International Proceeding
Universitas Tulungagung
2025

LEGAL PROTECTION OF PRIVACY AND PERSONAL DATA IN THE DIGITAL ECONOMIC ERA OF TECHNOLOGY IN INDONESIA

Retno Sari Dewi[1], Yapiter Marpi[2], Anang Sugeng Cahyono[3],
Surjanti[4], Galih Setyo Refangga[5]

sarie.soegito@gmail.com[1],yapitermarpi@gmail.com[2],akusukambahdi@gmail.com[3],
surjanti.unita@gmail.com[4] ranggagalih20@gmail.com[5]

[1,3,4] Universitas Tulungagung
[2] Universitas Jakarta
[5] Universitas Wisnu Wardhana

Abstract.

The current era of the digital economy has required business people business activities online. The Indonesian government must be able to guarantee and maintain online trust, namely if it wants to develop and enter the digital economy. This research uses a type of juridical-normative research. At the same time, there is also a need for stricter protection of privacy and personal data. This article, using normative or dogmatic juridical methods, discusses the issue of how Indonesian law should provide protection for privacy and personal data. In reality, Indonesia has privacy and personal data protection regulations that are spread across various laws and regulations and these provisions are not enough to encourage the development of Indonesia's digital economy. Apart from that, until now there is still uncertainty regarding the protection of privacy and personal data, because Indonesia does not yet have legal instruments that are suitable for the digital era. The author's view is that a legal instrument for the protection of privacy and personal data in the digital economy era must at least meet 3 criteria: (1) have an international character; (2) protect privacy and personal data as a positive right; and (3) is an element that binds individuals and economic society. Apart from that, it is a form of responding to the challenges of the times which have changed the direction of the economy and business towards digitalization. Of course, the government and business actors must work together to achieve the goal of good and healthy business competition.

Keywords: *Legal Protection, Digital Economic Era, Privacy and Personal Data*.

1 INTRODUCTION

The safeguarding of privacy and personal data significantly impacts the advancement of the digital economy inside a nation, particularly Indonesia. This is due to data emerging as a vital resource for propelling corporate operations in the digital age. Data has effectively become an individual's identity, which can be traded for numerous commodities. KBBI defines personal data as information pertaining to an individual's attributes, including name, age, gender, education, employment, residence, and familial situation. Article 1, Section 1 of the Minister of Communication and Informatics Regulation Number 20 of 2016 about the Protection of Personal Data in Electronic Systems (Permenkominfo No. 20 of 2016). Characterizes personal data as specific individual information that is saved, preserved, and regarded as accurate and confidential. Article 1, number 2 of Minister of Communication and Information Regulation No. 20 of 2016 defines certain individual data as any accurate and authentic information that can be directly or indirectly associated with an individual, provided its use complies with statutory regulations..[1]

In online transactions, it is essential to consider the buyer's perspective, as the seller, as a commercial entity, is obligated to compensate the buyer or consumer if the acquired items do not conform to the agreed specifications. This is done so that purchasers may claim their rights if there is product fraud performed by the vendor. The seller retains the authority to establish and receive the payment price for the sale of goods as per the agreement with the customer. Secure legal safeguards against the buyer's malevolent conduct. Legal detriment to consumers not attributable to the products and/or services being exchanged. Situated in Southeast Asia, Indonesia is a promising region for digital economic expansion. The great potential of Indonesia's digital economy is evidenced by its valuation of USD 27 billion in 2018. The expansion of the digital economy in Indonesia is characterized by a rising number of internet users. According to figures from the Central Statistics Agency (BPS) in 2019, internet users constituted 47.69 percent of the Indonesian population aged over 5 years, around 115 million individuals. According to the Indonesian Internet Service Users Association (APJII), internet user penetration in 2019 is predicted to be 64.8 percent of Indonesia's population, around 171.17 million individuals. This statistic positions Indonesia as the fifth country globally in terms of internet users, behind China, India, the United States, and Brazil.

