

Legal Protection of Consumers' Personal Data in E-Commerce Transactions: A Normative Analysis of Indonesian Regulation and the Liability of E-Commerce Providers

Tandyo Budi Revita¹
Universitas Mahendradatta

Ni Ketut Wiratny²
Universitas Mahendradatta

Erikson Sihotang³
Universitas Mahendradatta

Correspondence : Tandyo Budi Revita (buditandyo91@gmail.com)

Abstract

The rapid growth of electronic commerce (e-commerce) in Indonesia has made consumers' personal data a valuable asset that is routinely collected, stored, and transferred by business actors, and has also exposed it to leakage, hacking, and misuse. This article examines (1) the legal protection of consumers' personal data in e-commerce transactions and (2) the liability of e-commerce providers when such data are leaked. Using a normative legal research method with a statute approach and a policy-oriented approach, the study analyses primary legal materials, namely Law No. 8 of 1999 on Consumer Protection and Law No. 27 of 2022 on Personal Data Protection, together with the Electronic Information and Transactions Law, Government Regulation No. 80 of 2019, and secondary legal materials. The analysis is descriptive, interpretative, evaluative, and argumentative. The findings show that protection is layered, combining general consumer law, electronic transaction law, and the Personal Data Protection Law, with both preventive and repressive characteristics. Before Law No. 27 of 2022, sectoral rules were fragmented and lacked clear sanctions. Liability of providers can be constructed through default, unlawful acts under Article 1365 of the Civil Code, the compensation mechanism in Article 19 of the Consumer Protection Law, and the accountability duties of electronic system operators. The study concludes that the Personal Data Protection Law strengthens legal certainty, but effective protection depends on consistent enforcement, robust internal data governance by providers, and greater consumer awareness.

Keywords: personal data protection; consumer protection; e-commerce; legal liability; data breach; Indonesia

INTRODUCTION

Advances in information and communication technology have created new opportunities and new legal challenges. Technology allows people to connect across national borders and has been adopted in many sectors, including electronic commerce (e-commerce) in trade, electronic education, electronic health, and electronic government. Among these, online buying and selling is one of the forms of trade most strongly shaped by information technology. It has replaced the traditional market, in which buyers and sellers meet physically, with remote trading over the internet, and it has changed the way consumers obtain the products they want (Perdana et al., 2014).

In e-commerce, the offer, the agreement, and the performance of the contract are all carried out through electronic data over computer and internet connections. Payment may be made through websites, e-mail, social media, mobile banking, interbank transfer, or even convenience stores.

Although the basic logic of an online sale resembles a conventional sales contract, the parties usually never meet. Consumers often have to pay in advance without being able to verify the quality of the goods or being sure that the goods will be delivered as ordered. The internet is also a public and insecure network, so electronic transactions are inherently high-risk (Sjahdeini, 2001; Arief & Gultom, 2005).

A particularly serious risk concerns personal data. To use an e-commerce platform, a user must normally create an account containing a name, telephone number, date of birth, address, e-mail address, and sometimes payment card details. Digital technology allows such data to be collected and moved from one party to another easily and, in many cases, without the knowledge of the data subject. When leaked, personal data can be sold on the dark web and used for identity theft, online fraud, extortion, and other cybercrimes. Personal data protection is therefore part of the protection of human rights: Article 28G paragraph (1) of the 1945 Constitution guarantees the right to protection of the person, family, honour, dignity, and property, and Law No. 27 of 2022 on Personal Data Protection (the PDP Law) is the statutory embodiment of that mandate.

Before the PDP Law was enacted, Indonesian rules on personal data were scattered across many sectoral laws and regulations, such as the Electronic Information and Transactions Law (EIT Law), Government Regulation No. 71 of 2019, Government Regulation No. 80 of 2019 on Trading Through Electronic Systems, and Ministry of Communication and Informatics Regulation No. 20 of 2016. Repeated large-scale data leaks in the years before 2022 showed how vulnerable personal data were, and leaks are commonly attributed to weaknesses in standard operating procedures, human resources, and technology (Sinaga, 2020; Aryani & Susanti, 2022). At the same time, Law No. 8 of 1999 on Consumer Protection (UUPK) aims to create a balance between business actors and consumers, but it was not drafted with digital data risks in mind.

