Journal of Law and Legal Reform
Vol. 6 Issue 3 (2025) 1349–1376
DOI: https://doi.org/10.15294/jllr.v6i3.10252
Online since: July 31, 2025

Journal of Law & Legal Reform
https://journal.unnes.ac.id/journals/jllr

Personal Data Protection in Review of Legal Theories and Principles

Supeno Supeno [a] ✉, Rosmidah Rosmidah [b], Syed Mohd Uzair Iqbal [c]

[a] Faculty of Law, Universitas Batanghari, Indonesia
[b] Faculty of Law, Universitas Jambi, Indonesia
[c] Symbiosis Law School, India

✉ corresponding email: supeno@unbari.ac.id

Abstract

The abuse of personal data for certain interests and causing harm to other parties is often occur so that this raises concerns as a large community in conducting online transactions, in 2022 the President together with the Indonesian Parliament has enacted Law Number 27 of 2022 on Personal Data Protection (PDP) which aims to provide legal protection for the community against their personal data, this provides good hope to ward off various kinds of acts of misuse of personal data, the purpose of this study is to reveal the legal protection of customer data in online transactions after the legalization of personal data protection law seen from legal theory and how the personal data dispute resolution model is in line with the ultimum remidium principle. The type of research used is juridical-normative law using normative and theoretical approaches. The results showed that the protection of one's privacy rights in online transactions is an embodiment of absolute right theory because the protection of privacy rights is a basic right that everyone must respect, the utilization of one's privacy rights without the approval of the right owner is a violation of the law, the personal data dispute resolution model in the personal data protection law is not in following with the ultimum remidium principle, the personal data dispute by special organ with like such as the General Data Protection Regulation (GDPR) in the European Union, because it can resolve cross-border personal data cases.

Keywords
Personal, Data Protection, Theory, Principle, Special Organ.

Introduction

In 2022 the President together with the House of Representatives of the Republic of Indonesia have stipulated Law Number 27 of 2022 on Personal Data Protection (PDP),[1] as a law that aims to offer legal protection for the public to their right to privacy, The right to privacy concern is one of the rights inherent in everyone. The right to privacy is the dignity of every person that must be protected.[2] This provides hope to ward off various acts of misuse of personal data by responsible parties. Thus far, business actors or electronic system operators can accumulate personal data from customers or potential customers offline or online, where digital data can be traded without the knowledge and permission of the data owner.[3] Law Number 27 of 2022 on Personal Data Protection (PDP) is a legal effect of the attestation of four international conventions, namely the Universal Declaration on Human; Article 12; International Covenant on Civil and Political Rights: Article 17; Convention on the Rights of the Child: Article 16; dan International Convention on the Protection of All Migrant Workers and Members of Their Families: Article 14.

Personal data is facts about a person, whether known or not, alone or in combination with other information, directly or indirectly, by electronic systems or not. Personal data is something very essential for humans, personal data essentially includes all kinds of data belonging to a person, both physical data, health data, family data, data related to work, financial data, phone number data and so on, nowadays with the opening of facilities and communication through various electronic

---

1 "Data Base Jaringan Dokumentasi dan Informasi Hukum (JDIH)," JDIH Kementerian Sekretariat Negara, n.d.

2 Sekaring Ayumeida Kusnadi, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16, https://doi.org/10.47776/alwasath.v2i1.127.

3 Sahat Maruli Tua Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI* 27, no. 1 (March 25, 2021): 38, https://doi.org/10.47268/sasi.v27i1.394.

media opens up the widest possible opportunity to carry out activities, both individual activities and activities that are collective.

This activity includes 2 (two) types of activities, namely activities in the field of public services. In the current era of regional authonomy , it is necessary to realize good governance using information and communication technology, commonly called e-government. Through e-government, the improvement of public services can also be realized,[4] activities in the field of public services in the form of services provided by the government in carrying out public service functions such as Identity Card (KTP) management services, licensing services, health services at government hospitals, services at government-owned educational institutions, financial transaction services at government-owned institutions and so on, In contrast, activities in the private sector can include activities between private institutions and individuals in the field of employment relations, health services in private hospitals, educational services in private schools, financial services in privately owned financial institutions and so on, All components in e-Commerce refer to all aspects of e-commerce, such as customer service, product services, payment methods, and promotion methods.[5]

Almost all forms of these services use online service facilities, Examples that are rampant today are online, loan transaction that only a simple and easy application process,[6] In online services, transactions occur in the form of sending a person's personal data either through email, WhatsApp, special applications and so on, in this condition a person's personal data can be read and viewed by other parties either by individuals or by certain authorities to view and access a person's personal data. Business services involve transactions between traders,buyers, produccers and consummers, Variouse conveniences are found between service providers and service recipients, known as e-commerce, in e-

---

[4] Puji Ayu Lestari et al., "Digital-Based Public Service Innovation (E-Government) in the Covid-19 Pandemic Era," *Jurnal Ilmu Administrasi* 18, no. 2 (2021): 212–24, https://doi.org/10.31113/jia.v18i2.808.

[5] Maulidya Alffi Anita Zain et al., "E COMMERCE DALAM PENGEMBANGAN BISNIS: A BIBLIOMATRIK STUDY," *Hospitality* 11, no. 1 (2022): 335–46, https://doi.org/10.47492/jih.v11i1.1618.

[6] Supeno Supeno, "Legal Capacity in Online Loan Transactions (The Study on Legal Personal Liability Theory)," *Annals of Justice and Humanity (AJH)* 1, no. 2 (2022): 51–57, https://doi.org/10.35912/ajh.v1i2.1347.

commerce various kinds of conveniences are found, consumers convenience is as easy as clicking the mouse find various products. the company demands that efforts be made to create customer loyalty. In this stage, there is often a misuse of a person's personal data by other people or certain institutions, either aimed at making financial profits or not, which causes potential losses for the owner of personal data.