Strengthening the digital economy in Indonesia is also inseparable from the role of the government, where President Jokowi has emphasized that Indonesia is targeting to become the largest digital economic power in ASEAN by 2025. This prediction is not without reason considering that in 2015, the value of Indonesia’s digital economy was recorded at 8 billion US dollars. This figure then continued to increase to 40 billion US dollars in 2019. Don Tapscott originally introduced the concept of the digital economy, describing it as a social phenomenon that impacts the economic system. This phenomenon is characterized by an intelligent space encompassing information, diverse access to information tools, information capacity, and information processing. Zimmerman asserts that the digital economy is a term frequently employed to elucidate the worldwide ramifications of the fast advancement of information and communication technology, which influences socio-economic situations. Despite its apparent profitability, the trend of digital economic growth in Indonesia has not addressed consumer

protection, particularly in relation to personal data safeguarding. Whether we realize it or not, with the digital era, the circulation of data has become increasingly uncontrolled. Disruption in the use of internet technology which covers all levels has resulted in data owners losing control over their personal data. This is a genuine threat, particularly as the swift advancement of information technology has engendered a novel paradigm in the trading system. The fast increase in internet users in Indonesia indirectly indicates substantial market potential, which will affect the formation of diverse new business options. The industrial era 4.0 has caused consumer and producer buying and selling transactions to become unlimited overseas. In this era, almost everything uses digital devices, thus indirectly influencing consumer behavior patterns in Indonesia. This can become a real threat with the increasing use of technology which can no longer be stopped, especially online.

Empirical evidence indicates numerous instances of consumer personal data breaches that have led to fraudulent activities, such as the misuse of personal information in electronic transactions (e-commerce), banking, the fintech sector, and online transportation service providers (Gojek, Grab, Maxim), among others. The most recent example indicates that 91 million users of the Tokopedia application experienced disadvantages due to the breach of their personal data, which was susceptible to exploitation. This case has been filed in the Central Jakarta District Court with registration number PN JKT.PST-0502020, dated May 6, 2020. The breach of consumer personal data underscores the necessity of enhancing personal data protection in Indonesia. The situation is further worse by the absence of legislative certainty about the safeguarding of consumer personal data in Indonesia.[2] Unlike other nations with specific legislation for personal data protection, Indonesia now lacks any controlling laws on this matter. The regulation of personal data in Indonesia remains generic and is dispersed across many legislative frameworks. The various regulations governing the protection of personal data have unwittingly resulted in overlapping mechanisms and authority in protecting personal data itself so that the consumers who suffer the most are the ones who suffer the most. In economic dealings, customers are unequivocally afforded protection.[3]

Generally, laws to safeguard consumers are established under Law No. 8 of 1999 concerning Consumer Protection (Consumer Protection Law). This legislation was established to safeguard consumers by delineating the rights and obligations of consumers, commercial entities, and the responsibilities of the government. Nonetheless, the applicable provisions in the Consumer Protection Law pertain to the right to comfort and security in the consumption of goods and/or services; there is no specific article within this law dedicated to the protection of consumers' personal data. It is believed that the recovery procedure for personal data breaches is not yet regulated.. In fact, up to now, applications often still apply “standard clauses” when asking for personal data from consumers who want to use their applications. By not setting out details in the clause regarding the extent of data limitations that can be used or not by business actors, consumers can be trapped by the terms of use and unknowingly give the right to use and distribute their personal data to third parties. Worse yet, business actors often do not provide consumers with the option to choose whether to agree or not with certain detailed data and instead tend to issue disclaimers that they cannot be sued or are not responsible for any reason.

Furthermore, the Consumer Protection Law also does not accommodate consumer losses in terms of data leaks.

Typically, each online transaction involves an electronic document generated by the seller that outlines the terms and conditions to be adhered to, including payment terms, timelines, and delivery options. In actuality, although the seller and buyer frequently do not formalize an agreement, an implicit contract exists when the buyer places an order for the required items and the seller agrees to provide them, so establishing a sale and purchase transaction between the parties. These stipulations and regulations may serve as legal safeguards for both parties. The Agreement grants the seller the right to receive payment from the buyer for the items acquired by the buyer. If the purchaser fails to remit money within the designated timeframe, the vendor may annul the transaction and offer the merchandise to an other potential buyer. Establishing explicit regulations concerning the payment period safeguards the seller, ensuring that the seller cannot be held accountable for transferring goods to another potential buyer if the original buyer fails to remit payment within the designated timeframe; this constitutes legal protection for the seller. The customer is entitled to receive items that conform to the specified kind and specifications agreed upon. The agreement allows the buyer to have the right to seek reimbursement from the seller if the delivered products are unsuitable. The buyer may swap items or get monetary compensation from the seller, constituting legal protection for the buyer. In the contemporary digital age, evidence once confined to physical papers has evolved into electronic information and digital documents.[4] The Information and Electronic Transactions Law (UU ITE) specifically asserts that information, electronic documents, or printed outputs constitute legitimate evidence and serve as an extension of legal evidence under the procedural law applicable in Indonesia.[5]

