JRSSEM 2023, Vol. 03, No. 03, 603 – 620
E-ISSN: 2807 - 6311, P-ISSN: 2807 - 6494

LEGAL PROTECTION OF TELECOMMUNICATION SERVICE CUSTOMERS' PERSONAL DATA AS TRADE SECRETS IN MERGER AND ACQUISITION PROCESSES BASED ON POSITIVE LAW IN INDONESIA

Amelia Rossame[1]
Sinta Dewi Rosadi[2]
Rika Ratna Permata[3]
Faculty of Law, Universitas Padjadjaran, Indonesia[1,2,3]
Email: amelia19006@mail.unpad.ac.id, sinta@unpad.ac.i, permata_rika@yahoo.com
*Corespondence: amelia19006@mail.unpad.ac.id

ABSTRACT: The fast advancement of information and communication technology has had a positive influence on society. The free and open transmission of knowledge is the ideal condition for its application. Meanwhile, information technology itself serves as a channel for information dissemination. Customer data received by telecommunications service providers is a trade secret of the corporation since it has economic worth, is confidential, and is kept confidential. Customer personal data, on the other hand, is sensitive and deemed harmful since telecommunications service providers indirectly gain from someone's privacy. This paper will compare the legal framework if there is a legal conflict between personal data and trade secrets based on positive law in Indonesia that applies the GDPR principles to the personal data protection system adopted by other nations, take, for example, the United States, Europe, also Australia. In accordance with the attached case, namely a data breach by Optus, an Australian telecommunications company, the author wishes to examine it within the scope of positive law in Indonesia by comparing legal settlements that have been implemented in Australia, so that if a data breach occurs in Indonesian territory as a result of telecommunications industry mergers and acquisitions, the author will be able to analyze it within the scope of positive law in Indonesia and can be a basis for answering questions regarding legal protection and accountability. The research used normative juridical procedures, and the writing stage was completed by an in-depth review of secondary data, which comprised original legal documents, literature, articles, expert views, and teachings, as well as their application in statutory regulations.

Keywords: Personal Data Protection, Trade Secrets, Merger and Acquisition

INTRODUCTION

The rapid development of technology brings humans to continue to innovate with the aim of achieving effectiveness and efficiency in doing all work. In the era of the 5.0 industrial revolution, massive technological developments are a direct and indirect impact of the rapid flow of globalization, causing humans to continue to adapt in new changes that change the order system and way of life of people in various sectors. Indonesia is a country that is quite affected by the impact of globalization, especially in the field of technology. That indeed technology has coexisted with humans and cannot be separated. Technology became an important tool that will continue to be used in life even until the end of human civilization (Damar, 2018).

The optimal condition for the utilization of information is the free and open circulation of information. While the medium for information circulation is information and technology itself. According to Law Number 36 of 1999 concerning Telecommunications, the definition of telecommunications is as follows:

> "*Telecommunication is any transmission, transmission and/or receipt of any type of information in the form of signs, writing, images, sounds and sounds through wire, optic, radio or other electromagnetic systems.*"

Telecommunications are a human *platform* for communication that has advantages over other communication platforms, due to its ability to send information at high speed that can be received *in real time* and even able to penetrate national borders. Through telecommunication itself, whether by telephone, radio, facsimile or television, people can easily exchange information. This development is also supported by the existence of the internet that supports human activities. Directly social life in various sectors is transformed and digitalized due to the influence of the internet (Sugeng, 2020).

With good telecommunications infrastructure, it will certainly have an impact on the efficiency and productivity of the community at large. ICT-based platforms in Indonesia have seen an increase in their usage. Both the government and private sectors have used and improved their performance services through ICT so that the telecommunications service industry plays an important role in this. People have a position as consumers or can also be called users or customers. A customer is an individual that has signed up and agreed to follow the rules of an electronic contract. Customers in the telecommunications industry are consumers since they have purchased a product that they have used more than once (Zawil Fadhli, 2018).

The telecommunications service industry as a network provider has the right to collect customer data information for the benefit of the

company. Data obtained by the telecommunications service industry comes from the registrants of these *providers*, namely their users, from individuals and institutions, both voluntarily, and those reached directly. To be able to use telecommunication services, customers must register a prepaid cellular card or *simcard*.

