JURNAL JURISPRUDENCE
Vol. 14, No. 2, 2024, pp. 171-191
p-ISSN: 1829-5045 ; e-ISSN : 2549-5615
Website: https://journals2.ums.ac.id/jurisprudence/issue/view/257

Comparison of Protection Laws Private Data in Indonesia, and the Philippines

Amiludin
Universitas Muhammadiyah Tangerang, Indonesia
Amiludin@umt.ac.id

Siti Nurhalisa
Universitas Muhammadiyah Tangerang, Indonesia
siti.nurhalisa03012001@gmail.com

Undang Prasetya Umara
Universitas Muhammadiyah Tangerang, Indonesia

Hidayatulloh
Faculty of Law, University of Miskolc, Hungary
h.hidayatulloh@student.uni-miskolc.hu

DOI: 10.23917/jurisprudence.v14i2.4266

Submission Track:

Received:
February 6, 2024

Final Revision:
Mey 25, 2024

Available online:
December 30, 2024

Corresponding Author:

ABSTRACT

Purpose of the study : Comparing private data protection regulations in Indonesia and the Philippines, find out the court decisions and judges' considerations of private data cases in the two countries, and to know the dispute resolution mechanisms related to private data cases in the two countries.

Methodology : This research method uses literature review studies derived from books and journals or articles that have been published.

Results : The research found revealed comparison of regulations private data protection in the Philippines and Indonesia. Where the Philippines has an independent supervisory authority while Indonesia does not, although the Personal Data Protection Law provides for its establishment. Court decisions and judges' reasoning on private data cases in the two countries are also known, as well as the mechanisms for resolving private data theft disputes in Indonesia and the Philippines. It should be noted that in Indonesia, the Personal Data Protection Law will only come into full effect in October 2024.

Amiludin@umt.ac.id

Therefore, currently used the electronic information and transaction law is still reference.

Applications of this study : This study compares regulations in Indonesia and the Philippines about private data protection, especially the establishment of an independent watchdog agency, which is important to establish in Indonesia. It is also noted that court decisions and judges' reasoning regarding personal data cases in Indonesia are still used by the information and electronic transactions law. This is because, in October 2024 it will fully take effect. Whereas in the Philippines the law is already in active force. Then, the case resolution mechanism through Alternative Dispute Resolution can be taken into consideration in eliminating practices that tend to be slow, not simple, and expensive and stopping corrupt practices in the courts so that the Indonesian people feel safe and protected.

Novelty/ Orginalty of this study : No specific research has been found comparing the private data protection regulations in Indonesia and the Philippines such as the establishment of an independent watchdog agency to assist law enforcement officials in finding the perpetrators of private data theft, educating and answering questions about private data to the public. Furthermore, court decisions and judges' considerations regarding private data cases in Indonesia still refer by the information and electronic transactions law. This is because it will only come into full effect in October 2024. Unlike in the Philippines where the law is already in effect. In addition, the resolution of private data cases through alternative dispute resolution is considered superior to going through the courts because there are often slow, simplistic, expensive and corrupt practices that can reduce or even eliminate the trust of the Indonesian people in law enforcement officials.

Keywords: *Data, Data protection, Legal protection.*

ABSTRAK

Tujuan : *Untuk membandingkan peraturan perlindungan data pribadi di Indonesia dan Filipina, mengetahui putusan pengadilan dan pertimbangan hakim terhadap kasus data pribadi di kedua negara tersebut, serta mengetahui mekanisme penyelesaian sengketa terkait kasus data pribadi di kedua negara tersebut.*

Metodologi : *Digunakan studi tinjauan pustaka yang berasal dari buku-buku dan jurnal atau artikel yang telah dipublikasikan..*

Temuan : *Hasil penelitian membandingkan peraturan perlindungan data pribadi di Filipina dan Indonesia, dimana Filipina mempunyai otoritas pengawas independen sementara Indonesia tidak, walaupun*

Undang-undang perlindungan data pribadi mengatur pembentukannya. Juga diketahui putusan pengadilan dan pertimbangan hakim terhadap kasus data pribadi di kedua negara tersebut, serta diketahui mekanisme penyelesaian sengketa pencurian data pribadi di Indonesia dan Filipina. Perlu dicatat bahwa di Indonesia, regulasi Perlindungan Data Pribadi baru akan mulai berlaku sepenuhnya pada oktober 2024. Oleh karena itu, saat ini undang-undang informasi dan transaksi elektronik masih digunakan sebagai acuan.

Kegunaan : *Studi ini membandingkan peraturan perlindungan data pribadi di Indonesia dan Filipina terutama pembentukan lembaga pengawas independen yang penting untuk dibentuk di Indonesia, juga diketahui bahwa putusan pengadilan dan pertimbangan hakim mengenai kasus data pribadi masih digunakan undang-undang informasi dan transaksi elektronik sebagai acuan. Ini karena, pada Oktober 2024 sepenuhnya akan berlaku. Sedangkan di Filipina undang-undangnya sudah berlaku aktif. Kemudian, mekanisme penyelesaian kasus melalui Alternatif Penyelesaian Sengketa dapat dijadikan pertimbangan dalam menghilangkan praktik-praktik yang cenderung lambat, tidak sederhana, dan mahal serta menghentikan praktik-praktik koruptif di pengadilan agar masyarakat Indonesia merasa aman dan terlindungi.*

Kebaruan/Orisinalitas : *Belum ditemukan penelitian yang spesifik membandingkan regulasi Perlindungan Data Pribadi di Indonesia dan Filipina seperti pembentukan lembaga pengawas independen agar membantu aparat penegak hukum dalam menemukan siapa pelaku pencurian data pribadi, memberi edukasi dan menjawab pertanyaan seputar data pribadi kepada masyarakat, kemudian putusan pengadilan dan pertimbangan hakim mengenai kasus data pribadi masih digunakan Undang-undang Informasi dan Transaksi Elektronik sebagai acuan. Ini karena, pada Oktober 2024 sepenuhnya akan berlaku. Berbeda dengan di Filipina yang undang-undangnya sudah berlaku aktif. Selain itu, penyelesaian kasus pencurian data pribadi melalui alternatif penyelesaian sengketa dinilai lebih unggul dibandingkan melalui jalur pengadilan karena sering terjadi praktik-praktik yang lambat, tidak sederhana, mahal dan koruptif yang dapat mengurangi atau bahkan menghilangkan kepercayaan masyarakat Indonesia terhadap aparat penegak hukum.*