With the regulations surrounding this topic, it will give legal clarity about the adoption of electronic transactions in Indonesia. Some of the things above are legal aspects of e-commerce business and online buying and selling that must be understood when someone decides to carry out online transactions so that carrying out online business activities becomes easier and more comfortable. When someone decides to start their own business, risk is something that cannot be avoided. One of the risks commonly encountered by business people is being cheated by fellow company founders, losing personal assets because the business being run is not a legal entity, or clients suddenly canceling. And not paying the fees that should be paid. In this case, business law plays an important role in the running of business activities. Business law consists of two different things, namely law and business, where each has its own definition.

2 METHOD

This study employed normative legal research methodologies, namely by analyzing statutory legislation and international treaties pertinent to personal data protection. Law No. 8 of 1999, which pertains to consumer protection, Law No. 39 of 1999, which pertains to human rights, Law No. 36 of 2009, which pertains to health, Law No. 24 of 2013, which pertains to amendments to Law No. 23 of 2006, which pertains to population administration (UU Adminduk), Law No. 19 of 2016, which pertains to amendments to Law No. 11 of 2008, which pertains to electronic information and transactions (UU ITE), PP No. 40 of 2019, which pertains

to the implementation of Law No. 23 of 2006, which pertains to population administration as amended by Law No. 24 of 2013, and Regulation of the Minister of Communication and Informatics No. 20 of 2016, which pertains to the protection of personal data in electronic systems. Meanwhile, the international conventions referred to are the European Convention on Human Rights (European Charter of Human Rights), the Declaration of Human Rights of the Association of Southeast Asian Nations (ASEAN Human Rights Declaration), the General Declaration of Human Rights (Universal Declaration of Human Rights) and International Convention on Civil and Political Rights (International Covenant on Civil and Political Rights,[6] [5]

3 RESULT AND DISCUSSION

3.1 Factors Causing Misuse of Consumer Personal Data

The fast growth of information and communication technology has fundamentally given birth to different opportunities and difficulties. Information and communication technology has impacted the behavior of society and human civilization internationally. The advancement of information technology has facilitated active engagement between individuals and information service providers. Diverse sectors of life have employed information systems, including commerce (e-commerce), tourism, transportation, government, and the financial sector (e-payment)..[7] The theory of legal certainty put forward by Hans Kelsen defines law as a norm. A norm is a statement that emphasizes the “should” or das sollen aspect, by including several rules about what must be done. Each human being has freedom, but in living together he bears the responsibility to create an orderly life together. To realize an orderly life together, effective guidelines are needed which must also be adhered to together. These guidelines are what are called laws. If the law has determined a certain pattern of behavior, then each person should behave according to that determined pattern. Meanwhile, according to Satjipto Raharjo, legal protection is providing protection for human rights (HAM) that are harmed by other people and this protection is given to the community so that they can enjoy all the rights granted by law. Roscoe Pound stated that law is a tool of social engineering (law as a tool of social engineering). Human interests are demands that are protected and fulfilled by humans in the legal field. Roscoe Pound divides human interests protected by law into 3 (three) types, namely: first, interests in the state as a juridical body; second, interests as a state as a guardian of social interests; and third, the interests of individuals consist of privacy.

Due to globalization, nearly all aspects of "privacy" are exposed. With the advent of the digital world paired with the phenomena and promise of big data, privacy has become a precious commodity. In the digital economy, information, particularly personal data, is an invaluable asset due to its significant economic worth, leading to its extensive use by entrepreneurs. Big data has provided industries with chances to formulate business plans and innovate in the processing, analysis, and storage of large amounts of highly volatile data efficiently and swiftly. The significant function and economic worth of this data compel several entities to exploit it through hacking, whether online or offline, either individually or on behalf of an organization, without the data owner's consent.[8] Potential privacy infringements concerning personal data online frequently arise in extensive data collection endeavors (digital dossiers), direct