The identity contained in the customer registration process is in the form of NIK (Family Identification Number) and KK (Family Card) which are part of personal data. Card registration is the utilization of personal information, as it aligns with the personal data described in Article 1 Paragraph (1) of Law Number 27 of 2022 concerning the Protection of Personal Data:

> "*Personal Data is data about natural persons who are identified or can be identified separately or combined with other information either directly or indirectly through electronic or non-electronic systems.*"

The objective of delivering competitive advantages to telecommunications customers, such as reduced pricing, more quality, and greater innovation, has effectively removed numerous obstacles to entrance into the larger telecommunications sector. When these restrictions are lifted, some corporations may consider it strategically advantageous to join a new market by merging, acquiring, or creating partnerships with enterprises already present in that industry. Because information or data is considered a trade secret, there is some overlap between trade secret law and personal data protection legislation. Based on Law Number 30 of 2000 concerning Trade Secrets, what is meant by Trade Secrets is listed in Article 1 paragraph (1) of the Trade Secret Law, namely (Edwin. A., 1997):

> "*Trade Secrets are information that is not publicly known in technology and/or business, has economic value because it is useful in business activities, and is kept confidential by the owner of the Trade Secret*."

Customer data received by telecommunications service companies is a company trade secret because it is economically valuable, confidential, and kept confidential. However, on the other hand, customer personal data is also sensitive and considered detrimental because indirectly telecommunication service companies benefit from one's privacy. Moreover, in the event of a merger or takeover (mergers and acquisitions).

Merger is a legal action undertaken by one or multiple companies to consolidate with another established company which leads to the switched of the assets and liabilities of the merged company because of the law

to the company that agrees to the merger, then the legal entity status of the merging company terminates in accordance with the law. While takeover, also known as acquisition, refers to a legal action undertaken by either a legal entity or an individual to take over of a company's shares, consequently leading to a transfer of control over the company. The customer data will be distributed to other telecommunication service providers so that it can potentially be known to third parties without the consent of the individual whose personal data is involved, namely the customer. These personal data breaches can be caused by worker changes or system changes in telecommunications provider services.

The Personal Data Protection Law in Indonesia adheres to many of the arrangements of the *General Data Protection Regulation* (GDPR) applied by countries in Europe. However, in other nations such as the United States have different arrangements regarding when it comes to data as a trade secret.

In this study, the author will describe the comparison of legal arrangements if there is a legal cross between personal data and trade secrets based on positive law in Indonesia which applies the principles of GDPR with the personal data protection system adopted by other nations such as the United States and Australia. This paper will raise data breaches by Optus, which is a telecommunications company in Australia, the author wants to study it within the scope of positive law in Indonesia by comparing legal settlements that have been implemented in Australia, so that if data breaches due to *mergers* and acquisitions of the telecommunications industry occur within the territory of Indonesia, this research can be a focus to answer questions about protection law and its accountability.

RESEARCH METHODS

The research employed a normative juridical approach. The research specifications used are descriptive analysis research specifications, namely research methods that conducted by collecting data in compliance with the fact or truth, then the data is collected, organized, processed, and analyzed to offer a comprehensive analysis of the existing problem. This research uses qualitative juridical analysis, that is, the data obtained will be analyzed qualitatively from the legal science perspective and does not use formulas. The data analysis process will begin based on general facts and then compare with the results of the data that has been obtained for conclusions.

RESULT AND DISCUSSION

Crossover Analysis of Personal Data Protection Law and Trade Secret Law in Company Mergers and Acquisitions

Data is an intangible asset with economic worth since it is in the form of information, and information is an intangible asset whose development

process necessitates economic expenditure to be included in intellectual property. In theory, intellectual property may be defined as intangible value coming from human thought or creativity that results in a production or innovation with economic advantages in the disciplines of art, literature, science, and technology. Trade secrets cover intellectual property rights that include data protection. Researchers will investigate the overlap between data protection laws and intellectual property laws in determining the data position regime of telecommunications service clients.