Keywords: *Data, Perlindungan data, Perlindungan hukum.*

INTRODUCTION

The growing era followed by rapid technological advances like today makes accessing anything via the internet easier, assisted by electronic devices such as cellphones, computers, laptops, and others that are supported by a good network (Meliala, 2015). Increasingly sophisticated technology makes small data can be easily transferred to devices and applications such as email, websites, and others, making it easier for humans to access other people's private data. Advanced information technology creates a relationship between individuals and data controllers (Dewi, 2016). private data that is stored, processed and collected and sorted according to its type needs to provide clarity to the data owner about what the data is used for (Aliu, 2019). A worrying possibility is that the data can be misused by hackers or the company that stores it to be sold secretly to other parties for profit (Bunga, 2019). This is difficult to avoid because the increase in internet users in the world has an impact on private data security. This is due to free access by individuals, government agencies, and parties who misuse data or hackers.

The sophistication of hackers in stealing other people's private data always follows the times (Maskun et al., 2020). So that it can easily hack into the country's security system. Subsequently, Indonesia genuinely must have a regulation that expressly manages the private data. Many parties will exploit data without regulation (Prabowo et al., 2020). Data is closely related to online trust as a cornerstone of security; if misused, users can suffer financial losses that threaten their safety and security (Rosadi & Pratama, 2018). In Indonesia, for example, there is an online loan case in ruling no. 438/Pid.Sus/2020/PN.JKT.UTR ensnared a debt collector as a suspect. In its verdict, the North Jakarta District Court stated that the suspect DS was sentenced to one year and a half year and an auxiliary fine of Rp 100,000,000, - or three months imprisonment. In this decision, there is also injustice in it, because there is a party, namely his superior named T, who is the deputy director of the company, who did not receive criminal sanctions for his actions (Prasetio, 2020). In addition, the rise of online crime that occurs uses more sophisticated methods so that it seems that it does not leave evidence (Susanto et al., 2017). In the Philippines, for example, there was discussed in NPC decision 21-086. The plaintiff, RTB, filed a complaint with the National Privacy Commission (NPC) alleging that East West Banking Corporation (EWBC) had unlawfully handled and unveiled its confidential data to an outsider assortment organization. After reviewing the complaint, the NPC decided to dismiss RTB's complaint against EWBC after concluding it was done under legitimate criteria. As a result of EWBC's negligence, NPC awarded RTB a compensation (privacy.gov.ph). Until now, no case of personal data has reached the Supreme Court, as only Supreme Court decisions are publicly accessible.

In accordance with the 1945 Constitution, Indonesia is a constitutional state that guarantees equality for all people under the law. Emphasizing that every individual has the right to acknowledgment, safeguard, security, regulatory certainty, and equivalent treatment under the steady gaze of the law. However, the public authority once in a while disregards the freedoms of its residents because of reasons of "public protection and security" (Nugraha,

2018). The presence of regulation is very important to control humans because it is binding so that humans are expected not to create chaos in the country. Law aims to maintain stability, security, justice, certainty, and usefulness in order to create a prosperous society (Mawardi, 2015). This goal can be realized if the government, law enforcement and the community have legal awareness. In addition, the law must adapt to the times, especially given the social conditions that continue to change due to technological advances (Atmasasmita, 2014). As a state of law, it is necessary to have a legal system because it is a combination of components that form a complex unit that has its own function and is connected into a system according to a pattern.

Different regulations in different countries based on their legal systems. Until now, Indonesia actually complies to the Continental European legal system, a Dutch heritage regulation that is closely related to the element of legal certainty realized by law enforcement. If a crime occurs, it can be processed criminally because there are laws that are regulated in writing. This system consists of statutes, and customs. Dissimilar to the Philippines, which complies to a mix of the Common Law and Civil Law legal system. The Common Law legal system is constitutional law, procedure, taxation, and more. Conversely, the Civil Law legal system covers succession, property rights, family relations, and more.

Although law aims to maintain stability, security, justice, certainty, and usefulness. However, legal issues in this digital era are often problematic regarding private data security. One of the state's efforts to protect private data is to make regulations on private data protection (Putri et al., 2021). The conversation of the Personal Data Protection Law (PDP Law) began because unrest over violations felt by individuals, companies, or related organizations which would certainly cause both material and non-material losses (Djafar, 2017). However, the above laws do not explicitly regulate private data, so the PDP Law was passed which is a standardization that can be applied in various sectors that can follow the characteristics of the industry to guarantee and protect the basic rights of citizens to private protection, ensuring that people receive services from corporations, public bodies, International Organizations, governments, and others. This regulation is made to protect human rights as the basis of individual privacy that can identify the owner (Priscyllia, 2019). In Indonesia, there is a need for digital literacy education so that no private data is misused (Djafar, 2019).

Meanwhile, in the Philippines, the Data Privacy Act of 2012 (DPA) enacted to conserve human rights, serving as the foundation for individual privacy. In addition, the above has become the duty of an independent oversight institution called the National Privacy Commission. The public can use the various platforms provided by this institution if they have questions about private data issues that are being experienced. In addition, this institution can assist law enforcement in addressing issues related to private data leaks. Independent supervisory institutions in Indonesia have been regulated in the PDP Law to establish supervisory institutions for data control and processing. However, the law only contains more in-depth content regarding the watchdog agency as there are no rules regarding its institutional structure, position, and authority.