Against this background, this article addresses two research questions: (1) how does Indonesian law protect consumers' personal data in e-commerce transactions? and (2) how are e-commerce providers held liable to consumers for the leakage of personal data? The article contributes to the literature by connecting three strands that are often treated separately, namely consumer protection law, electronic transaction law, and the new personal data protection regime, and by analysing them through the theories of the rule of law, legal protection, and legal liability.

Literature Review

The Rule of Law and the Hierarchy of Norms

The idea of the state based on law (*rechtsstaat* in the continental European tradition and the *rule*

of law in the Anglo-Saxon tradition) places the activity of the state not on persons but on a system of rules that binds and limits state administrators (Sibuea, 2010; Thohari, 2016). Stahl identified the core elements of the *rechtsstaat* as recognition of human rights, separation of powers, government according to law, and administrative courts, while Dicey described the rule of law through the supremacy of law, equality before the law, and a constitution based on individual rights (Asshiddiqie, 2008). Article 1 paragraph (3) of the 1945 Constitution declares that Indonesia is a state based on law, and its concept is commonly described as a Pancasila-based state of law whose norms must reflect Pancasila values as the *rechtsidee* (guiding ideal) of national law.

Legislation is understood both as the process of forming state regulations and as the body of regulations produced (Indrati, 2002). Hans Kelsen described a hierarchy of norms, and his student Hans Nawiasky elaborated it into four levels: the fundamental norm of the state (*Staatsfundamentalnorm*), the basic rules of the state (*Staatsgrundgesetz*), formal statutes (*Formell Gesetz*), and implementing and autonomous regulations (*Verordnung & Autonome Satzung*). Attamimi applied this scheme to Indonesia, where the hierarchy of legislation is regulated in Law No. 12 of 2011 as amended, and lower regulations, such as government regulations and ministerial regulations, are valid only insofar as they are based on higher norms. This theory matters for the present study because personal data protection in Indonesia is arranged across several levels of the hierarchy, from the Constitution, through statutes such as the UUPK, EIT Law, and PDP Law, to government and ministerial regulations.

Theory of Legal Protection

Legal protection means safeguarding the interests of people, especially those in a weak legal or economic position, by allocating rights and obligations and by keeping legal certainty. Rahardjo (2002) defines it as providing shelter for human rights harmed by others so that people can enjoy the rights granted by law. Setiono and Muchsin, as discussed in Indonesian legal scholarship, describe it as protecting society from arbitrary action and harmonising values in social relations. Mertokusumo argues that, to protect human interests, law must create an orderly and balanced society by dividing rights, duties, and authority and by maintaining certainty. In consumer relations, protection is typically understood in two forms: preventive protection, which prevents harm through information and regulation, and repressive protection, which provides remedies, sanctions, and compensation after harm occurs.

Theory of Legal Liability

Legal liability corresponds to the concept of *liability*, meaning legal responsibility for a wrongful

act, as distinguished from *responsibility* in a political sense (Ridwan HR, 2016). According to Kelsen (2006), a person is legally responsible for a certain act when he or she can be subjected to a sanction for a contrary act. Kelsen distinguished four kinds of liability: individual liability, collective liability, liability based on fault, and absolute liability. Traditional theory also separates liability based on fault from strict liability, and in some circumstances a person may be liable for wrongful acts of others, as with employers for their employees (vicarious liability) and organisations for their workers (corporate liability).

In Indonesian civil law, the general principle is liability based on fault under Articles 1365 to 1367 of the Civil Code, which require an act, fault, loss, and a causal relationship. Another principle is the presumption of liability, under which the defendant is presumed liable until he or she proves otherwise, so that the burden of proof lies with the defendant. Where the loss arises from non-performance of a contract, liability arises as default (*wanprestasi*). These principles provide the conceptual tools for determining when an e-commerce provider must answer for a data breach.

