *Al Was Jurnal Ilmu Hukum*, Vol. 2, No. 1.

[9] Soraja, Alga. 2021. *Perlindungan Hukum Atas Hak Privasi dan Data Pribadi Dal*

p-ISSN: 2502-826X / e-ISSN: 2503-1163
DOI: https://doi.org/10.35457/jares.v9i2.3572
Prespektif HAM, Seminar Nasional - Kota Ramah Hak Asasi Manusia, Vol. 1.

[10] Tsamara, Nadiah. 2021. Perbandingan Aturan Perlindungan Privasi atas Data Prib Antara Indonesia dengan Beberapa Negara. *Jurnal Suara Hukum*, Vol. 3, No. 1.

[11] Zaman, Akbari Amarul, Jumadi Anwar, Aryo Fadlian. 2021. Pertanggung Jawaban Pid Kebocoran Data BPJS dalam Perspektif UU ITE. *De Juncto Delictio,* Vol. 1, No