Based on data analysis, the worth of an individual's personal information has revolutionized marketing techniques and company structures. The sophistication of digital telecommunications system technology has resulted in processes in information systems that anyone can access, causing legal issues such as privacy, criminal action, proprietary rights in information, ownership of and access to information, legal rights to communicate, and territoriality concepts. In terms of data's role in privacy, in today's digital technology era, private data is becoming increasingly accessible to access, process, gather, and alter rapidly and inexpensively. Today, customer information (client list and all customer-related data) is critical for any company since it is economically useful as a form of protection for its own clients as well as a foundation for marketing plans, corporate rules, and so on (Danriyanto, 2017); (Yuniarti, 2019).

Data is currently being monetized as a financial growth strategy by various organizations and corporate entities. As discussed in the last chapter regarding information or data, in industry 5.0, data is an intangible commodity that may raise the worth of a company organization. Telecommunication service customer data has value in the telecoms service business and may be maximized such that an increase in the number of registrants or registrants of a provider results in an increase in the asset values of the telecommunications service provider firm. Most of the protected information is held as data, including customer data covered by the trade secret regime. Assets are intended to generate a profitable value for the entity and that value is expected to be able to fulifill the requirements of the entity's activities in question, so that there is a close relationship between Personal Data information and Trade Secrets, particularly in cases of data breaches (Eleanor, 2023). Because trade secrets are one of the assets, property rights theory is one of the ideas concerning trade secret protection. Trade secrets are proprietary property that can be guarded against anybody who tries to misuse or exploit them without permission. Provided that it does not infringe applicable laws, the owner has the right to make the broadest possible use (Mind agus, 2004).

Regarding how trade secrets can be given legal protection is contained in Article 3 of the Trade Secret Law, namely:

(1) Trade secrets are protected if the information is confidential, has economic value, and is kept confidential through appropriate efforts.
(2) Information is considered confidential if the information is only known by certain parties or is not publicly known by the public.
(3) Information is considered to have economic value if the confidential nature of the information can be used to carry out activities or businesses of a commercial nature or can increase economic profits.
(4) Information is kept confidential if the owner or the parties who control it have taken appropriate and appropriate steps.

Based on the explanation of the article, data containing customer personal information is included in trade secrets that need to be protected because they meet the elements in Article 3 of Law Number 30 of 2002 concerning Trade Secrets, namely secrets, have economic value, and are kept confidential through adequate efforts where only known by certain parties or not generally known by the public, which in this case is only known by telecommunications service companies. Furthermore, it can be utilized to carry out activities or businesses that has commercial purposes or it can also be utilized to increase monetary profit.

Indonesia already has a trade secret regulation, specifically laws Number 30 of 2000 Concerning Trade Secrets. While the Uniform Trade Secret Act of 1985 (UTSA) governs civil elements of trade secrets in the United States. In Article 1, section (4) of the *Uniform Trade Secrets* Act, initially promulgated in 1979 and subsequently revised in 1985 in the United States, it is stipulated that:

> "*Trade secret*" *means information, including formulas, patterns, compilations, program devices, methods, techniques, or processes, that: (i) derives independent, actual or potential economic value, from not generally known, and not readily ascertained in a manner appropriate by, others who can derive economic value from its disclosure or use, and (ii) is the subject of reasonable efforts under the circumstances to keep it confidential*."

The United States also regulates the criminal aspects of trade secrets regulated in the *Economic Espionage Act of 1996* (EEA). This regulation has been amended by the *Defend Trade Secret Act of 2016* (DTSA) specifically aimed at regulating trade secret theft. DTSA itself

also explains what trade secrets are with more complicated content, namely:

> "*The term 'trade secret' means any form and type of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, x programs, or code, whether tangible or intangible, and whether stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if or in any form - (A) the owner has taken reasonable measures to keep confidential such information; and (b) the information derives economic value independently, actual or potential, from not publicly known, and not easily ascertained by appropriate means, others who could derive economic value from the disclosure or use of the information.*"

In line with the Law in the United States, positive law in Indonesia has regulated the provisions regarding trade secrets contained in Article 1 paragraph (1) of Law Number 30 of 2000 concerning Trade Secrets which reads:

> "*Trade Secrets are information that is not publicly known in technology and/or business, has economic value because it is useful in business activities, and is kept confidential by the owner of the Trade Secret.*"