Several research results and legal scientific writings related to personal data can be presented as a form of illustration of the Junaidi, Pujiono and Roslinda Muhammed Fadzil in the conclusion of their research entitled Legal Reform of Artificial Integence's Liability to Personal Data Perspective of Progressive Legal Theory stated that Law Number 27 of 2022 requires of Government Regulation in Implementing Personal Data Protection, in edition there must be clear regulations regarding the right of data subject[7], emphasizing that there must be clear provisions on the rights of data subjects related to the use of intelligence artificial. Ririn Aswandi in his article entitled Protection of Data and Personal Information Through the Indonesia Data Protection System (IDPS) said that the problem related to the security of a person's data and information is that a person's personal data is usually directly provided by the data manager without the knowledge of the owner of the personal data, with the existence of this IDPS if a company or government agency wants to use data and a person's information must be reported in advance and have a period of no later than 60 minutes and no later than 3 x 24 hours to confirm, if the period has passed or the data owner ignores it, then the company and related agencies have the right to be provided with data accompanied by supervision.[8] IDPS is believed to be able to provide a solution for personal data protection, problem of the authority to use a person's personal data by official government agencies can be answered with this system, but if the user is a private and/or

---

[7] Junaidi Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil, "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspective of Progressive Legal Theory," *Journal of Law and Legal Reform* 5, no. 2 (2024): 587–612, https://doi.org/10.15294/jllr.vol5i2.3437.

[8] Ririn Aswandi, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan, "PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIAN DATA PROTECTION SYSTEM (IDPS)," *LEGISLATIF* 3, no. 2 (2020): 167–90, https://doi.org/10.20956/jl.v3i2.14321.

commercial institution, it must obtain permission from the owner of the personal data because the owner's permission is an absolute requirement in the use of a person's ownership, including personal data. Dewa Gede Sudika Mangku in his research entitled The Personal Data Protection of Internet Users in Indonesia said that This Contrasts with the increasing development of technology and increasing number of digital base service users who demand personal data protection efforts that require a stronger legal basic,[9] It gives an idea that the unequal conditions at the time of technological development and the increasing use of digital-based services are not followed by personal data protection efforts so that the use of personal data without rights and against the law is difficult for law enforcement. Regarding data protection in the international context, Muhammad Fakih Adhiwisaksana in this research entitled The Competence Forum and Applicable Law in Personal Data Protection with Foreign Element said that at the international level, corporate in the formulation regional or international conventions related to the protection of personal data needs to be carried out.[10]

In the personal data protection law that government has set, there are still several crucial problems that must be fixed because they will affect its implementation in the future, the role of a legal theory and principle plays a very significant role in strengthening the construction of a norm in legislation, a norm will be problematic if it is not in line with the principles and legal theories that apply globally, Norms built without paying attention to legal principles and theories will be fragile and weak, so they will cause problem in the enforcement later and even collapse public trust in this rules many legal norms are subject to judicial review because they contain problematic norms. It is understood that with the enactment of the law on the protection of personal data, it is actually hoped that there will no longer be an unauthorized use of personal data by other people, However this law is considered to be able to increase

---

[9] Dewa Gede Sudika Mangku et al., "The Personal Data Protection of Internet Users in Indonesia," *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 202–9, https://doi.org/10.35741/issn.0258-2724.56.1.23.

[10] Muhammad Faqih Adhiwisaksana and Tiurma M.Pitta Allagan, "THE COMPETENT FORUM AND THE APPLICABLE LAW IN PERSONAL DATA PROTECTION WITH FOREIGN ELEMENT," *Indonesian Journal of International Law* 20, no. 3 (2023): 442–70, https://doi.org/10.17304/ijil.vol20.3.2.

public trust, but in some of the articles in this law several things still cause concern for their personal data. Therefore, several articles in this law need to be tested in depth using legal theories and principles relevant to the issue. The author highlights some provision about ptotecting personal data from absolute right theory ultimum remidium and privat autonomy.

Method

The type of research used is legal-normative law, legal research with a norm doctrinal oncoming, normative legal research is basically an activity that will examine the aspects (to solve problems that exist in) the internal aspects of positive law,[11] namely research to study a law from the point of view of its norms, the approach used is the approach Legislation and Approach of Legal Principles/Principles and Theories, with this approach will be scientifically and in-depth tested the norms that are the central issue by using principles/principles and theories that have relevance to the norms in question, legal materials are obtained from sources of laws and regulations, sources of books, scientific articles and other data sources, legal materials are processed, developed and analyzed using theories so that accurate conclusions will be obtained.

Result and Discussion

A. Protection of Privacy Rights in Online Transactions Reviewed from the Absolute Right Theory

Digital transactions are open transactions where everyone is free to make transactions even beyond the country's territorial borders, which offer a wide variety of open products and services, several digital business models appear in the digital economy. Open markets are digital transactions that are open to everyone directly through of peer-to-peer. The open market removes the barriers between one country and another

[11] Kornelius Benuf and Muhamad Azhar, "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Kontemporer," *Jurnal Gema Keadilan* 7, no. 1 (August 7, 2020): 20–33, https://doi.org/10.24246/jrh.2019.v3.i2.p145-160.

without having to have a special permit in establishing these transactions, economically the open market has a positive impact on economic growth, but on the legal side it still leaves various kinds of problems that threaten the protection of citizens' interests by the State, including the protection of citizens' privacy rights in economic relations in the international trade arena (global market). Independent data protection authorities oversee enforcement, enhancing trust in the digital ecosystem and supporting sustainable economic growth in an increasingly data-centric world.[12] David Banisar classifies privacy into 4 (four) types, namely information privacy, body privacy, communication privacy, and territorial privacy.[13] If you look at the legal rules in Indonesia, the regulation on personal data protection is still inadequate. This means that the protection of personal data is still weak and general.[14] The problem in the implementation of the Personal Data Protection Law (PDP) is that the warranty of legal protection for personal data owners in the country is if they face a dispute with a personal data controller in another country, namely that the warranty of personal data protection by a personal data protection institution in another country can be reabile and does not pervert the organizer of personal data, include Indonesian citizens by personal data overseer in other countries. Chapter VII Article 56 paragraph (1) states that the personal data controller may transfer personal data to the personal data overseer and/or personal data processor outside the jurisdiction of Indonesia in conformity with the clause regulated in this Law. This paragraph (1) does not clearly include the phrase, "with the clearance of the personal data subject" which is the basic of the transfer of personal data, whether or not the personal data owner is approved, the agreement is the main condition for entering into an agreement. Suppose, in law the agreement or licence is an absolute

---

[12] Lu Sudirman, Hari Sutra Disemadi, and Arwa Meida Aninda, "Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective," *Journal of Etika Demokrasi* 8, no. 4 (2023): 497–510, https://doi.org/10.26618/jed.v%vi%i.12875.

[13] Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)* (Jakarta Timur: Sinar Grafika, 2023).