Therefore, Indonesia needs to follow the example of the Philippines by establishing an independent oversight institution so that there is no intervention from any party. Moreover, this law applies to individuals and public bodies in various sectors (Khansa, 2021). If there is no supervisory institution, it is feared that in the future it will not be easy if it only relies on the Ministry of Communication and Information. Private data collected is also stored in extensive data systems need the government's attention by providing assurance and certainty that the data is protected and ensuring that cases of private data leakage such as those that occurred in 2021 and 2022 do not occur again. The following is the anomalous traffic of cyber attacks in Indonesia in 2021 and 2022 sourced from the Annual Report of the National Cyber and Encryption Agency (BSSN) "cybersecurity monitoring" (cloud.bssn):

Figure 1. Chart of Private Data Cases in Indonesia
Source : (cloud.bssn)

Anomalous traffic in 2022 dropped significantly by 40% compared to the previous year. Meanwhile, in the Philippines, based on 2021 and 2022 data sourced from the National Computer Emergency Response Team (ncert.gov.ph):

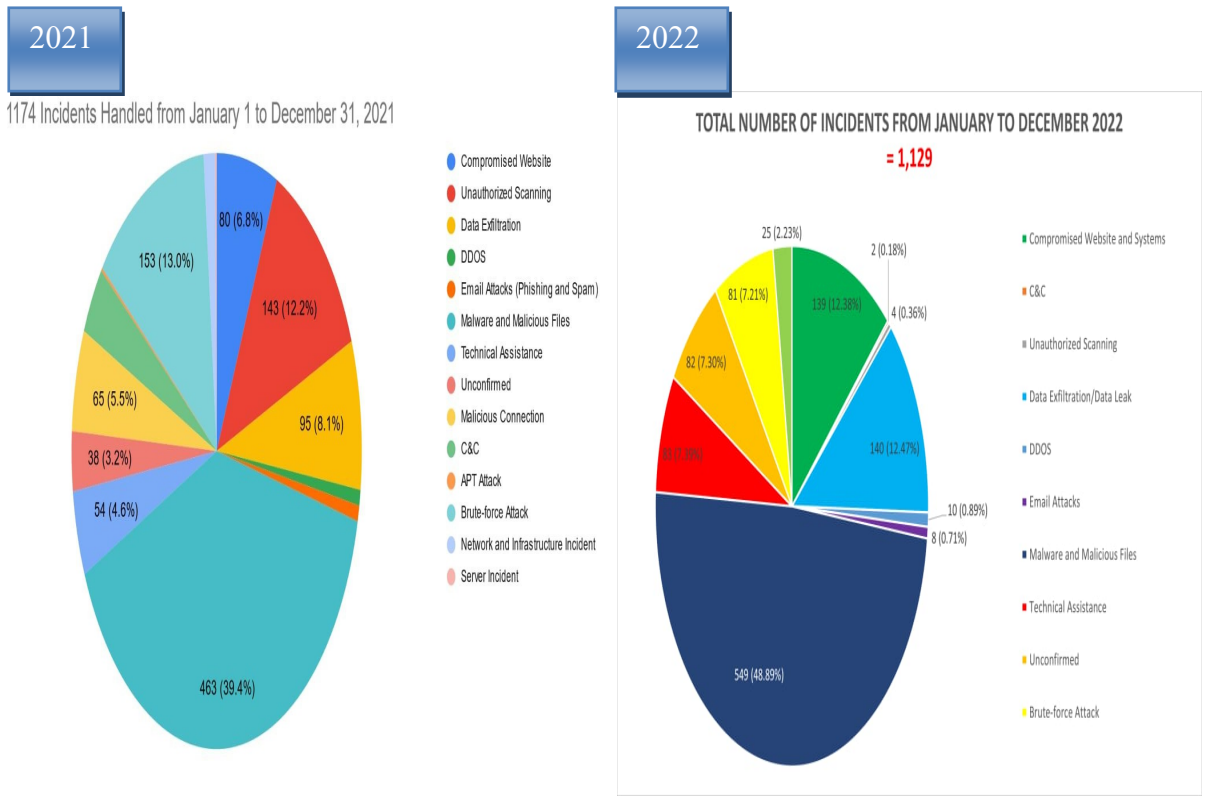

Figure 2. Chart of Private Data Cases in Philippines
Source : (ncert.gov.ph)

As we can see above, the number of cases in Indonesia has decreased, just like in the Philippines where it has also decreased, but by 45% in the Philippines. Previously, in Indonesia the Electronic Information and Transaction Law (ITE Law) has regulated to protection private data. However, the ITE Law needs to regulate specifically. As a result, the government created the PDP Law.

RESEARCH METHOD

The research method used is a literature review study taken from various references, such as journals or articles that have been published that are searched through electronic databases such as Google Scholar using keywords: data, data protection, and legal protection. As well as take data related to private data leaks taken from the official website of the National Cyber and Encryption Agency and the National Computer Emergency Response Team in 2021-2022.

RESULTS &DISCUSSION

A. Comparison of the Private Data Protection Act In Indonesia and The Philippines

As mentioned earlier, private data must be protected, but do you know what private data is? and why it matters so much to us? There are several definitions regarding private data, as follows :

1. Jerry Kang defines private data as information closely associated with individuals and can be differentiated based on their characteristics.
2. According to Purwanto, data is a collection of information that is interpreted as a set of symbols that describe numbers, objects, actions, and so on in the form of letters, numbers, or sure signs.
3. According to the regulation of the minister, private data is data that is maintained, stored, and protected because it contains a person's original information content that can be distinguished according to its characteristics so that related parties try to keep it to themselves or limit other parties from spreading it to anyone and abusing it (Rosadi, 2015).

So that explains private data; why is it so influential? Cause to achieve satisfaction or profit, for example, used to bully someone through social media, deceive someone by using someone else's identity to be sent some money until the victim is killed, defamed, and so on. Therefore, private data is very important to be stored, maintained, and maintained its authenticity and protected both by individuals and data controllers to be safe from unexpected parties (Gutwirth et al., 2015). So, private data is essential to be stored, maintained, and maintained its authenticity and protected both by individuals and data controllers. In Indonesia, special regulations governing private data, namely the Personal Data Protection Law (PDP law). Protection, which means how to use, disclose, and share data legally with related parties so that if data is exchanged but there is no legal basis to regulate it, it is considered invalid.

The PDP law is guided in European General Data Protection Regulation (GDPR). Discuss collection, using, sharing, and disclosing data, addressing aspects such as data quality, accuracy, and data subjects. There are three things in this law include data subjects which themselves are attached to private data, such as people or corporations, data controllers consisting of individuals, public bodies, international organizations, then the data processor processes private data in the name of private data controllers with the condition that a data must be kept confidential. A data owner has the right to know what his data is used for and sue and receive compensation in case of violations when processing data, except for law enforcement and national defense and security.

Data is grouped into General and specific data in the PDP law. General data encompasses complete details such as full name, gender, amalgamated private information for individual identification and etc. Conversely, specific data comprises biometric data, genetic data, crime records, information about children, private financial data, and other data stipulated by legal provisions. Another example is a photo; a photo

is not specific data but can be particular data if a picture is used for authentication. So far, the Ministry of Communications and Information Technology receives data breaches mainly related to negligence or vulnerabilities in the information security aspects of electronic systems. In case of a data leak, the processor must inform the data owner in writing within 3 x 24 hours, which contains information about the type of private data leaked, the time and mechanism of the leak, and efforts to overcome or recover from data leak.