Personal Data, Privacy, and Consumers

Personal data are data about an individual who is identified or identifiable, alone or in combination with other information, directly or indirectly, through electronic or non-electronic systems (Article 1 point 29 of Government Regulation No. 71 of 2019). Protection of personal data is closely connected to the concept of privacy, which includes the right to enjoy private life free from interference, the right to communicate without surveillance, and the right to control access to information about one's personal life and data. The PDP Law distinguishes between specific personal data (such as health data, biometric data, genetic data, criminal records, children's data, and personal financial data) and general personal data (such as full name, gender, nationality, religion, and marital status).

A consumer under Article 1 point 2 of the UUPK is every person who uses goods and/or services available in society for the benefit of themselves, their family, other people, or other living beings, and not for trade. The UUPK protects only the ultimate consumer, as distinguished from the commercial and intermediate consumer (Nasution, 2001). The UUPK is founded on the principles of benefit, justice, balance, consumer safety and security, and legal certainty, and Article 4 lists consumer rights, including the right to comfort, security, and safety, the right to correct, clear, and honest information, and the right to compensation. Articles 5 and 19 respectively set out consumer obligations and the duty of business actors to compensate consumers for loss.

E-Commerce Transactions and Electronic Contracts

E-commerce is the sale and purchase of products, services, and information through computer networks, principally the internet (Matsuura, 2002). A marketplace is one model of e-commerce, acting as an intermediary that brings sellers and buyers together, while other forms include online stores owned by a brand or a company. Transactions are commonly classified as business-to-business, business-to-consumer, consumer-to-consumer, consumer-to-business, non-business, and intra-organisational. In Indonesian law an electronic sales contract is a species of contract under Book III of the Civil Code and must satisfy the four conditions of Article 1320: agreement, capacity, a specific object, and a lawful cause. Article 5 of the EIT Law gives electronic information and documents the status of valid legal evidence, and Article 20 provides that an electronic transaction occurs when the offer is received and accepted.

METHOD

This study uses normative legal research, also known as library research, which examines library materials or secondary data (Soekanto & Mamudji, 2012; Amiruddin & Asikin, 2004). The objects of normative research include legal principles, legal systematics, the degree of synchronisation of law, legal history, and comparative law. Here, the study focuses on legal principles and the rights of consumers concerning the protection and liability regimes for personal data in e-commerce.

Two approaches are used. The statute approach involves an inventory and analysis of legislation relating to personal data, consumer protection, and electronic transactions. The policy-oriented approach considers the goals, rationality, economic and pragmatic considerations, and values underlying the regulation of personal data (Marzuki, 2006). The two approaches complement one another in producing legal materials that can be analysed.

The study draws on two types of legal material. Primary legal materials are binding, authoritative sources, namely Law No. 8 of 1999 on Consumer Protection and Law No. 27 of 2022 on Personal Data Protection, supported by the 1945 Constitution, the Civil Code, the EIT Law, Government Regulation No. 71 of 2019, Government Regulation No. 80 of 2019, and Ministerial Regulation No. 20 of 2016. Secondary legal materials are books, legal journals, articles, and research results that explain the primary materials. Materials were collected through systematic note-taking that classified them by relevance to the research questions.

The analysis uses four techniques. The descriptive technique sets out the existing condition of legal norms as they are. The interpretative technique applies grammatical interpretation (by the

meaning of words) and systematic interpretation (by relating provisions to one another). The evaluative technique assesses the adequacy of norm formulations, and the argumentative technique supports the evaluation with legal reasoning. Together they lead from the identification of norms to conclusions about their sufficiency.

RESULTS AND DISCUSSION

The Legal Framework for Personal Data Protection in E-Commerce

The analysis shows that Indonesia protects consumers' personal data through a layered system of regulation rather than a single instrument. At the constitutional level, Article 28G paragraph (1) of the 1945 Constitution and Law No. 39 of 1999 on Human Rights recognise privacy as a human right and impose on the state a duty to protect it. Below this level, a number of statutes and regulations address personal data in electronic transactions, as summarised in Table 1.