The UTSA and DTSA do not restrict the amount of information that may protected in a Trade Secret to the extent that it is kept private by the holder of the trade secret and has value to the economy, either actual or hypothetical, from informational ignorance and cannot be ascertained through appropriate means by others who can benefit financially from the disclosure or use of the information. The DTSA describes more diversified types of trade secrets, including both tangible and intangible sensitive knowledge. The Trade Secret Law does not specify what information can be protected in what form, but the scope of the trade secret is defined in Article 2 of Law Number 30 of 2002 Concerning Trade Secrets, which states:

> "*The scope of Trade Secret protection includes production methods, processing methods, sales methods, or other information in the field of technology and/or business that has economic value and is not known to the general public.*"

Trade secret infringement is governed by Article 13 of Law Number 30 of 2002 concerning Trade Secrets, which reads in part, "Trade Secret infringement also occurs if someone intentionally discloses a Trade Secret, reneges on an agreement, or reneges on a written or unwritten obligation to safeguard the Trade Secret concerned." This point is further supported by Article 14, which states that "a person is considered to violate another party's Trade Secret if he obtains or controls the Trade Secret in a manner contrary to applicable laws and regulations. "Although section 1839 para. 5 of the DTSA, which regulates data breaches, defines misappropriation (misuse) in a different way, namely:

> "*The term 'misuse' means—(A) the acquisition of a trade secret from another person by a person who knows or has reason to know that the trade secret was obtained by improper means; or (B) disclosure or use of another party's trade secret without the express or implied consent of a person who— (i) uses improper means to obtain knowledge of the trade secret; (ii) at the time of disclosure or use, knew or had reason to know that knowledge of the trade secret — (i) was obtained from or through a person who had used improper means to obtain the trade secret; (II) obtained in circumstances that give rise to an obligation to maintain the confidentiality of trade secrets or restrict the use of trade secrets; or (III) originates from or through a person who owes a duty to the person seeking assistance to maintain the confidentiality of trade secrets or restrict the use of trade secrets; or (iii) prior to a material change of such person's position, knew or had reason to know that— ''(i) a trade secret is a trade secret; and ''(II) knowledge of trade secrets has been acquired by accident or error.*"

Customer information is generally protected as a "trade secret," which is a sort of intangible information monopoly. European data protection legislation, on the other hand, limits the processing of this data, providing data subjects a sort of "monopolistic control." Because they concern the same substance (customer personal data), these two sorts of intangible monopolies are clearly antagonistic. In such cases, an examination into when and how customer data may qualify as trade secrets and personal data is required in order to establish when the extent of trade secret laws concretely collides within the purview of data protection legislation.

Because some data is part of the business's economic monopoly while also subject to the monopoly of individual 'privacy' (consumers, users), data management becomes extremely difficult. According to the European

Data Protection Supervisor (EDPS), trade secrets include "data such as information about customers and suppliers, business plans or market research and strategies," "client/customer lists; internal datasets containing research data," "private collections of each publicly available item of information," and "customer data and their behavior, as well as the ability to collect and monetise such data.".

Telecommunication Service Providers' Responsibilities as a Legal Protection Measure for Customer Service Customer Data in Avoiding Data Breaches of Customer Privacy Data Throughout Company Mergers and Acquisitions

The state fundamentally protects human rights based on Article 28 G of the 1945 Constitution, which states that the right to private privacy is a human right, even though it is expressed indirectly in the article. As noted in Article 1 paragraph (3) of the 1945 Constitution, Indonesia is a state of law, which means that the guarantee of protection of human rights, including the right to protect personal data from being accessed, used, or disclosed without consent, is founded on the rule of law. According to Article 1 Paragraph 1 of Law Number 27 of 2022 Concerning Personal Data Protection, "personal data" refers to information or data related to individuals that can be identified or identified when combined with other data directly or indirectly, whether through electronic or non-electronic means. The owner of the data means that the data has a relationship with a party that is used to solve an issue or make identification. Because trade secrets are becoming more valuable in the age of disruption and digitization, there is an urgent need for regulation. To uphold the respect of personal privacy, it is imperative to establish the right to data protection, and that is precisely why this study merges the principles of data protection with telecommunications services (D. Priadi, 2018).