[14] Albert Lodewyk Sentosa Siahaan, "URGENSI PERLINDUNGAN DATA PRIBADI DI PLATFORM MARKETPLACE TERHADAP KEMAJUAN TEKNOLOGI," *Majalah Hukum Nasional* 52, no. 2 (2022): 209–23, https://doi.org/10.33331/mhn.v52i2.169.

condition in the transaction. In this case it is also an absolute requirement in a data transfer transaction, if there is no consent from the personal data owner, there is a "defect of will", with the defect of the will in the transaction, what is done by the Personal Data Controller does not have the force of law, a defect in the will whose indicator is an error, coercion, and fraud can be used as a basis for canceling agreements,[15] assuming that, the owner of personal data has the right to demand the termination of the data transfer and if the owner of the personal data suffers losses from the data transfer, then has the right to demand compensation to the Personal Data Controller, the aspect of privacy protection, the use of any information through electronic media that concerns data about a person's personal must be done with the consent of the person concerned unless otherwise stipulated by laws and regulations. [16]

This provison is considered to disregard definitive rights of the personal data owner. Absolute rights include personality rights, rights within the scope of family, and material rights of which personal data categorized under metrial right[17] this is the opposite of the main goal of the formation of the Personal Data Protection Law, In this context, Article 56 stipulates solution of personal data protection is carried out by Arbitration, courts, or other dispute resolution bodies, however, these do not guarantee the protection of personal data of a person or a particular legal entity. In affair of a conflict between the owner of personal data, both personal data and corporate data to be resolved through an international arbitration institution must be included in the preliminary agreement which provides that in the event of a dispute, both parties agree to submit the settlement to a specific arbitration institution so that it must be expressly included in the clause of the data processing agreement. The arbitration agreement is the basis for the emergence of the arbitral authority to accept and resolve disputes between the parties.

---

[15] I Ketut Widia and I Nyoman Putu Budiartha, "Cacat Kehendak Sebagai Dasar Batalnya Perjanjian," *KERTHA WICAKSANA* 16, no. 1 (January 27, 2022): 1–6, https://doi.org/10.22225/kw.16.1.2022.1-6.

[16] Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity* (Refika Aditama, 2023).

[17] Aditya Nabilah Lubis and Abdul Salam, "Perlawanan Pihak Ketiga Sebagai Pemilik Benda Terhadap Benda Yang Dijadikan Jaminan Fidusia Tanpa Persetujuan Pemilik Benda (Studi Kasus: Putusan Mahkamah Agung 1012 K/PDT/2021)," *Lex Patrimonium* 1, no. 1 (2022): 1–16.

Without an arbitration agreement, there is no arbitration authority by itself.[18] There are 2 (two) types of arbitration agreements, namely Pactum Decompromittendo and Deed of Compromise, pactum compromittendo is only possible if previously between the two parties is bound in an agreement and the agreement to appoint an arbitral institution has been specified in the principal agreement, for legal acts that do not originate from the agreement, the appointment of an arbitral institution is only possible using the deed of compromise appointed after a dispute over mutual agreement arises.

International Arbitration Bodies are known to have a stronger legal standing than national courts, so it can be predicted that the defeat will be on the side of Indonesian citizens, as well as the obligations imposed on the Personal Data Controller and the owner of personal data are very naïve because first, the provision has touched the legal realm of a foreign country and second, the limitation of the authority of the Personal Data Controller to "enforce" the compliance of the Personal Data Controller in other countries. Moreover, in the event of a criminal offense that is very difficult in practice without mutual assistance in criminal matters or extradition. The surrender or extradition of criminal offenders from the requested state to the requesting country often encounters obstacles or cannot be carried out because there is no extradition treaty between the two countries.[19]

In international trade transactions it is known as the principle of most favorite nation, which in the sense of this principle mandates that WTO members do not discriminate against each other and requires each WTO member to give the same, unconditionally, to every other WTO member,[20] in international trade it is required that each country provides

---

[18] Basuki Rekso Wibowo, "PERJANJIAN ARBITRASE DAN KEWENANGAN ARBITRASE DALAM PENYELESAIAN SENGKETA BISNIS DI INDONESIA," *Juris and Society: Jurnal Ilmiah Sosial Dan Humaniora* 1, no. 1 (2021): 1–17, https://journal.pppci.or.id/index.php/jurisandsociety/issue/view/2.

[19] Nahdia Nazmi and Hayati Fauziyah, "URGENSITAS PERJANJIAN EKSTRADISI SEBAGAI UPAYA PENEGAKAN HUKUM PIDANA," *Journal Of Islamic And Law Studies* 7, no. 1 (2021): 1–10, https://doi.org/10.18592/jils.v7i1.9531.

[20] Elizabeth Sefanya Roulina, "Pengaturan Prinsip Most Favoured Nation (Mfn) World Trade Organization Dalam Pelaksanaan Ekspor Impor Di Indonesia," *Jurnal Kertha Negara* 11, no. 5 (2023): 527–36, https://ojs.unud.ac.id/index.php/Kerthanegara/article/view/99974.

equal opportunities for other countries to establish trade cooperation without discrimination. Without prioritizing the interests of one country over another, this is a global principle that must be adhered to by all countries that are members of the World Trade Organization (WTO). However, in digital global transactions, this principle cannot be applied because every country has a greater responsibility than just upholding the principle, the state has the responsibility to protect every citizen both in the relationship of individual transactions and legal entities formed based on Indonesian law, the protection of personal data is a right of privacy and must be protected by the State.[21] In the relationship of such global transactions, there may be disputes between Indonesian citizens and/or legal entities and citizens/legal entities of other countries, including if the personal data of Indonesian persons/legal entities is misused by foreign persons/legal entities. Therefore, this Personal Data Protection Law has reached legal protection for Indonesian citizens in carrying out global business transactions or vice versa, including the institution to be formed, namely the Personal Data Protection Institution.

The existence of the Personal Data Protection Institution (Chapter IX) can strengthen the implementation of the PDP Law and ensure that the PDP Law and its enforcement ensure legal certainty, fairness and benefit for domestic business transaction relations as well as relations between countries. In Chapter IX the role of this institution is devoted to the settlement of administrative disputes only, administrative law on the one hand provides juridical means for government bodies to realize the objectives of government, and on the other hand provides the public with guarantees against improper and illegal government actions that are contrary to the law, the institution should also be responsible it can be asked for assistance to provide information as a witness experts who supervice from the upstream and downstream of the agreement in the processing and controling personal data. In such a way, it is hoped that the settlement of administrative or criminal disputes can obtain legal certainty and guarantee a fair and beneficial settlement.