In the Philippines, private data can be defined as human aspiration in controlling or influencing information about themselves in an effort to protect private information that comes from the wishes of individuals and is recognized by democratic societies (Romanou, 2017). Therefore, the government ought to communicate the methods it employs to fulfill the desires of its citizens regarding their private data. Furthermore, the commission's decisions and resolutions play a crucial role in interpreting and enforcing these regulations.

The commission issued a circular to fill in the details, supplement the DPA provisions, or provide the means to implement the act. It provides advice to guide interpreting the law about specific data privacy matters. The commission issues advisory opinions through its advisory functions. The circular complements the DPA provisions and the IRR to strengthen private data protection. Data privacy includes all types of private information, such as private, sensitive, and privileged information. Private information is a data subject that refers to the information holder. Private information includes name, occupation, bank account number, transaction history, last known address of former employee, email, signature, and others. Sensitive private information includes information that, when processed, results in a higher potential risk to data subjects and the increased protection necessary to prevent such danger. Privileged information is data that arises from confidential communications based on court rules and other relevant laws.

The purpose of processing private data is as follows:

a. Scientific and statistical research is subject to applicable ethical and legal standards and processes.
b. Investigations are carried out by authorized persons/bodies according to laws and regulations concerning criminal, administrative, tax, and other provisions.
c. National security interests.

In the Philippines, it enacted laws to regulate private data and established an independent regulatory body called the National Privacy Commission (NPC) to protect private data. The NPC is in charge of regulating and implementing the provisions of Private data protection regulations and complying with its international standards. The NPC approach to providing education and literacy to the public is to increase awareness of data protection laws by providing education and literacy through online platforms that can make it easier for people to access information (Hasan et al.,) such as the official

website of the National Privacy Commission and social media, Facebook (@privacy.gov.ph), Twitter (@privacyphp), and the AI chatbot feature on the National Privacy Commission's website is "AskPriva."In addition to providing education and literacy, the platform facilitates questions related to Data privacy laws.

In contrast, in Indonesia, which does not yet have a supervisory institution for Private data protection, a supervisory institution should be established according to the mandate of the PDP Law. If there isn't supervisory agency, it is feared that it will be difficult. The president is responsible for establishing an autonomous supervisory body accountable directly to them, and must be free from any influence of private interests and groups, with the existence of a private data protection supervisory institution is expected to help the public not to become victims. The supervisory board for the protection of private data when it has been established will have the following tasks (hukum online):

a. Supervise the implementation of private data protection.
b. Enforce administrative Law measures to address infringements
c. Facilitate alternative dispute resolution outside the formal judicial process.

B. Court Decisions and Judges' Considerations in Private Data Cases in Indonesia and the Philippines

Litigation involves judges who, according to Cik Hasan Bisri etymologically, are the one who decide the law (Isnantiana, 2017). In addressing incidents of private data breaches, law enforcement is crucial to maintain legal compliance and prevent further breaches (Ngape, 2018). In delivering judgments, judges bear great responsibility not only to humans but also to God Almighty (Asshidiqie, 2014). Therefore, the challenge faced lies in the ability to adapt given the ongoing social dynamics alongside technological advancements (Atmasasmita, 2014).

When giving a decision in a case, the judge's contains reasons and considerations and from these considerations, one can recognize the motivation, namely to give legal certainty and justice to all engaged involved in a legal dispute. Judges must be fully engaged in exploring and achieving legal justice in every trial, not just mechanically applying the law. In a progressive legal framework, judges can challenge norms by interpreting legal texts through hermeneutics to explore the values of justice, especially in the context of laws. Therefore, judges must fully utilize their intellect, wisdom, and humanism in court to decide a case with full justice (Lesmana, 2020).

As law enforcers, judges must have an understanding of the legal regulations and values that apply in society, and use reasoning in decision making. This is important because judges are seen as those who understand all laws, so the court cannot refuse to examine and hear cases (Harahap, 2016). Reasoning is an attempt to reach the truth through the use of reason or logical thinking, which is used by judges to think logically and give consideration to the truth or error of a matter. Law enforcers need good legal reasoning skills to formulate legal arguments. (Qodri, 2019). Legal reasoning is the

process of finding the basic principles underlying a judge's ruling in a legal matter, the manner in which an attorney employs legal arguments, and the approach through which a legal expert comprehends the law (Vera & Ainudin, 2016). Therefore, a judge must have good skills and abilities in understanding legal reasoning.

It is important for a judge to have an adequate understanding of legal reasoning as this plays a crucial role in drawing up legal considerations when making decisions. In Indonesia, courts in making decisions and passing judgments are based on considerations that are in accordance with the right reasons and regulations. Therefore, judges are expected to act wisely because court decisions are complex matters (Pamungkas, 2021). The judge should focus on the essence of the verdict, namely whether the consideration can be burdensome or mitigating the crime because sufficient consideration cannot be made of legal remedies. In the Philippines, courts generally make decisions based on evidence, and such decisions are not seen as biased against just one sector. Generally, courts make decisions based on the evidence presented, yet there's a perspective suggesting that courts might show partiality toward affluent and influential individuals (Panao & Leon, 2018). Also rely on evidence, while complying with the Constitution and other regulations that support the principles of social justice, human rights, and gender equality (Tetch, 2019). Judges need to uphold equilibrium in society by reinstating the social order to its initial condition (Djanggih, 2018).