Instrument	Relevant provisions	Role in protecting consumer data
Law No. 8 of 1999 (UUPK)	Articles 3, 4, 5, 19	General basis for consumer rights, security, information, and compensation.
Law No. 11 of 2008 on EIT (as amended)	Articles 5, 9, 15, 20, 26	Recognises electronic evidence; requires consent for use of personal data; obliges operators to run reliable, secure systems.
Gov. Reg. No. 71 of 2019	Articles 1 point 29, 3, 31	Defines personal data; requires reliable and secure electronic systems and protection of users.
Gov. Reg. No. 80 of 2019 (PP PMSE)	Articles 58 and 59	Personal data are private property; business actors act as trustees of the data.
Ministerial Reg. No. 20 of 2016	Article 2 paragraph (2)	Sets principles: privacy, consent, relevance, system reliability, notification of failure.
Law No. 27 of 2022 (PDP Law)	Whole law	Comprehensive standard for processing of personal data, data subject rights, controller duties, and sanctions.

Under Article 26 paragraph (1) of the EIT Law, the use of any information concerning a person's personal data through electronic media must be done with the consent of the person concerned, and paragraph (2) allows a person whose right is violated to file a lawsuit for the resulting loss. Article 15 of the same law obliges every electronic system operator to run the system reliably and securely and to be responsible for its operation, except where force majeure, or fault or negligence on the part of the user, can be proven. Government Regulation No. 71 of 2019 repeats the duty to operate a reliable and secure system and to protect users and the wider public from losses caused by that system.

Government Regulation No. 80 of 2019 is the most specific instrument for trade through electronic systems. Article 58 paragraph (1) treats personal data as the private property of the person or business actor concerned, and paragraph (2) requires business actors that obtain personal data to act as trustees in storing and controlling it. Ministerial Regulation No. 20 of 2016 supplements these rules with ten principles, among them respect for personal data as privacy, consent, relevance to the purpose of processing, adequacy of the electronic system, good faith to notify data owners in writing of any failure of protection, availability of internal rules, and ease of access and correction by the data owner.

The PDP Law then unifies these fragments into a general standard applicable to both electronic and non-electronic processing, while allowing each sector to apply protection according to its own characteristics. Its objectives include protecting the basic rights of citizens, ensuring that people receive services from corporations and public bodies, encouraging the growth of the digital economy, and strengthening the competitiveness of domestic industry. The PDP Law incorporates the principle of public interest, meaning that enforcement of personal data protection must take account of the interests of society at large. Its classification into specific and general data is directly relevant to e-commerce, where financial data, such as card and account numbers, fall within the category of specific personal data that deserves stronger protection.

Preventive and Repressive Characteristics of Protection

The regulatory design shows five recurring characteristics of consumer protection in Indonesian e-commerce. First, the preventive character emphasises transparency of information so that consumers can decide knowingly, as in the duty of business actors under Article 9 of the EIT Law to provide complete and correct information on contract terms, the producer, and the product offered. Second, the repressive character provides compensation and complaint mechanisms, notably Article 19 of the UUPK. Third, the principle of good faith, based on Article 1338 paragraph (3) of the Civil Code, requires honesty and forbids misleading conduct. Fourth, electronic evidence and agreements are recognised in Articles 5 and 6 of the EIT Law. Fifth, accountability of business actors for the security

of the systems they operate is emphasised in the EIT Law and Government Regulation No. 80 of 2019.

These characteristics indicate a hybrid approach that combines preventive and repressive protection and places the consumer as a legal subject entitled to legal certainty, justice, and digital security. This is consistent with the theory of legal protection outlined above, which treats the law as both an instrument for maintaining order and a guarantee of rights for weaker parties. Consumers in e-commerce are structurally weak: transactions are impersonal, information is asymmetrical, and the consumer cannot inspect either the goods or the data-handling practices of the platform.

Regulatory Gaps Before the PDP Law

Despite this layered framework, the analysis identifies several weaknesses that existed before the PDP Law. First, the earlier instruments were sectoral and general in nature. The EIT Law recognised the right to privacy but did not provide a detailed regime for how personal data must be processed, and it contained no definition of personal data itself. Second, Articles 58 and 59 of Government Regulation No. 80 of 2019 entrust business actors with managing personal data but do not stipulate sanctions or a clear form of liability when protection fails. Third, Indonesian law had not given a specific definition to sensitive personal data. Fourth, a large number of statutes (around thirty-two, according to legislative studies) contain provisions touching on personal data, mainly granting authority to collect and manage such data, which produced overlapping and inconsistent rules.