marketing (direct selling), social media, the execution of e-KTP initiatives, the implementation of e-health programs, and cloud computing operations. The misuse of personal data is exacerbated by its application in criminal activities, including the creation of fraudulent accounts, online fraud, the commercialization of telecommunications operator data leading to spam for users, the sale of banking customer information, and the trafficking of demographic data. Meanwhile, in the Personal Data Protection Law, strict sanctions are provided not only for data controllers but also data processors and/or third parties who are proven to have intentionally and unlawfully misused personal data. The sanctions provided are not only criminal but also civil, even compensation for immaterial losses is emphasized in this bill. Firm and binding sanctions are needed not only for interpersonal, private/corporate conflicts but also for state institutions. It cannot be denied that the potential for misuse of personal data can also be carried out by the state, for example in cases where the state deals with or enters into work agreements with private parties. Massive data collection carried out by the state is considered to be at risk of opening up opportunities for misuse of personal data by the state. Unfortunately, the Personal Data Protection Law does not yet accommodate sanctions regulations against state institutions. Therefore, according to the author, if the state is committed to providing personal data protection, the state needs to make regulations in which there are sanctions for the state if the state violates the protection of personal data. In this way, people will feel protected from abuse of authority or power that involves using people's (consumers') personal data for one-sided interests.

The large number of misuses of personal data is considered to be very disturbing to the public. For example, E-KTP and child identity cards (KIA) are considered very vulnerable to data leaks if uploaded via social media (social media), because the data will appear in Google search engine data searches so there is a risk of being easily misused or even traded. Apart from misuse of personal population data, widespread news about fraud using e-commerce sites (trading sites) is also something that is often encountered and is detrimental to consumers. It cannot be denied that the large number of internet users in Indonesia has indirectly encouraged the birth of many new business sectors (start ups), especially those operating in the e-commerce sector. Many start-ups, especially those operating in the e-commerce sector, have produced enormous amounts of new data. When engaging in online buying, individuals are required to provide personal information, including their name, address, telephone number, and email. During the payment process, the purchaser will input their credit card information. Upon making a purchase on an online platform, the buyer's personal information is acquired by the retailer or marketplace. When consumers consistently shop on a single site, data on their purchasing behavior and buying frequency is also collected by the online retailer.

private and personal data have become paramount, since people are unlikely to engage in digital transactions if they perceive a danger to the protection of their private and personal information. In the history of its evolution, privacy is a notion that is universal and known in numerous nations, both written in the form of laws and unwritten in the form of moral principles. The notion of the right to privacy originated in 1890 when Samuel Warren and Louis Brandeis authored an essay titled "The Right to Privacy," published in the Harvard Law Review. The article advocates for the acknowledgment of the individual right to privacy, or the right to be

left undisturbed, which should be safeguarded by current legislation, since individual rights constitute a fundamental aspect of human rights.[9] The safeguarding of personal data is typically regarded as an aspect of privacy protection, wherein privacy is a distinct notion and a basic human right, with data protection serving as a mechanism to uphold that privacy. Privacy constitutes a fundamental human right that recognizes the safeguarding of personal data as a significant entitlement. The right to privacy via data protection is essential for individual freedom and dignity..

The European Convention on Human Rights and the ASEAN Human Rights Declaration acknowledge the right to personal data protection as a human right. The right to safeguard personal data emerges from the intersection of the right to information and the right to privacy, having undergone significant change since the acknowledgment of human rights in the Universal Declaration of Human Rights. Article 12 of the Universal Declaration of Human Rights asserts that: "no individual shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to assaults on their honor and reputation." All individuals possess the right to legal protection from such interference or assault. The General Declaration of Human Rights is the principal component of international human rights legislation (International Bill of Rights) that governs fundamental rights and freedoms..