The PDP Law is set to be fully enforced starting from October 2024, while currently still using the ITE Law while currently still using the ITE Law to regulate cybercrime (Sutrisno & Paksa, 2019). For example, in the ruling no. 438/Pid. Sus/2020 / PN.JKT.UTR this is a case in which a person is sentenced for violating the rules on data transfer. The defendant, who worked as a debt collector in an online loan company, was involved in a case where the victim felt aggrieved by the defendant's actions. The victim, who was a debtor in one online loan, was pressured in an inappropriate manner by the defendant. These include verbal intimidation with harsh words, threats via text messages, and threats to disclose information about the debts owed to the victim's family and close people if they do not fulfill the defendant's wishes. In this case, the defendant was sentenced for one year and six months. The punishment is given because the defendant has been proven to be legally in violation of the law as outlined in Article 45 paragraph (4) Jo. Article 27 paragraph (4) of Law No. 19 of 2016 amending Law No. 11 of 2008 concerning ITE Law. Here is the verdict:

ORDERED

1. Stating that the Defendant DEDE SUPARDI Bin H. SUPRIADI has been legally and convincingly proven guilty of committing the crime of "intentionally and without the right to distribute and/or transmit and/or make accessible Electronic Information and/or Electronic Documents that contain extortion and/or threats" as in the second indictment;

2. Sentenced to the Defendant DEDE SUPARDI Bin H. SUPRIADI therefore with imprisonment for: 1 (one) year and fine in the amount of Rp.70,000,000.00 (seventy million rupiah) provided that if the fine is not paid, it shall be substituted with confinement for 2 (two) months;
3. Determining that the period of arrest and detention that has been served by the Defendant shall be fully deducted from the punishment imposed;
4. Determine that the Defendant remains in custody;
5. Determine the evidence in the form of: - 1 (one) unit of cellphone Redmi 7 3/32 black color (confiscated from Bayu Prasetya); Used in another case; - 1 (one) unit of cellphone Realme red blue color No. 081546121647 (confiscated from Dede Supardi Bin H. Supriadi); - 1 (one) curriculum vitae (confiscated from Dede Supardi Bin H. Supriadi); Confiscated for destruction;
6. Charged the Defendant with paying court costs in the amount of Rp5,000.00 (five thousand rupiah);

Thus decided in a deliberation session of the Panel of Judges of the North Jakarta District Court, on Tuesday, June 9, 2020, by Agung Purbantoro, S.H., M.H. as Chief Judge, Drs. Tugiyanto, Bc.I.P., S.H., M.H., and Fahzal Hendri, S.H., M.H., each as Member Judges, which was pronounced in a hearing open to the public on the same day by the Presiding Judge accompanied by the aforementioned Member Judges, assisted by Ari Palti Siregar, S.T., S.H., M.H., Substitute Registrar at the North Jakarta District Court, and attended by Erma Octora, S.H. Public Prosecutor and Defendant.

In this case, the judge still referred to the ITE Law as the basis for his consideration. In its ruling, the judge ensured that all elements of the alleged violation of the ITE Law were met, in particular with regard to the private data violation. On this occasion, the author seeks to investigate aspects of private data protection in Indonesia regulates the transfer of private data of a person who must obtain the relevant permission. Violation of this provision may result in the data owner filing a claim for damages in court, but difficulties in proving cases in civil courts in Indonesia hamper the ability of data owners to legitimately highlight breaches in the security of their private data. The PDP Law allows the resolution of disputes related to the protection of private data through civil courts and alternative dispute resolution mechanisms like arbitration (Article 64). This finding is an important note for all of us. Independent supervisory authorities have an important role as a mechanism for societal oversight of governmental authority and can safeguard private data for the sake of legal progress (Sukmariningsih, 2014).

In the Philippines, private data cases are handled and decided by the National Privacy Commission (NPC) whose information can be accessed through its official website. To date, no case of private data has reached the Supreme Court, since only decisions of the Supreme Court are accessible to the public. For example, in the NPC ruling 21-086. This was a case where the complainant, RTB, had previously taken out a

car loan secured by a mortgage pledge with the Philippine Bank of Communications (PBComm), and then transferred the loan and mortgage to the East West Banking Corporation (EWBC). Next provided EWBC with several dated checks to repay the loans granted, but because EWBC personnel failed to deposit the checks, the complainant's account was marked as overdue resulting in a referral to a collection agency. So that the complainant received a bad phone call that was misleading and tried to take the car. Accordingly, the complainant filed a complaint with the NPC, claiming that EWBC process also disclosed his private information to a third-party collection agency in an unauthorized manner.

Discussion

1. The Commission resolves to close the case.
2. The Commission notes that EWBC complied with the order to pay RTB nominal damages in the amount of Fifteen Thousand Pesos (P15,000.00) as stated in the Decision dated 03 February 2022. The acknowledgement receipt signed by RTB together with RTB's confirmation of the payment of nominal damages through his email to the Commission are deemed sufficient to prove that the payment has been made.
3. As regards RTB's statement in his email that he intends to file a Motion for Reconsideration, the Commission notes that he did not file a Motion for Reconsideration within the prescribed period under NPC Circular 2021-01 (2021 NPC Rules of Procedure).

WHEREFORE, premises considered, Commission resolves that NPC 21-086 – RTB v. East West Banking Corporation is hereby CLOSED. Further, East West Banking Corporation's Compliance and Manifestation (Re: Letter/Order dated 25 April 2022 and Decision dated 03 February 2022) dated 02 May 2022 is hereby NOTED.

After reviewing the complaint, the NPC based on Section 12(b) of the DPA decides to reject that, after determining that EWBC processes RTB's private information within the legitimate criteria. As a result of EWBC negligence, the NPC compensated RTB. In this context, EWBC does not comply with its responsibilities as a controller of private information based on Section 11 (c) of the DPA. The commission noted that EWBC had complied with RTB's indemnity payment. The payment was deemed to have been made based on the confirmation of payment of the nominal compensation, accompanied by RTB's signature of receipt, emailed to the commission. Despite RTB's intention for reconsideration in the email, RTB did not do so by the deadline set by the commission in NPC Circular 2021-01. Therefore, based on these considerations, the Commission decided to close the case. (privacy.gov.ph).

As the Personal Information Controller (PIC), EWBC must keep the data subject's personal information up to date as a form of accountability. EWBC is supposed to check the date of deposit of the check that has passed the date given by the complainant. Accidental failure to deposit a check past the specified date causes the

complainant's personal information to unnecessarily be revealed to third-party collection agency. EWBC violated the KPR terms and conditions of the mortgage in collecting the debt by not giving prior written notice to the complainant. EWBC proved to be grossly negligent in carrying out the obligations given by the banking institution. If EWBC had fulfilled its obligations in accordance with the loan contract and DPA, then EWBC would not have needed to disclose the complainant's private information. Nevertheless, EWBC recklessness was not enough to propose prosecution. Although the processing carried out by EWBC has a valid legal basis, EWBC is still liable for nominal losses.