---

[21] Rizky P.P Karo Karo and Teguh Prasetyo, *Pengaturan Perlindungan Data Pribadi Di Indonesia: Perspektif Teori Keadilan Bermartabat* (Bandung: Nusa Media, 2020).

The existence of the Personal Data Protection Institution that will be established should be given the competence to resolve personal data disputes as the first institution that will see, assess and process allegations of misapplication of personal data that are commercial in nature and cause losses to one of the parties. Suppose this institution is only given the authority to impose administrative anctions concerning the missue of personal data within the state, In this case it may be feasible, Still whether this institution will be able to impose administrative sanctions if the violator is an institution outside Indonesia, of course it is difficult to implement because administrative law is very closely related to the authority of the State over institutions/legal entities/individuals within the scope of a State mandate of a law and regulation that orders the State to provide administrative sanctions. Meanwhile, global e-commerce transactions are activities in the civil domain of businesses that can penetrate the legal boundaries of one country with another country because the basic principle is that whoever harms others must compensate for the loss due to their fault.

Based on the above agument, that privacy data is one of the basic rights owned by every person and other parties must uphold the right to privacy, the use and utilization of a person's privacy rights must be with the permission of the owner of the privacy right, without permission from the owner of the right, the user or who uses the right can be held responsibility both civilly and criminally. Respect for the right to privacy is respect for the absolute right theory.

In simple terms, Privacy as autonomy can be interpreted as a person's right to legally protect everything that is attached in the form of activities and property rights without being influenced and disturbed by other, which place more emphasis on the right to limit the discrimination of information relating to them. The concept of privacy of autonomy is a basic concept that is very important and becomes the foundation in the context of information dissemination, everyone needs to understand and uphold this concept, it is not justified for someone to take data, or utilize or disseminate information that is personal to someone without the license of the owner of personal data. Legally, suppose someone take data or utilizes or disseminates personal information belonging to another person with permission but not for their purpose and causes harm to the data owner, in that case the action is a civil wrongdoing because it fulfills

the elements of Article 1365 of the Civil Code. On the other hand, if the personal data is taken, or utilized or disseminated without the data owner's permission, the act is a criminal offense as stipulated in Law Number 11 of 2008 as amended by Law Number 19 of 2016, if the unauthorized act causes harm to the dignity, honor or position of the data owner, the act is a criminal offense of defamation. Based on these considerations, the concept of privacy as autonomy becomes the basis for applying of personal data protection.

B. Personal Data Dispute Resolution Model Reviewed from the Principle Law

The issue of legal protection is very closely related to Human Rights (HAM), There is no conflict between the theory of legal protection of privacy rights and human rights, human rights are the basic foundation for the fulfillment of basic human rights belonging as the right to opinion, the right to expression, the right to security, the right to legal protection and so on, in principle, the protection of personal data aims to ensure the preservation of human rights, opening, utilizing, processing and informing personal data without permission is contrary to human rights. Protectiing personal data directly related to the 1948 United Nations Declaration of Human Rights (UNDHR), where some of the rights that must be protected in the declaration include the right to security and legal protection. Everyone must obtain security from crimes against themselves and their property, one of the property rights of every human being is personal data, and everyone must obtain legal protection from the State from acts of abuse of everyone's data by enacting data protection regulations, establishing supervisory organs and establishing legal settlement mechanisms in the event of a violation of personal data.

The challenges to the protection of personal data will be greater along with advances in information technology such as Artificial Intelligence (AI) and machine study, technological advances to support the progress of human science must be regulated in such a way as not to violate the personal rights of others, the theory of "privacy as autonomy" must be upheld in anticipation of these technological advances, This theory will remain relevant and in line with technological advances as

long as the parties using information technology uphold this theory, this theory will be able to ward off the manipulation of personal data in the use of Artificial Intelligence or machine learning, even otherwise Artificial Intelligence technology is designed to protect personal data and be able to track violations of one's person.

Everyone must fundamentally get fair legal protection from the authorities, legal protection is a basic right owned by everyone as a human nature as a civilized person, including legal protection of their data, personal data is used or not used by another person who does not have the owner's permission, then this is included in the unlawful act, based on the formulation in the Nieuw Nederlands Burgerlijk Wetboek, an unlawful act is an act that violates the (subjective) rights of another person or acts (or omissions) that are oppsite to obligations under the law or opposite to what according to not regulated writing should be execute by a person in his association with fellow citizens,[22] especially if the personal data is used without the right to obtain personal benefits, then this can be classified as entering the realm of criminal law. In addition to the legal consequences, the PDP Law lists various sanctions for data violations or misuse that cause losses. Consumers also have the right to demand and take in compensation for violations of personal data processing. In the Personal Data Protection Law, no provision that expressly separates the application of administrative or civil sanctions must take precedence in resolving personal data management disputes rather than criminal sanctions. The application of sanctions in legal practice in Indonesia in the context of international agreements on personal data protection must be seriously observed by the Indonesian government after the enactment of the Personal Data Protection Law, especially under the supervision of personal data protection institutions.

In legal theory, principles are guidelines both in the formation of laws and regulations and in the application and enforcement of laws so that the law can be enforced based on legal principles and not violate the law, every law and regulation that is made is always based on basic principles or principles, legal principles are the foundation of a law and

---

[22] Afiif Hadiani Pratiwi, Edi Wahjuni, and Nuzulia Kumala Sari, "Perbuatan Melawan Hukum Dalam Kebocoran Dara Penumpang Lion Air Group," *Journal of Private and Economic Law* 1, no. 2 (2021): 107–34, https://doi.org/10.19184/jpel.v1i2.24615.

regulation, if the legal principle is conveyed, the building of the implementing law will fall.[23] Because the position of legal principles in a legal system is so important, it is not justified to be set aside or ignored, if it happens, it has collapsed the legal building itself because a legal building depends on how strong the legal foundation is that must be upheld and obeyed. The legal principle that is the foundation of positive law is actually an abstraction of a more general rule whose application is wider than the provisions of positive legal norms, legal norms must be in line with legal principles and even norms aim to uphold legal principles because therefore the position of legal principles is higher than the legal norms themselves.