3.2 The Impact of Misuse of Consumer Personal Data in the Digital Economy Era

The author's study findings indicate the consequences of the improper use of consumer personal data in the digital economy age as follows: Initially, consumers are the primary parties that are susceptible and disadvantaged by cybercrime owing to the extensive accumulation and aggregation of personal data. This is justified, given that both the government and commercial entities might unilaterally engage in operations to gather and compile customer personal data. The compilation of personal data, including name, NIK, dwelling address, email, and telephone number, is deemed inconsistent with the standardization of personal data protection rules. In the event of a disagreement, the customer is the disadvantaged party and would incur losses; moreover, research indicates that insufficient consumer awareness about personal data protection further undermines their position.[10]

Most consumers tend not to actively ask business actors or service providers when carrying out a transaction. The lack of information provided by companies in the terms of the agreement (standard clauses) submitted to consumers also worsens the position of consumers. Consumers can be trapped by the terms of use on the site, thereby unknowingly giving the right to use and disseminate their personal data to third parties without the consumer’s knowledge as the data owner. This is not without reason because there are no regulations regarding the issue of disclosing personal data and company accountability in managing personal data in Indonesia. In fact, the existing regulations do not even mention the terms of use and privacy policy of a company, which should be the information rights of consumers.

Many companies do not include their corporate obligations to provide notifications of data leaks or damage to consumers. Companies also often do not explain the mechanisms for recovering consumer data where their privacy rights have actually been violated. In fact, this should be a form of the company’s commitment to protecting consumer personal data. Furthermore,

companies also often do not include the retention period for consumer data that has been used. Indeed, there are also companies that include retention matters, but unfortunately they do not communicate clearly to consumers how long the data will be stored or destroyed. As a result, consumers themselves suffer losses. What's worse, the Consumer Protection Law also does not accommodate consumer losses if personal data is leaked.[11]

Consumers' data is very susceptible to exploitation, as personal information is frequently interconnected when individuals utilize services or purchase products. For instance, the improper use of personal data resulting from promotional activities conducted by service providers or commercial entities for specific purposes. Promotional activities are governed by Article 1, number 6 of the Consumer Protection Law; nevertheless, the law does not contain rules that restrict the use of consumer personal data for promotional purposes without the consent of the individual involved. Article 9 of the Consumer Protection Law alone forbids commercial entities from supplying, producing, or promoting products and/or services that are false. These provisions do not address the safeguarding of consumer personal data. Consequently, customers lack a robust legal foundation to ensure their privacy rights, resulting in gaps or loopholes within the Consumer Protection Law that let businesses to disregard the privacy of consumer data. The aforementioned points indicate that while personal data protection has been addressed through various sector-specific regulations, there remains a necessity for comprehensive personal data protection laws to address cross-sectoral issues, given the complexity and interconnectivity of digital economy business models. In contrast, the European Union possesses a dedicated organization for personal data protection, known as the Data Protection Authority (DPA), responsible for overseeing the interchange of personal data. Referring to global data protection legislation (global Data Protection Regulation or GDPR), DPA is autonomous and not associated with the government or any private entity. The creation of a dedicated entity for the protection of personal data is essential, given the numerous entities engaged in data gathering and storage in Indonesia. Furthermore, legislation pertaining to personal data will be obligatory for all entities, including those in the public, commercial, and governmental sectors. Consequently, it is preferable for this specialized organization to maintain independence and own its own budget, free from affiliations with other entities.

The author asserts that, in addition to consumers being required to be more discerning when sharing personal data, there must also be stringent legal regulations about data limitations to prevent customers from getting ensnared by terms of use. These constraints: firstly, obtaining customer agreement is obligatory. The processing of personal data between the consumer, as the data owner, and the controller will occur pursuant to an agreement. The agreement must be explicit, utilize the Indonesian language, and avoid acronyms that may mislead buyers. The objective and intent of collecting user data must be explicitly defined from the outset, together with the specific types of information to be gathered. This aligns with Article 28(b) of Permenkominfo No. 20 of 2016, which mandates that "every electronic system operator must uphold the truth, validity, confidentiality, accuracy, relevance, and appropriateness of data usage for the purposes of obtaining, collecting, processing, analyzing, storing, displaying, announcing, transmitting, disseminating, and destroying personal data.".[12]

Second, investment is hampered. It cannot be denied that the misuse of consumer personal data in the digital economy era is considered to also have a negative impact on the country, namely that it can threaten investors' confidence in investing in Indonesia. Moreover, Indonesia currently has not specifically regulated personal data protection regulations in one law. With increasing cases of misuse of consumer personal data, of course investors will refuse to collaborate with Indonesia because there is no guarantee of legal certainty.