C. Theft Private Data Dispute Resolution Mechanism in Indonesia and The Philippines

In the digital age, numerous challenges are associated with the security of private data especially in Indonesia and the Philippines. International law governs the safeguarding of private data as outlined below:

1. Universal Declaration of Human Rights (UDHR)

It marks the inaugural instrument upholding an human right to privacy, the term "privacy" is regarded as a comprehensive term, encompassing the safeguarding of a range of additional rights, including family, honor, reputation and others. As time has progressed, additional dimensions of protection have emerged, covering physical privacy, dignity, privacy deciding, and privacy of information. This evolution emphasizes the necessity for regulations concerning the privacy of private data.

2. International Covenant on Civil and Political Rights (ICCPR)

Doesn’t clearly mention that the right to privacy encompasses private data. Nonetheless (Kuner, 2014) offers a comprehensive right to privacy from guidelines that explain the extent, and it is said that the purpose of getting protection in human private life is that everyone needs to have the right to make sure a form can be understood and what kind of private data is in automatic data files. Everyone needs to know and check individuals or public/private bodies related to whether their data is wrong or has been collected/processed against the law. Hence, everyone should possess the entitlement to seek the removal of their data. Connected to the aforementioned discussion, it is evident that private data is intricately linked to the right to privacy, necessitating safeguarding.

3. European Convention on Human Rights (ECHR)

The Council of Europe, functioning; regional international organization, possesses an agreement concerning the privacy, particularly detailed in Article 8 ECHR. This article became foundation for the establishment of an additional convention that specifically delves into the safeguarding of private data. After being signed by representatives of member states in 1981, this convention was enforced in 1985 following the requisite ratifications from several countries (Themba, 2016).

Regarding the things that have been described above, it proves that protecting private data is very important because it is part of individual life, has a great complexity and amount and can make others know something about ourselves (Riahi et al., 2015) such as data leakage such as name and the Population Identification Number (NIK). This information can be used by hackers. Hackers are always up to date with technology; therefore, they always find a way to exploit vulnerabilities on the websites of companies/government agencies to determine whether the stolen private data is then sold to the detriment of a particular company or out of political motives. There are two forms of private data protection, including physical security of both visible and invisible data, and regulations that govern the unauthorized use of data, data misuse for specific purposes, and damage to the data itself (Sautunnida, 2018). Disputing parties have several considerations in choosing the appropriate mechanism to resolve conflicts, including legal system components that will influence their choices.

The dispute resolution mechanism for private data security in Indonesia and the Philippines differs. In Indonesia, if there is an indication of a private data leak, it can take general steps first. If a private data leak is detected, it must be responded to quickly; for example, companies or organizations that experience such incidents need to immediately identify and confirm private data leaks by checking systems and networks to determine the source and scale of the leak. Second, if it is confirmed that there is a data leak, then access to the affected system must be disconnected first, then repair the security gaps that allow attacks and restore damaged or lost data. Third, ask for the help of a computer security team or forensic company to find out who the culprit is and the motive behind it. To find out carried out Forensic investigation is carried out that involves analyzing logs, digital traces, and other investigative techniques. Fourth, the information and evidence collected during the investigation are submitted to the National Cyber and Encryption Agency (BSSN) or the police to be processed legally. Fifth, if the case has been resolved, the affected organization or company needs to implement measures such as training employees, improving network security, conducting periodic security audits, and updating software. Sixth, evaluate and monitor the security system regularly because this can help determine the existence of potential threats and new weaknesses that may arise.

In addition, the PDP law if we see in Article 64, paragraphs 1 and 2 concluded dispute resolution is done in court or alternatively through institutions with statutory provisions, see the principle of lex specialis, that procedural law is used to resolve disputes. The trial process can be carried out behind closed doors to protect private data. In Indonesia, safeguarding private data is imperative as it constitutes one of the fundamental human rights. They protect private privacy, and there should be a legal basis that can guarantee the rights of citizens by regulating the protection of private data. Data subjects who experience losses due to data leakage are entitled to receive compensation by filing a civil lawsuit. As for an alternative dispute resolution as stated in law number 30 of 1999 in Article 6, which regulates that if the dispute is resolved by

non-litigation based on the good faith of the parties, it is carried out by meeting directly within 14 days. Then, an agreement that has been successfully reached is made in writing.

However, if it does not work out, the parties can seek the help of a mediator or expert advisor. If, within a period of 14 days, the parties have sought the assistance of a mediator or expert advisor but have not reached an agreement, the disputing parties may request an alternative dispute resolution institution or arbitration institution to appoint a mediator to initiate mediation involving a third party, with a deadline of 7 days (Rezki, 2019). While carrying out its responsibilities, the mediator should possess the capability to maintain confidentiality, and a written agreement, endorsed by the concerned disputing parties, must be reached within a 30-day period. In addition, the outcome of the agreement is recorded within 30 days at the court from the date of ratification by the parties to the dispute. Nevertheless, these initiatives may not bring about a resolution to the dispute. In such instances, the disputing parties have the option to pursue dispute resolution through an arbitration institution or ad hoc arbitration, contingent upon a documented agreement.

Resolution of disputes through arbitration depends on written agreements between the parties engaged in disputes outside the General Court. Arbitrators, designated by either the parties, the district court, or an arbitration institution, are tasked with making a decision on the dispute that arises; the outcome is a win-lose decision, is final, and has the force of law binding on all parties involved. Anyone can voluntarily resolve private data leakage disputes through out-of-court dispute resolution. The parties to the dispute may choose according to their needs, such as negotiation, mediation, conciliation, arbitration, or other options based on their agreement in dispute. Then, if this effort is successful, the results of the written agreement shall be final and binding on the parties unless otherwise provided by law. However, the parties may dispute with the court when the above attempts are unsuccessful.

Unlike in Indonesia, in the Philippines, the general step that must be taken when there is an indication of private data leakage is first, the individual company or organization concerned determines what violation occurred, for example, whether there is unauthorized use of private data, unauthorized access, and others. Second, gather all available evidence, e.g., screenshots and copies of documents, to support our statement. Third, report violations that occur and submit all evidence to the National Privacy Commission (NPC) so that it can take appropriate steps to resolve the problem. Fourth, we can also contact the police or the court so that they can take investigative steps and take legal action if necessary. Fifth, ask for the help of lawyers experienced in privacy law and data protection because we can be given the right solution and assisted in resolving the case. In the Philippines, it was resolving disputes primarily through the judicial system. However, the large number of cases that went to court caused the file to become clogged due to limited resources in responding to the increase in cases. Hence, the judicial process seemed protracted and expensive.