Currently in positive law in Indonesia there is no specific regulation that regulates information, especially in Telecommunication Services. Information that is limited to access to its owner relates to trade secrets that are confidential. Protection regarding own data related to the telecommunications service industry has actually been regulated in Law Number 36 of 1999 concerning Telecommunications, PP Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, Law Number 11 of 2008 concerning Electronic Information and Transactions. Based on Law Number 36 of 1999 concerning Telecommunications, article 42 paragraph (1) stipulates that:

> "*Telecommunication service providers must keep confidential information sent and or received,*

by telecommunication service customers through telecommunication networks and / or telecommunication services they organize."

Then, Article 40 of the Telecommunications Law also states, namely: "*Everyone is prohibited from intercepting information transmitted through telecommunications networks in any form.*"

In accordance with the data breaches of telecommunications firms that have completed mergers and acquisitions, the author brings up the case of the Optus provider data breach, Australia's largest telecommunications services provider. Through its Australian division, SingTel Australia Investment Ltd (SingTel Australia), Optus is a fully owned subsidiary of Singapore Telecommunications Limited (SingTel). Singtel Australia has completed the obligatory acquisition of all outstanding ordinary shares of Cable & Wireless Optus Limited (Optus), and because of this transaction, Singtel Australia currently owns 100% of Optus shares. On September 22, 2022, a cyber assault was directed at Optus, which resulted in the leak of personal information about its customers. Customer information from Optus, including personal details such as full name, birthdate, email address, passport number, driver's license, and Medicare card, and has been compromised. More than six months after Optus announced the big attack, a class action lawsuit was launched on behalf of consumers who believed the business was putting at risk their safety. Slater and Gordon, a legal firm, has filed a class action lawsuit in Federal Court, representing the interests of more than one hundred thousand people who have signed up.

According to the case, Optus violated the privacy of its customers and broke the rules governing telecommunications companies and failed to safeguard consumers from harm. An Optus representative stated that the business was aware of Slater and Gordon's class action filings and will handle them through the proper legal processes. Personal information from around 10 million current and past Optus customers was taken in the attack, which the major telecommunications firm reported in September last year. Singtel established a "customer action programme" to respond to the incident, which includes external reviews, third-party credit monitoring services for concerned clients, and replacement of customer identity papers. The company acknowledges that at this stage the full financial impact of the various investigations into the breach is unknown and continues to take legal action.

In the case of such an infraction, Optus has committed to fund the costs of replacement passports. Optus' communications manager expressed regret for the data breach and allocated

one hundred forty million dollars to assist customers who were affected update their identification documents and to commission independent investigations into the incident. The company also pledged to invest more in protecting its networks and regaining customer trust. Optus will notify all current and previous customers who are affected. Optus has been punished by the federal government for what Home Secretary Clare O'Neil regards as a "basic" cybercrime attempt. The business vehemently denied any involvement in the incident, which is being probed by the Australian Federal Police, the Australian Information Commissioner, and the ACMA (Australian Communications and Media Authority). As a follow-up and accountability action, an Australian Government Agency prepared a pamphlet about the Optus data leak. Scamwatch ACSC (Australian Cyber Security Centre) has been designated by the government as the principal point of contact for clients seeking guidance on how to secure their personal information.

Scamwatch also provides information on the latest scams that reference Optus violations. The government is taking steps to minimize the negative consequences of the Optus data breach and is exploring every possible way to protect and regenerate the identity documents of victims following a cyber-attack. The government is considering all options for protecting and documenting victims' identity. The Australian Federal Police (AFP) has launched two operations to investigate and address the cybercrime incident. Operation Hurricane will focus on the criminal aspects of the offence, while Operation Guardian, under APF-led JPC3, a joint initiative with the private sector and industry, will focus on combating cybercrime more broadly. Guardian is committed to helping consumers who have been harmed by cybercrime and working with industry to improve public protection.

The AFP also monitors criminals who are trying to exploit compromised data on online forums such as the internet and the dark web. The AFP will not hesitate to pursue anyone who violate the law. Optus receives cybersecurity incident response assistance from the Australian Cyber Security Centre, which also helping other Australian telecommunications companies to improve their cybersecurity. The Department of Home Affairs collaborates with state, territory, and commonwealth authorities to limit the use of potentially fraudulent papers. If an Australian resident's Medicare card information has been compromised, Australian Health Services will replace your Medicare card at no cost.

If the consumer later suspects illegal activity on one of our Services Australia accounts, the customer should notify the Fraud and Identity Theft Help Desk. Passports continue to be legitimate for travel to foreign countries.