In the legal system known as a principle called ultimum remidium, Van De Bunt stated that criminal law as ultimum remidium means that criminal law is used if other laws are unable to solve the problem of law violations, so that if the violation is a violation in the realm of administrative law, then administrative sanctions should be carried out first, Suppose the perpretator does not want to carry out civil sanction, In that case can be elevated to a criminal case as criminal law deliberately inflicts suffering in maintaining the norms recognized in the law. This is why criminal law must be considered as the ultimate remedium, namely the "last resort" if the sanctions in other laws are incapable or considered inadequate or unenforceable, the use of personal data is part of the transaction between the data owner and the personal data processor which is based on the agreement of both parties so that the basis for its implementation is the existence or absence of consent, if one of the parties does not carry out the content of the agreement or there is an allegation of irregularities to the agreement, it must be resolved first using a civil law approach, namely based on Article 1238 of the Civil Code, the debtor is declared negligent with a warrant or with a similar deed, or Based on the strength of the agreement itself, that is, if this agreement results in the debtor must be considered negligent with the passage of the specified time. and one of the parties can demand to pay costs, damages and interest based on Article 1243 of the Civil Code, compensation for

[23] Djumikasih Djumikasih, "MODEL PENCANTUMAN ASAS HUKUM DALAM PEMBENTUKAN HUKUM PERIKATAN NASIONAL," *Jurnal Hukum & Pembangunan* 52, no. 3 (2022): 768–30780, https://doi.org/10.21143/jhp.vol52.no3.3374.

costs, losses and interest due to the non-fulfillment of an obligation begins to be required if the debtor, even though he has been declared negligent, is still negligent to fulfill the agreement or something that must be given or done can only be given or done within a time beyond the predetermined time. If the party who has to compensate for costs, losses and interest does not carry it out based on their own awareness summons or the judge's order, they can be held criminally liable. This is in by principle of primum remidium that civil law must be enforced first, if what is obligatory is not carried out, then the last resort can be made, namely criminal law based on the principle of ultimum remidium. Therefore, wherever an act that harms a person/legal entity economically occurs, it can be held accountable. Civil sanctions are applied if the enforcement of the laws and regulations causes losses to the person affected by the provisions in the laws and regulations.

Thus, the legal principles of privacy data protection must be seen from several legal aspects, namely; First, the domain of civil law, if the legal relationship begins from a transaction between legal subjects, here it contains various agreements that regulate the rights and obligations of the parties, including if one of the parties will use, utilize or transmit its privacy rights, it must be the permission of the owner of the privacy rights, if there is a violation of the agreement that causes losses, then the violator can be sued civilly. Domain The criminal law domain occurs if a person uses, utilizes or transmits a person's privacy data without rights aimed at benefiting himself or others, especially to the extent that it disturbs a person's dignity, then it can be criminally prosecuted. Meanwhile, in the domain of administrative law, if the personal data controller does not implement the provisions of laws and regulations, the personal data controller can be given administrative sanctions according to the error level.

In the national context, if there is a use of personal data without a person's rights, it should be resolved civilly, because based on Supreme Court Regulation Number 1 of 1956, it is stated that if in the examination of a criminal case it must be decided that there is a civil matter or an item or about a legal relationship between two specific parties, then the examination of a criminal case can be suspended to wait for a court decision in the examination of the case civil about the

existence or absence of civil rights.[24] Thus, in a civil examination, it can be seen whether there is a loss of a person or corporation to their rights in the transaction carried out, PERMA Number 1 of 1956 and SEMA Number 4 of 1980, is a delay and suspension, not a termination because stopping the case is the authority of the investigator to stop the investigation and the public prosecutor to stop the prosecution. The judge is not authorized to stop the examination because there is of a pre-judicial dispute but rather to postpone or postpone the examination.[25] After that, it can only be developed whether there are criminal elements in the case, so that the case can be assessed comprehensively and integrally, all legal loopholes must be explored and a case can be resolved completely. There is a legal view that if a case has been processed civilly, it does not need to be resolved criminally or administratively, this view is a wrong opinion because this is partial and not resolved comprehensively even though a case must be seen to be fulfilled or not the legal elements, therefore in a case a person and/or corporation can be prosecuted and asked to be held accountable simultaneously (integrally) in a court collaboration to create a deterrent effect for actors and the community.

The problem of using personal data in absence of rights or no permission from holder of personal data, especially for commercial purposes through the internet, is not only carried out in one country, but the use of the internet is a global and international affair, be it in the form of transactions, the use or misuse of personal data can occur between citizens of different countries or an institution between countries so that the settlement scheme that must be used must also be a settlement scheme that must be used by with the principles of settlement globally and not nationally, In principle, there are two models of international dispute resolution in International Law, the first model is the peaceful dispute resolution model the second is the settlement model using violence. Article 2 of the Charter of the United Nations states that United Nations member states must settle disputes peacefully.

---

[24] "Peraturan Mahkamah Agung Nomor 1 Tahun 1956," Pub. L. No. 1 (1956).

[25] Sabrina Hidayat et al., "Penangguhan Putusan Perkara Pidana Melalui Putusan Sela Hakim Dengan Alasan Menunggu Putusan Perkara (Studi Putusan Sela Pengadilan Nomor/Pid.B/2021/PN.Kdi)," *Halu Oleo Legal Research* | 5, no. 1 (2023): 90–104, http://dx.doi.org/10.33561/holrev.v2i1.4198.

The model of peaceful dispute resolution can be carried out using 2 (two) channels, namely the litigation channel and the non-litigation route, the litigation channel for business disputes can be resolved using international arbitration institutions such as the ICC (International Chamber of Commerce), ICSID (International Centre for Settlement Dispute Between States and National of Other State) and UNCITRAL (United Nation Commission on International Trade Law). Meanwhile, the non-litigation route uses a scheme of consultation, negotiation, conciliation, and mediation. In Islamic literature, it is also known as a dispute resolution model called deliberation, al-sulhuh (peace agreement), hisbah and at-Tahkim (mediation),[26] it needs to be stated that the dispute resolution model related to civil and business relations has a global foundation and principles that can become a guideline in formulating a global/international dispute resolution model.