Therefore, an alternative dispute resolution or ADR emerges, which refers to other dispute resolutions that include alternatives to litigation (Blake et al., 2021). Alternative dispute resolution is considered an intervention against the accumulation of case files. Consequently, this alternative dispute resolution should be considered based on its superiority as an effective system to resolve disputes more quickly and efficiently, with lower costs. The Alternative Dispute Resolution Act of 2004 was established by the Philippine government. Alternative dispute resolution mechanisms in the Philippines include mediation, conciliation, and arbitration. Although mediation and conciliation are two different things, they are used interchangeably in the Philippines. Thus, in this case, the third party facilitates the negotiation with two or more parties to the dispute. When facilitating it, third parties help to provide the best solution to benefit the parties to the debate. The agreement can be reached because the mediator orders the parties concerned to express all their views on a condition until they understand each other about the problems that occur. The role of a mediator in a successful negotiation lies with the parties to the dispute because the negotiation results are in their hands. In carrying out its duties, the mediator must ensure that the negotiation process can run effectively, systematically, and fairly.

It distinguishes itself from arbitration as it involves a third party that assesses the information presented by the disputing parties and examines the case. Then arbitration is the one that gives the decision on how to resolve the dispute and often assesses who is the proper party among the other parties to the dispute. In contrast to mediation, the third party is a facilitator only, and the parties to the dispute decide the final solution to the disputed problem.

There are advantages if you resolve a dispute out of court rather than through the courts:

a. The settlement is private so that outsiders do not know the company's kitchen, so the company's reputation is well preserved, and the verdict results are not published.
b. The settlement is faster than through the court because the provisions regarding the time limit, the selection of arbitrators, and Law resolution of disputes agreed by the parties submitted by themselves are made relatively quickly and flexibly.
c. It realizes the results of a win-win dispute resolution with the hope that in the future, it is not placed as a losing or disadvantaged party despite the conflict between the parties.

Therefore, this alternative settlement can keep the business relationship in the future. Of course, some advantages of the Alternative Dispute Resolution Mechanism are "contradictory" when compared with the settlement mechanism through the courts. Dispute resolution through the courts is closely related to practices that tend to be slow or not fast (takes a long time), not simple (complicated), and expensive. In addition, sometimes, the judicial world, in some cases, is full of corrupt practices.

CONCLUSION

Private Data is valuable data often misused by other parties to benefit, so private data must be stored, maintained, maintained authenticity, and protected by both individuals and data controllers. In Indonesia, the PDP Law, data is grouped; special and general data. Then in the Philippines, covers all types of private information and established a private data protection supervisory body called the National Privacy Commission to protect private data. In Indonesia, private data protection has no supervisory body, while the supervisory body is formed based on the PDP Law. If there is a regulatory body, it is likely accessible.

Judges in deciding a case contain reasons and considerations. Judges are not just mechanically applying the law but must use their full intellect, wisdom and humanism in court to decide a case with full justice. In Indonesia, personal data cases can be resolved through the courts. However, court decisions and judges' considerations regarding private data cases still refer to the ITE Law. This is because the PDP Law will only come into full effect in October 2024. Unlike in the Philippines, private data cases are handled and decided by the National Privacy Commission (NPC) whose information can be accessed through its official website. Until now, no case of personal data has reached the Supreme Court, as only Supreme Court decisions are publicly accessible.

The dispute resolution mechanism for private data security in Indonesia refers to Article 64, Regulating that in the event of a dispute, the settlement can be carried out through courts, arbitration, and alternatively, institutions. An alternative dispute resolution regulation can be seen in Law No. 30 of 1999. If the dispute is resolved through the court, the proceedings can be conducted behind closed doors to protect private data. In the Philippines, they are resolving disputes primarily through the judicial system. However, the large number of cases that go to court causes the case file to become clogged due to limited resources in responding to the increase in cases, Therefore, the implementation of alternative dispute resolution in the Philippines was initiated by introduction of the Alternative Dispute Resolution Act of 2004 by the Philippine government.

REFERENCES

Aliu, B. (2019). Big data phenomenon in banking. *Texila International Journal of Academic Research*, *6*(2), 81–87. https://doi.org/10.21522/tijar.2014.06.02.art008

Asshidiqie, J. (2014). *Peradilan Etika Dan Etika Konstitusi*. Jakarta: Sinar Grafika.

Atmasasmita, R. (2014), *Hukum Kejahatan Bisnis Teori dan Praktik di Era Globalisasi*. Jakarta: Prenadamedia Group.

Blake, S. H., Browne, J., & Sime, S. (2021). *A practical approach to alternative dispute resolution*. Oxford University Press.

Bunga, D. (2019). Politik Hukum Pidana Terhadap Penanggulangan Cybercrime. *Jurnal Legislasi Indonesia*, 16(1), 1-15. https://doi.org/10.35141/jyu.v1i1.100

Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi dikaitkan dengan Penggunaan Cloud Computing di Indonesia. *Yustisia*. 5 (1). https://doi.org/10.20961/yustisia.v5i1.8712

Djafar, W. (2019, Agustus). *"Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan". Seminar Hukum dalam Era Analisis Big Data*. Program Pasca Sarjana Fakultas Hukum UGM.

Djanggih, H. (2018). "Pertimbangan Hakim Dalam Perkara Pencemaran Nama Baik Melalui Media Sosial (Kajian Putusan Nomor: 324/Pid./2014/PN.SGM). *Jurnal Penelitian Hukum De Jure*. Vol.18 No.1: 96. https://doi.org/10.30641/dejure.2018.V18.93-102

Gutwirth, et al. (2015) Reforming European Data protection Law. *Springer, Dordrecht*, (p.16). https://doi.org/10.1007/978-94-017-9385-8

Harahap, Y. (2016). *Hukum Acara Perdata Tentang Gugatan, Persidangan, Penyitaan, Pembuktian Dan Putusan Pengadilan*. Jakarta: Sinar grafika.