The Australian Government acknowledges that Optus customers who were affected may have concerns regarding passport identity theft. Customers who want to update their passports can get in touch with the Australian Passport Office. The Australian Securities and Investments Commission has also provided instructions for safeguarding Australian nationals from identity theft on Moneysmart's website.

Positive law is a substance utilized in court to decide cases. Lex Specialis Derogat Legi Generali is a legal theory that states that a special law will take precedence over a general law (Peter, 2020). Although personal data protection is indirectly regulated in other laws such as the ITE Law or PP PSTE, considering that Indonesia already has special regulations governing personal data so that the Personal Data Law (PDP Law) becomes the main reference if there is a breach involving personal data, especially in this study where companies that have or will merge or acquire. Indonesia has passed a personal data protection regulation through Law Number 27 of 2022 concerning Personal Data Protection. In the context of company mergers and acquisitions, It has been regulated in relation to the transfer of personal data subjects to personal data controllers in the form of legal entities doing legal operations such as mergers and acquisitions. According to Article 48 of Personal Data Protection Law Number 27 of 2022:

"*(1) The Personal Data Controller in the form of a legal entity that merges, splits, expropries, merges, or dissolves a legal entity must notify the transfer of Personal Data to the Personal Data Subject.*
(2) Notification of transfer of Personal Data as referred to in paragraph (1) shall be made before and after the merger, separation, acquisition, amalgamation, or dissolution of a legal entity.
(3) In the event that the Personal Data Controller in the form of a legal entity dissolves or is dissolved, the storage, transfer, or destruction of Personal Data shall be carried out in accordance with the provisions of laws and regulations.
(4) The storage, transfer, deletion, or destruction of Personal Data as referred to in paragraph (3) shall be notified to the Personal Data Subject.
(5) Further provisions regarding notification procedures as referred to in paragraph (l), paragraph (21, and paragraph (4) shall be regulated in Government Regulations."

As already explained, Article 48 of the Personal Data Protection Law has explained the obligation of a legal entity company to provide the person whose personal data is being collected or

processed in the event with information about a merger or takeover (merger and acquisition) either after or before the legal action is carried out. Legal acts such as mergers and acquisitions of telecommunications companies have the potential to transfer personal data between company A and company B. The provisions regarding the transfer of personal data by the personal data controller in the jurisdiction of Indonesia are clearly regulated in Article 55 paragraph (2) of the Personal Data Protection Law, namely:

> "*(2) The Personal Data Controller who transfers Personal Data and who receives the transfer of Personal Data shall carry out Personal Data Protection as referred to in this Law*."

If the data transfer is outside the territory of Indonesia, then based on the provisions stated in Article 56 paragraphs (2), (3) and (4) of the PDP Law, the personal data controller must ensure that the place of residence of the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data has a degree of Personal Data Protection similar to or greater than that provided in this Law, but if this is not met, the Personal Data Controller should guarantee appropriate and enforceable Personal Data Protection. If the country where the personal data is being sent to does not have regulations governing personal data or cannot ensure that there are legal protections for personal data in the country where it is being sent to, the controller of personal data is required to secure the consent of the individual whose personal data is involved.

Issues that frequently arise in the trade secret regime concern how trade secret owners and recipients understand their rights and obligations in protecting trade secrets, the importance of trade secret protection in creating competitive competition for trade secret owners, and, most importantly, the form of default in trade secrets and the actions taken to guarantee that trade secrets do not leak. A non-disclosure agreement (NDA) is a legally binding contract between two or more parties that outlines confidential information that the parties wish to share with each other for specific purposes, such as employment or business deals. A non-disclosure agreement, often known as an NDA, is a confidentiality agreement that is widely used in a collaboration or employee bond with employers or in a cooperation between the Parties to preserve sensitive information belonging to the disclosing Party (Subekti, 1987); (Asry, 2019).