4 CONCLUSION

Current technological advances have greatly facilitated various human activities, one of which is buying and selling transactions carried out online. Sellers and buyers do not meet in person, with all the convenience, comfort, efficiency and effectiveness of time and money, buyers will be satisfied with getting the goods they want without spending time coming directly to the seller's shop, there are even many choices of websites and social media that can be accessed at any time just. Business competition in e-commerce is very tough, especially if the goods or services being sold are also offered by many other parties. Ecommerce encompasses all purchasing and selling transactions conducted over the internet. Ecommerce has several advantages over traditional retail establishments. In e-commerce, the complete trade process, encompassing product ordering, data interchange, and payment transfer, is conducted online. Amidst the growing complexity of digital technology and information, e-commerce represents an application of e-business or electronic business.

The urgency of protecting consumer personal data in the digital era is very important to implement immediately. The entry of the digital era combined with the phenomenon and potential of big data has resulted in personal data being transformed into a valuable commodity. This is not without reason considering that the development of the digital economy has been proven to encourage economic growth. Despite its significant economic importance, the safeguarding of customers' personal data remains suboptimal. When a purchaser conducts a transaction through a website or electronic platform operated by an e-commerce provider, the purchaser has entered into a contract with the e-commerce organizer or seller as outlined in the privacy policy. The legal protection afforded to sellers and purchasers remains consistent, regardless of whether they meet in person during the transaction. Business law in e-commerce transactions is applicable in the same manner as in conventional purchasing and selling operations. The laws concerning this topic will ensure legal clarity for the execution of electronic transactions in Indonesia.

REFERENCES

[1] Julisar and E. Miranda, "Pemakaian E-Commerce untuk Usaha Kecil dan Menengah guna Meningkatkan Daya Saing," *ComTech*, vol. 4, no. 2, pp. 638–645, 2013.

[2] M. Indriyani, "Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System," *Justitia J. Huk.*, vol. 1, no. 2, 2017, doi: 10.30651/justitia.v1i2.1152.

[3] T. D. Pohan and M. I. P. Nasution, "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce," *Sammajiva J. Penelit. Bisnis dan Manaj.*, vol. 1, no. 3,

pp. 42–48, 2023, [Online]. Available: https://e-journal.nalanda.ac.id/index.php/SAMMAJIVA/article/view/336

[4] A. L. S. Siahaan, "Urgensi Perlindungan Data Pribadi di Platform Marketplace terhadap Kemajuan Teknologi (Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances)," *Maj. Huk. Nas.*, vol. 52, no. 2, pp. 209–223, 2022, doi: 10.33331/ mhn.v52i2.169.

[5] L. Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia Urgency of Personal Data Protection Law in Indonesia; Comparative Study of English and Malaysia Law," *Kanun J. Ilmu Huk.*, vol. 20, no. 2, pp. 369–384, 2018.

[6] M. Fuady, *Konsep Hukum Perdata*. Jakarta: Rajawali Pers, 2014.

[7] D. R. M. Insana and R. S. Johan, "Peningkatan Kepuasan Konsumen Melalui Penggunaan E-Commerce," *Sosio e-Kons*, vol. 12, no. 02, p. 125, 2020, doi: 10.30998/sosioekons.v12i02.6451.

[8] S. Dewi Rosadi and G. Gumelar Pratama, "Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia," *Verit. Justitia*, vol. 4, no. 1, pp. 88–110, 2018, doi: 10.25123/vej.2916.

[9] A. Pujianto, A. Mulyati, and R. Novaria, "Pemanfaatan Big Data Dan Perlindungan Privasi Konsumen Di Era Ekonomi Digital," *Maj. Ilm. Bijak*, vol. 15, no. 2, pp. 127–137, 2018, doi: 10.31334/bijak.v15i2.201.

[10] R. A. Nugraha, "Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era Big Data," *Mimb. Huk. - Fak. Huk. Univ. Gadjah Mada*, vol. 30, no. 2, p. 262, 2018, doi: 10.22146/jmh.30855.

[11] S. Dewi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia," *Yust. J. Huk.*, vol. 5, no. 1, pp. 22–30, 2016, doi: 10.20961/yustisia.v5i1.8712.

[12] M. Rustam, "Internet dan Penggunaannya (Survei di Kalangan Masyarakat Kabupaten Takalar Provinsi Sulawesi Selatan)," *J. Stud. Komun. dan Media*, vol. 21, no. 1, pp. 13–24, 2017, doi: 10.31445/jskm.2017.210102.