Hasan, M.D.M., Popp, J., & Olah, J. (2020). " Current Landscape and Influence of Big data on Finance", *Journal of Big Data*, Edisi No. 21, Vol 7, Springer, (p. 8). https://doi.org/10.1186/s40537-020-00291-z

https://cloud.bssn.go.id/s/3S5B2ToddAFsiXs , accessed 29 July 2023

https://cloud.bssn.go.id/s/Lyw8E4LxwNiJoNw, accessed 29 July 2023

https://privacy.gov.ph/wp-content/uploads/2023/05/NPC-21-086-RTB-v.-East-West-Bank-Corporation-Resolution-Final.pdf, accessed 09April 2024

https://www.hukumonline.com/berita/a/tugas-tugas-lembaga-penyelenggara-pelindungan data-pribadi-dalam-uu-pdp-lt633e0a93602a2/, accessed 10 August 2023

https://www.ncert.gov.ph/statistics/, accessed 29 July 2023

Isnantiana, N.I. (2017). "Legal Reasoning Hakim Dalam Pengambilan Putusan Perkara Di Pengadilan,". *Jurnal Islamadina 18*, no. 2, 41–56. https://doi.org/10.30595/islamadina.v18i2.1920

Khansa, F.N. (2021). Penguatan Hukum dan Urgensi Otoritas Pengawasan Indepen Dalam Perlindungan Data Pribadi di Indonesia. *Jurnal Lex Generalis*, 2(8), 649-662. https://doi.org/10.56370/jhlg.v2i8.114

Kuner, C. (2014). "The European Union and the Search for an International Data Protection Framework". *Groningen Journal of International Law*. 2. 76. https://doi.org/10.21827/5a86a82b67dab

Lesmana, Y.E.M. (2020). "Modalitas Hakim Progresif,". *Verstek: Jurnal Hukum Acara 08*, no. 02. https://doi.org/10.20961/jv.v8i2.44116

Mawardi, D.R. (2015). "Fungsi Hukum Dalam Kehidupan Masyarakat". *Jurnal Masalah-Masalah Hukum*, Edisi No. 3 Vol. 44, Fakultas Hukum Universitas Diponegoro, 3. https://doi.org/10.14710/mmh.44.3.2015.275-283

Meliala, S.M. (2015). Analisis Yuridis Terhadap Legalitas Dokumen Elektronik Sebagai Alat Bukti Dalam Penyelesaiaan Sengketa. *Jurnal Wawasan Yuridika*, 32(1), 99-111. https://doi.org/10.25072/jwy.v32i1.92

Ngape, H.B.A. (2018). Akibat hukum putusan hakim yang menjatuhkan putusan di luar dakwaan penuntut umum. *Justitia Jurnal Hukum*, 2(1), 127-143. https://doi.org/10.30651/justitia.v2i1.1229

Nugraha, R.A. (2018). Perlindungan Data Pribadi dan Pribadi Penumpang Pada Era Big Data. *Mimbar Hukum Jurnal Universitas Gaja Mada*, Edisi No. 2 Vol. 30, Fakultas Hukum Universitas Gajah Mada, 3. https://doi.org/10.22146/jmh.30855

Pamungkas, A. (2021). "Dialektika Pertimbangan Hakim Perkara Tindak Pidana". *Jurnal Verstek*. Vol.2, No.2: 431

Panao, A.L. & Leon, B.X.D. (2018). "Balancing the Interests of Labor and Capital: An Empirical Analysis of Philippine Supreme Court Labor Cases from 1987 to 2016." *Philippine Political Science Journal 39 (1)*: 24–46. https://doi.org/10.1080/01154451.2018.1498606

Prabowo, W.H., Wibawa, S., & Azmi, F. (2020). "Perlindungan Data Private Siber di Indonesia,". *Padjadjaran Journal of International Relations.* 1 (3). 227. https://doi.org/10.24198/padjir.v1i3.26194

Priscyllia, F. (2019). "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum." *Jatiswara 34,* no. 3: 239-49. https://doi.org/10.29303/jtsw.v34i3.218

Putri, F., Destriani, D., & Fahrozi, M.H. (2021). "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)." *Borneo Law Review 5*, no. 1: 46-68. https://doi.org/10.35334/bolrev.v5i1.2014

Qodri, M. (2019). "Benang Merah' Penalaran Hukum, Argumentasi Hukum Dan Penegakan Hukum," *Jurnal Hukum Progresif 7*, no. 2: 182. https://doi.org/10.14710/hp.7.2.182-191

Rezki, A., Anggraeni, R.R., Dewi, Yunus, N.R. (2019). "Application of Civil LawTheory In the Termination of Custody of Adopted Children in Indonesia," *Journal of Legal Research, Volume 1, No. 6*. https://doi.org/10.15408/jlr.v1i6.15301

Riahi, et al. (2015). "Big Data and Big Data Analytics: Concepts, Types and Technology", *International Journal of Research and Engineering*, Edisi No. 9, Vol. 5, (p. 525). https://doi.org/10.21276/ijre.2018.5.9.5

Romanou, A. (2017). The necessity of the implementation of Privacy by Design insectors where data protection concerns arise. *Comput. Law Secur.* Rev. 1–12. https://doi.org/10.1016/j.clsr.2017.05.021

Rosadi, S.D. (2015). *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung: PT Refika Aditama.

Rosadi, S.D., & Pratama, G.G. (2018). "Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia", *Jurnal Veritas et Justitia*. 4 (1). 89. https://doi.org/10.25123/vej.2916

Sautunnida, L. (2018). "Urgensi Undang-undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia*", Kanun Jurnal Ilmu Hukum, Vol. 20, No.2*. https://doi.org/10.24815/kanun.v20i2.11159

Sukmariningsih, R.M. (2014). Penataan Lembaga Negara Mandiri dalam Struktur Ketatanaegaraan Indonesia. *MIMBAR HUKUM*, 26(2): 194-204. https://doi.org/10.22146/jmh.16039

Sutrisno, B., & Paksa, FX.B.B. (2019). "Penegakan Hukum Terhadap Tindak Pidana Pencemaran Nama Baik Menurut Pasal 27 Ayat (3) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE). *Mizan; Jurnal Ilmu Hukum*. Vol.8 No.1. https://doi.org/10.32503/mizan.v8i1.495

Tetch, T.T. (2019, August). *"Ati Tribe Wins Boracay Land Case vs Private Claimants."Philippine Daily Inquirer.* Retrieved from https://www.newsinfo.inquirer.net/1158638/ati-tribe-wins-boracay-land-case-vs-private-claimants

Vera, N.L.P, & Ainudin, N. (2016). "Logika Hukum Dan Terobosan Hukum Melalui Legal Reasoning,". *Jurnal Hukum Jatiswara 31*, no. 1: 99–110