In disputes over the use of personal data without the permission of the data owner and the misuse of personal data belonging to individuals or legal entities, the dispute resolution that occurs must refer to the principles of international civil dispute resolution, the principle of prioritizing the efforts of a reconciliation based on compensation agreement (reconciliation based on compensaton) is the right settlement model to be applied, in this reconcilement based on compensation settlement model the parties given the opportunity to express rational reasons for the use of personal data, the owner of personal data is allowed to submit evidence that the data used is their own data and what losses have been experienced by the data owner, a peace agreement is made in writing and signed by both parties, witnessed and known. This written peace agreement is an important document for the parties to determine the next legal steps, the parties, especially unauthorized users of personal data, must have good faith towards the peace agreement, because if they do not have good faith to carry out the results of the peace, including an agreement to provide compensation for the part of the data owner.

As a legal basis, the demand for compensation is Article 1365 of the Civil Code which stipulates that every action that contravenes the law

---

[26] Abd. Rahman et al., "Pendekatan Sulh Dan Mediasi Sebagai Alternatif Terbaik Penyelesaian Sengketa Ekonomi Syariah," *Jurnal Ilmiah Ekonomi Islam* 7, no. 2 (July 1, 2021): 961–69, https://doi.org/10.29040/jiei.v7i2.2488.

and causes prejudice to another person obliges the person who induces the loss due their mistake to compensate the other person. If the reconciliation efforts based on compensation are not successful, the second step that can be taken is mediation efforts by a neutral party who has the competence to mediate on a mutual agreement in appointing a mediator, if This attempt also fails, then one of the parties can appoint an arbitration institution to resolve their dispute using a compromise deed, which is an arbitration agreement made by the parties after the dispute arises in the form of a separate agreement that is not stated in the main agreement, if the parties use the services of an arbitration institution then this step has entered the path of non-court litigation, the parties shall duly submit and comply with the mechanisms and awards to be taken by the arbitral tribunal.

With this pattern, the principle of ultimum remidium which teaches that the criminal path is the last effort can be carried out properly, a new criminal path can be applied if the above steps and efforts fail, if the failure is caused by the user who does not want to provide compensation experienced by the owner of the personal data, then the criminal offense can be used with the premise that the perpetrator has malicious intentions towards the owner of the personal data in using the data owner lawfully. Criminal law sanctions must be commensurate with the need to protect and defend social interests. Criminal Law is only justified if it useful to the community. Criminal law is necessary and justified if it is considered to have interfered with the interests of society aimed at protecting the interests of social lefe, or the public interest. Criminal law is a law that is used in the event of violations and crimes against the public interest, in the case of the use of personal data that requires the permission of the owner of personal data does not interfere with the public interest but is detrimental to the individual, the party who feels aggrieved by the use of his personal data can demand compensation, every consumer has the right to get compensation as well as in material content of the personal data protection bill.[27] If the user of personal data uses the personal data of many people and the victim is the

[27] Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *Law Reform* 18, no. 2 (2022): 144–63, https://doi.org/10.14710/lr.v18i2.43307.

wider community, then in addition to each individual having the right to sue, the State in this case is authorized to take action because the actions of the perpetrators have caused restlessness, shock and mass losses, if this condition is not acted upon, there will be a potential for the perpetrators to commit their acts even more widely and take more victims. Therefore, efforts through criminal law must be made if the act has disturbed the public interest, the principle of ultimum remidium is a legal principle embraced in the modern criminal law system, the principle of ultimum remidium is one of the characteristics of modern criminal law.[28]

In Europe, the General Data Protection Regulation (GDPR) aims to provide greater rights to individuals to control their personal data information including controlling their data freely, the application of this regulation not only affects companies in the European Union but also companies outside the European Union that process personal data of European Union citizens, this regulation has a significant impact in protecting personal data of European Union citizens. Personal data protection regulations in the United States were first established through the Fair Credit Reporting Act (FCRA) which campaigned for information accuracy, fairness and privacy, the Code of Fair Information Practices (FIPs) became a rule for all organizations that utilize and store personal data. In addition, the Privacy Act 1974 was implemented. In some fields, special regulations are also applied, such as the Family Education Rights (FERPA) of 1974 for the field of education, the Financial Privacy Act (RFPA) of 1976 for banking information, the Electric Communication Privacy Act (ECPA) of 1986, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and some of these regulations.[29]

The difference between personal data protection regulations in the European Union and the United States is that first, the European unon has stricter rules than the United States, second, the European Union prioritizes personal data over economic interests, Third, the Europen

---

[28] Ade Adhari, Pujiyono Pujiyono, and Sidharta Sidharta, "THE ULTIMUM REMEDIUM PRINCIPAL FORMULATION IS PARTIAL IN NATURE TO CORPORATE IN INDONESIA," *Indonesia Law Review* 14, no. 1 (2024): 1–30, https://doi.org/10.15742/ilrev.v13n3.1.

[29] Ridho Bima Pamungkas, Lemahnya Peraturan Hukum Perlindungan Data Pribadi: Studi Kasus Equifax Amerika Serikat Pada 2017, Center For Digital Society,3

Union uses an independent supervisory organ. At the same time, in the United States, it is left to internal organs. Fourth, the Europen Union has a single regulation. At the same time , it contains several different regulation based on the affairs and states in the United States. Fifth, regulations in the European Union have a very broad range of regulatory enforcement, namely, all Europenan Union member states. In contrast, in the United States the range is not board.

An example of a data misuse case in Europe, the Irish Data Protection Authority penalized Meta Platform Ireland Limited with a penalty of 1.2 billion EURO, this decision was based on the General Data Protection Regulation (GDPR) regulation, the penalty was given because of Meta's transfer of personal data to the United States based on the bad clause since 2020, Meta was also ordered to adjust its data transfer using the General Data Protection Regulation (GDPR) standards, this violation is considered very serious because it involves systematic, repeated and continuous transfers. This crime is not just about invading someone's privacy but triggers various cyber crimes such as extortion, threatening, abuse and fraud.

One of the cases in the United States is Avast which is an Antivirus company fined USD 16.5 million for unlawfully selling browsing data of its users, the FTC considers Avast failed to anonymize consumer browsing information adequately, the company sold data with unique identification for each browser and revealed the website, time, device type and location and lied to users that their software could eliminate tracking on the web while what happened was that they did tracking.