In maintaining confidential company information, the company owner uses a confidentiality agreement to bind workers so as not to violate the rights of Trade Secrets. With the *confidentiality agreement*, workers are not only bound when they are still working but also when the worker is no

longer working at the company. So the confidentiality agreement gives obligations and responsibilities to workers to keep information secret and prevent it from being disclosed from the company in accordance with the *agreed confidentiality agreement* at the time of employment and the end of the work period. The presence of a Merger or Acquisition in a firm has the possibility for position rotation, replacement of human resources, or termination of work rights, as well as the transfer or mutation of workplaces from workers. Article 52 paragraph (1) point an of Manpower Law Number 13 of 2003 states: "the employment agreement is made on the basis of: a. agreement of both parties." In the work agreement, both parties agree to make confidentiality clauses containing trade secrets that must still be maintained even after the employment agreement has ended, because the confidentiality agreement is continuous. Workers have entire responsibility for their responsibilities to safeguard the confidentiality of firm information in accordance with the confidentiality agreement that has been agreed upon with business actors as the possessor of trade secrets under the confidentiality agreement. If the employee fails to fulfill his responsibilities, it is deemed a Trade Secret infringement. According to Article 13 of Trade Secrets Law Number 30 of 2000:

> "*Trade Secret infringement also occurs when a person knowingly discloses a trade secret, reneges on an agreement or reneges on a written or unwritten obligation to safeguard the Trade Secret in question*."

Meanwhile, Article 4 of Law Number 30 of 2000 concerning Trade Secrets explains the rights of Trade Secret owners:

> "*The owner of the Trade Secret has the right to:*
> *a. use of its own Trade Secrets.*
> *b. grant a License to or prohibit others from using Trade Secrets or disclosing Secrets*."

In the event of a Trade Secret's rights being violated, the article stipulated in Article 11 of Law Number 30 of 2000 concerning Trade Secrets:

> "*(1) The Trade Secret Rights Holder or the Licensee may sue any person who intentionally and without rights commits the acts referred to in Article 4, in the form of:*
> *a. claims for damages; and/or*
> *b. termination of all acts as referred to in Article 4.*
> *(2) The claim referred to in sub-article (1) shall be filed in the District Court*."

Breach of a Non-Disclosure Agreement is considered to occur if, first, information is obtained without the consent of the people or organizations

that have the legal right to control the information, such as information gained through spying activities, computer data hijacking, or information theft, even if unintentionally, such as a misaddressed fax. In this regard, there remains the view that the obligation to maintain confidentiality remains and is imposed on the person who obtained the information without such consent. Second, where the information obtained has been misused without the consent of the party who legally has control over the information, then any use or disclosure of the information will be considered as without authority. Basically, the information is limited purpose which means that the information may only be used and disclosed for a limited purpose (Rahmi, 2007).

According to these regulations, trade secret infringement occurs when someone deliberately exposes information or reneges on an agreement or reneges on the responsibility (breach) for the engagement he has made to preserve the trade secret, either directly or implicitly. Article 14 of Trade Secrets Law Number 30 of 2000 clarifies that "a person is considered to violate another party's Trade Secret if he obtains or controls the Trade Secret in a manner that is contrary to applicable laws and regulations". *Non-Disclosure Agreement* can be used as one of the legal protections where the rights and obligations incurred by it. There can be a clause in the confidentiality agreement that the parties agree on, at least the party who receives information about the trade secret is prohibited from divulging to the public or any party outside the agreement, starting the receiving party's work begins or is completed and calculated within a certain period of time since the employee or employee quits, is dismissed, or mutated to another company that undergoes a merger or takeover. As a result, the Non-Disclosure Agreement can be utilized as a preventative instrument to safeguard the trade secret owner's proprietary knowledge.

CONCLUSION

In light of the research, it is conceivable to conclude that there is an overlap of telecommunications service customer data because the data in the form of personal information has economic value that is useful to the company but on the other hand is individual personal information, so the interaction between the two clearly should not be based on absolute exploitation but must be subject to applicable regulations or appropriate personal data processing principles. In the Telecommunications Law, there is no provision regarding the legal protection of personal data subjects, especially in mergers and acquisitions of telecommunications companies, so that if there is a violation, it must refer to Article 48 of the PDP Law which regulates Personal data controllers in

the form of legal entities that carry out mergers and acquisitions are required to notify Personal Data Subjects of the transfer of Personal Data. A notice to the individual or organization whose personal data is being transferred aims to prevent unwanted leakage of data to third parties outside the data processing agreement unknown to the Personal Data Subject. In the Trade Secret Law, it is also stated that if there is a violation of the Trade Secret, the company that has the legal right to control the use and disclosure of the trade secret can settle it civilly by referring to Article 11 of the Trade Secret Law, namely through a claim for compensation, termination of trade secret infringement activities or a lawsuit to the district court. As a preventive measure for companies, *Non-Disclosure Agreement* or NDA can also be used as an alternative because NDA binds workers to comply with company confidentiality agreements, which in this case is telecommunications service customer data.