Based on the examples of cases in Europe and the United States, it will be a lesson and a hand for developing countries including Indonesia, where the high level of use of information technology in developing countries is not in line with the existence of adequate data protection regulations, the absence of organs that will handle data abuse and the level of knowledge and legal awareness that is considered still low will lead to high potential for personal data abuse. Awareness of the importance of the principle of "informed consent" in personal data protection that any form of data processing must be with the permission and knowledge of the data owner because the data owner has the right to determine the processing of his data, other parties can process data only to the extent of

interests based on an agreement with the data owner, thus other parties do not have full rights to the data they process.

Learning from impelementing of the General Data Protection Regulation (GDPR) in the European Union, the GDPR is a case in point. The GDPR applies to "the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union,[30] and several regulations in the United States, in Indonesia a special organ is needed that is authorized to supervise and process legally if there is misuse of personal data, the model applied in the European Union is considered more effective in Indonesia as a unitary state, where the supervisory organ must be independent instead of being handed over to the State court, this organ must be free from interference from the State and State institutions because state may carry out violations of personal data through State institutions. The basic principles and theories that overshadow and are used to protect of personal data are moral and ethical forces that must be upheld. As moral and ethical forces, these principles and theories will be able to influence and change the behavior of data users so that they can form good character not to use, process and inform people's personal data unlawfully.

The main task of the special organ in conducting supervision is in the context of administration to ensure that the data protection law has carried out the processing, use, transmission and delection of personal data, if there are allegations of violations committed by data processors, the injured party can make a written report to this special organ, based on of the report, the organ is authorized to carry out stages in the form of examining evidence, If the violation is administrative, the organ can impose administrative sanctions, if there is a civil loss, it can provide recommendations for filing a lawsuit for the injured party, if there is a criminal violation, it will be handed over to police investigators. If the violation is within the scope of an agreement between 2 (two) or more parties, then in the civil dispute resolution scheme it is possible to be resolved through an Arbitration mechanism either based on a Pactum de compromittendo made before the dispute occurs or a deed of compromise made after the dispute occurs as a separate agreement,

---

[30] Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation?, Cambridge University Press, https://doi.org/10.1017/aju.2019.80.

related to the issue of stages and mechanisms following those that apply in the designated arbitration institution.

The basic principles that overshadow and are used in the protection of personal data are moral and ethical forces that must be upheld, as moral and ethical forces, these principles and theories will be able to influence and change the behavior of data users so that they can form good character not to use, process and/or inform people's personal data unlawfully. The moral principle about the use and/or dissemination of other people's personal data requires everyone to have a moral foundation to uphold respect for one's personal rights that it is not justified for someone to use and/or disseminate other people's personal data without rights, fully realizing that the use and/or dissemination of other people's personal data without rights is an unlawful act, if there is misuse of other people's personal data then legally it can be prosecuted criminally. On the other hand, the ethical principle in the use and/or dissemination of other people's personal data must have the permission of the owner of the personal data, this permission is absolute and cannot be overridden by anyone, this ethical principle is called informed consent which is the basis for a person to be given the right by others to use and/or disseminate information on the owner's personal data, the use and/or dissemination of personal data belonging to others is an unlawful act, by law if the violation occurs, it gives the owner of the personal data the right to sue civilly, if done by a corporation, it allows the imposition of administrative sanctions by a special organ authorized to impose administrative sanctions. Therefore, upholding moral and ethical principles in the use and/or dissemination of other people's personal data is a very important element and determines the success of protecting personal data, without moral and ethical awareness, the use and/or dissemination of personal data without rights and misuse of personal data belonging to others will be difficult to realize. As a final recommendation, the researcher proposes that an special organ be immediately formed that is given the authority to supervise and process the misuse of personal data in Indonesia.

Conclusion

Personal data protection law has not fully provided legal protection for absolute rights, namely the right to privacy in online transactions, if the use or misuse of personal data carried out by foreign parties in foreign countries will be difficult to use the provisions of this law, even though this law is intended to provide protection for the personal data of Indonesian citizens, so that the existence of the Personal Data Protection Institution will be difficult to protect the interests of Indonesian citizens in global e-commerce transactions is considered incapable of protecting the personal data of citizens, the model of resolving personal data disputes without the rights or permission of the data owner in this law is not in line with the legal principles of ultimum remidium, the organ to dispute settlement of personal data in Indonesia is special organ like GDPR in the European Union, because it is able to resolve cross-border personal data cases.

References

Adhari, Ade, Pujiyono Pujiyono, and Sidharta Sidharta. "THE ULTIMUM REMEDIUM PRINCIPAL FORMULATION IS PARTIAL IN NATURE TO CORPORATE IN INDONESIA." *Indonesia Law Review* 14, no. 1 (2024): 1–30. https://doi.org/10.15742/ilrev.v13n3.1.

Adhiwisaksana, Muhammad Faqih, and Tiurma M.Pitta Allagan. "THE COMPETENT FORUM AND THE APPLICABLE LAW IN PERSONAL DATA PROTECTION WITH FOREIGN ELEMENT." *Indonesian Journal of International Law* 20, no. 3 (2023): 442–70. https://doi.org/10.17304/ijil.vol20.3.2.

Aswandi, Ririn, Putri Rofifah Nabilah Muchsin, and Muhammad Sultan. "PERLINDUNGAN DATA DAN INFORMASI PRIBADI MELALUI INDONESIAN DATA PROTECTION SYSTEM (IDPS)." *LEGISLATIF* 3, no. 2 (2020): 167–90. https://doi.org/10.20956/jl.v3i2.14321.

Ayunda, Rahmi. "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?" *Law Reform* 18, no. 2 (2022): 144–63. https://doi.org/10.14710/lr.v18i2.43307.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Kontemporer." *Jurnal Gema Keadilan* 7, no. 1 (August 7, 2020): 20–33. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160.

Budhijanto, Danrivanto. *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity*. Refika Aditama, 2023.

Djumikasih, Djumikasih. "MODEL PENCANTUMAN ASAS HUKUM DALAM PEMBENTUKAN HUKUM PERIKATAN NASIONAL." *Jurnal Hukum & Pembangunan* 52, no. 3 (2022): 768–30780. https://doi.org/10.21143/jhp.vol52.no3.3374.

Hidayat, Sabrina, Handrawan Handrawan, Herman Herman, Oheo Kaimuddin Haris, Heryanti Heryanti, and Irayana Irayana. "Penangguhan Putusan Perkara Pidana Melalui Putusan Sela Hakim Dengan Alasan Menunggu Putusan Perkara (Studi Putusan Sela Pengadilan Nomor/Pid.B/2021/PN.Kdi)." *Halu Oleo Legal Research* | 5, no. 1 (2023): 90–104. http://dx.doi.org/10.33561/holrev.v2i1.4198.