SUGGESTION

Unlike trade secret arrangements or regulations such as in America, the Positive Law in Indonesia does not explain in detail what kind of data position can be categorized as assets that fall into the scope of intellectual property. More diverse forms of trade secrets are described in the United States DTSA, namely the storage of Trade Secrets which are tangible or intangible confidential information. In the Indonesian Trade Secret Law, it is not clearly explained what information can be protected, it is only implicitly explained in Article 25 of the ITE Law. To fill the legal void, there must be a clear provision regarding the position of data not only in the context of privacy but also in the context of trade secrets, because as humans' and technological advances' ability to analyze data improves, the accepted notion of privacy will inevitably change.

Related to the writing of this final project which raises telecommunications service companies as the object of research, because there are no regulations regarding mergers and acquisitions of telecommunications companies that require companies to maintain the confidentiality of personal data subject information so that the PDP Law that has been passed becomes a legal instrument that can accommodate in the event of a data breach because. Furthermore, the Optus Case, which the author has addressed, may be used as a reference if there is a data breach of telecommunications firms that have completed mergers and acquisitions in Indonesia, and corporations and the Indonesian government can take appropriate steps, as occurred in Australia.

REFERENCE

Budhijanto, D. (2017). *Revolution Cyberlaw Indonesia: Updates and Revision Law Information and Transaction Electronic 2016*. Bandung: Refika Aditama.

Damar, A. M. (2018, February 12). *Indonesia Has Startup Most in the World after The U.S. and English*. Retrieved from Liputan 6: https://www.liputan6.com/tekno/read/3276742/indonesia-have-Most-startups-in-the-world-after-as-and-English

European Union Agency for Fundamental Rights and Council of Europe. (2014). *Handbook on European Data Protection Law*. Belgium: Council of Europe.

Fadhli, Z., & Marine, S. (2018). Protection Law Towards Customer Telecommunication Services Deep Registration Cards Of Prepaid Through Outlets (One Research in Banda Aceh City). *Journal Scientific Student Field Law Civil Affairs Faculty University Law Shia Kuala, Vol. 2(4)*, 744.

Jened, R. (2007). *Hak Kekayaan Intelektual Penyalahgunaan Hak Eksklusif*. Surabaya: Airlangga University Press.

Marzuku, P. M. (n.d.). *Pengantar Ilmu Hukum*. Jakarta: Kencana Prenada Media Group.

Muhammad, Abdulkadir. (2001). *Kajian Hukum Hak Kekayaan Intelektual*. Bandung: PT. Citra Aditya.

O'Neill, E. (n.d.). *10 Companies That Are Using Big Data*. Retrieved from CA Today: https://www.icas.com/ca-today-news/10-companies-using-big-data

Pariadi, D. (2018). Supervision E Commerce deep Law Trade and Law Protection User. *Journal Law and Development, Vol. 48, Number 3*, 653.

Rismawaty, A. (2019). Non Disclosure Agreement Sebagai Perlindungan Hak Kekayaan Intelektual Dalam Perjanjian Kerjasama. *Journal Aktualita Vol.2, Number 1*, 341-342.

Riswandi, M. A., & Shamsudin, M. (2004). *Rights Wealth Intellectual Property and Culture Law*. Jakarta: PT. Raja Grafindo Persada.

Rosenberg, Edwin A. (1997). *Telecommunications Mergers and Acquisitions : Key Policy Issues and Options for State Regulators*. Columbus: The National Regulatory Research Institute.

Subekti, R. (1987). *Hukum Perjanjian*. Jakarta: PT. Intermasa.

Sugeng. (2020). *Hukum Telematika Indonesia*. Jakarta: Kencana.

Yuniarti, S. (2019). Protection Data Law Personal In Indonesia. *Journal Becoss, Vol. 1 No.1*, 147-154.