JDIH Kementerian Sekretariat Negara. "Data Base Jaringan Dokumentasi dan Informasi Hukum (JDIH)," n.d.

Junaidi, Junaidi, Pujiono Pujiono, and Rozlinda Mohamed Fadzil. "Legal Reform of Artificial Intelligence's Liability to Personal Data Perspective of Progressive Legal Theory." *Journal of Law and Legal Reform* 5, no. 2 (2024): 587–612. https://doi.org/10.15294/jllr.vol5i2.3437.

Karo, Rizky P.P Karo, and Teguh Prasetyo. *Pengaturan Perlindungan Data Pribadi Di Indonesia: Perspektif Teori Keadilan Bermartabat*. Bandung: Nusa Media, 2020.

Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16. https://doi.org/10.47776/alwasath.v2i1.127.

Lestari, Puji Ayu, Amelia Tasyah, Anada Syofira, Cintania Ade Rahmayani, Rizka Dwi Cahyani, Novita Tresiana, and Universitas Lampung. "Digital-Based Public Service Innovation (E-Government) in the Covid-19 Pandemic Era." *Jurnal Ilmu Administrasi* 18, no. 2 (2021): 212–24. https://doi.org/10.31113/jia.v18i2.808.

Lubis, Aditya Nabilah, and Abdul Salam. "Perlawanan Pihak Ketiga Sebagai Pemilik Benda Terhadap Benda Yang Dijadikan Jaminan Fidusia Tanpa Persetujuan Pemilik Benda (Studi Kasus: Putusan Mahkamah Agung 1012 K/PDT/2021)." *Lex Patrimonium* 1, no. 1 (2022): 1–16.

Mangku, Dewa Gede Sudika, Ni Putu Rai Yuliartini, I Nengah Suastika, and I Gusti Made Arya Suta Wirawan. "The Personal Data Protection of Internet Users in Indonesia." *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 202–9. https://doi.org/10.35741/issn.0258-2724.56.1.23.

Nazmi, Nahdia, and Hayati Fauziyah. "URGENSITAS PERJANJIAN EKSTRADISI SEBAGAI UPAYA PENEGAKAN HUKUM PIDANA." *Journal Of Islamic And Law Studies* 7, no. 1 (2021): 1–10. https://doi.org/10.18592/jils.v7i1.9531.

Peraturan Mahkamah Agung Nomor 1 Tahun 1956, Pub. L. No. 1 (1956).

Pratiwi, Afiif Hadiani, Edi Wahjuni, and Nuzulia Kumala Sari. "Perbuatan Melawan Hukum Dalam Kebocoran Dara Penumpang Lion Air Group." *Journal of Private and Economic Law* 1, no. 2 (2021): 107–34. https://doi.org/10.19184/jpel.v1i2.24615.

Rahman, Abd., Faizatul Fitriyah, Herman Efendi, and Adi Kusno. "Pendekatan Sulh Dan Mediasi Sebagai Alternatif Terbaik Penyelesaian Sengketa Ekonomi Syariah." *Jurnal Ilmiah Ekonomi Islam* 7, no. 2 (July 1, 2021): 961–69. https://doi.org/10.29040/jiei.v7i2.2488.

Ridho Bima Pamungkas, Lemahnya Peraturan Hukum Perlindungan Data Pribadi: Studi Kasus Equifax Amerika Serikat Pada 2017, Center For Digital Society,3.

Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta Timur: Sinar Grafika, 2023.

Roulina, Elizabeth Sefanya. "Pengaturan Prinsip Most Favoured Nation (Mfn) World Trade Organization Dalam Pelaksanaan Ekspor Impor Di Indonesia." *Jurnal Kertha Negara* 11, no. 5 (2023): 527–36. https://ojs.unud.ac.id/index.php/Kerthanegara/article/view/99974.

Ryngaert, C., & Taylor, M. (2020). The GDPR as global data protection regulation?, Cambridge University Press, https://doi.org/10.1017/aju.2019.80.

Siahaan, Albert Lodewyk Sentosa. "URGENSI PERLINDUNGAN DATA PRIBADI DI PLATFORM MARKETPLACE TERHADAP KEMAJUAN TEKNOLOGI." *Majalah Hukum Nasional* 52, no. 2 (2022): 209–23. https://doi.org/10.33331/mhn.v52i2.169.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (March 25, 2021): 38. https://doi.org/10.47268/sasi.v27i1.394.

Sudirman, Lu, Hari Sutra Disemadi, and Arwa Meida Aninda. "Comparative Analysis of Personal Data Protection Laws in Indonesiaand Thailand: A Legal Framework Perspective." *Journal of Etika Demokrasi* 8, no. 4 (2023): 497–510. https://doi.org/10.26618/jed.v%vi%i.12875.

Supeno, Supeno. "Legal Capacity in Online Loan Transactions (The Study on Legal Personal Liability Theory)." *Annals of Justice and Humanity (AJH)* 1, no. 2 (2022): 51–57. https://doi.org/10.35912/ajh.v1i2.1347.

Wibowo, Basuki Rekso. "PERJANJIAN ARBITRASE DAN KEWENANGAN ARBITRASE DALAM PENYELESAIAN SENGKETA BISNIS DI INDONESIA." *Juris and Society: Jurnal Ilmiah Sosial Dan Humaniora* 1, no. 1 (2021): 1–17. https://journal.pppci.or.id/index.php/jurisandsociety/issue/view/2.

Widia, I Ketut, and I Nyoman Putu Budiartha. "Cacat Kehendak Sebagai Dasar Batalnya Perjanjian." *KERTHA WICAKSANA* 16, no. 1 (January 27, 2022): 1–6. https://doi.org/10.22225/kw.16.1.2022.1-6.

Zain, Maulidya Alffi Anita, Miftahul Zanna Arsyad, Sudarmiatin Sudarmiatin, and Bambang Supeno. "E COMMERCE DALAM PENGEMBANGAN BISNIS: A BIBLIOMATRIK STUDY." *Hospitality* 11, no. 1 (2022): 335–46. https://doi.org/10.47492/jih.v11i1.1618.

This Page Is Intentionally Left Blank

Acknowledgment

None.

Funding Information

None.

Conflicting Interest Statement

There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.