The absence of a comprehensive law had practical consequences. Data leaks became a public concern from about 2020, and without a governing statute there was no standard operating procedure that obliged data controllers to maintain, safeguard, and manage personal data. Data controllers therefore had little legal incentive to invest in security, and business actors themselves expressed uncertainty about how to implement personal data protection. The enactment of the PDP Law in 2022 responded to this vacuum and is best understood as a move from fragmented sectoral protection to a comprehensive regime that sets uniform norms for all parties who process personal data.

The value of the PDP Law lies, first, in legal certainty. Legal certainty means that a person can obtain what is expected under certain conditions and that norms are clear enough to serve as guidance. By setting out behavioural limits for buyers, platforms, and sellers, the PDP Law gives all stakeholders a clearer expectation of how personal data will be treated. Second, it strengthens trust in digital trade: adequate protection encourages people to provide personal data for broader purposes without fear that it will be misused, and it reinforces Indonesia's position as a trusted place for business and investment. Third, it fulfils the constitutional obligation of the state to protect all Indonesians in the digital era.

Where Consumer Data Is Exposed in the Transaction Process

Understanding liability requires locating the points at which data are exposed. E-commerce transactions can be divided into pre-contractual, contractual, and post-contractual stages. In the pre-contractual stage, consumers search for goods, examine product information, place items in a cart, and check out, which requires them to register and complete forms containing personal information. At the contractual stage, the electronic contract is formed when the seller accepts the buyer's order, in line with Article 20 of the EIT Law, and the contract must meet the requirements of Article 1320 of the Civil Code and of the implementing regulation on electronic contracts. At the post-contractual stage, payment and delivery are performed, and payment data (for example credit card information transmitted through a payment gateway to the acquirer and issuer) and delivery data are processed by several parties.

The parties involved in an electronic sale are therefore more than just the seller and the buyer. They also include banks or payment providers, internet service providers, and, in a marketplace model, the platform that mediates the transaction. Every one of these actors handles personal data, which is why the allocation of responsibility among them is a central legal question. In the marketplace model the platform operator functions as an electronic system operator and holds the accounts and transaction histories of users, so that a breach of the platform's systems can expose the data of a very large number of consumers at once.

Liability of E-Commerce Providers for Data Leakage

The second research question concerns how providers are held accountable when personal data leak. Several complementary legal bases can be identified from the analysis. Where the relationship between the consumer and the provider is contractual, for example through acceptance of the platform's terms of use, a party that fails to perform or violates its obligations commits default. If the provider promises to keep users' data confidential and secure but fails to do so, the resulting loss can be classified as default, giving rise to a claim for compensation.

Unlawful acts. Article 1365 of the Civil Code requires four elements: an act, fault, loss, and a causal link between fault and loss. A provider that neglects reasonable security measures may be found at fault, and the consumer's loss, such as identity theft, financial fraud, or misuse of an account, may be attributed to that fault. Because consumers often find it hard to prove fault inside a provider's technical systems, the principle of presumption of liability is particularly useful: the provider is presumed liable unless it proves that the leak did not result from its negligence.

Consumer protection law. Article 19 of the UUPK obliges business actors to compensate

consumers for loss arising from the goods or services they provide. Applied to digital services, a data leak that causes consumer loss can be qualified as a breach of contract or an unlawful act that gives the consumer a right to compensation. Article 4 of the UUPK further supports the consumer's claim through the right to security and to compensation.

Electronic transaction law. Article 26 of the EIT Law allows a lawsuit when personal data are used without consent, and Article 15 makes electronic system operators responsible for the reliable and secure operation of their systems, with exemptions only for force majeure or the fault of the user. Government Regulation No. 80 of 2019 adds that business actors must act as trustees of personal data, and the provider's duty of trusteeship provides an additional normative basis for holding it accountable.

The PDP Law. The PDP Law provides the most direct basis. It imposes duties on personal data controllers and processors to protect and secure the data they handle, gives data subjects the right to seek compensation for violations, and requires notification of data subjects and the authorities in the event of a protection failure. It also attaches administrative and criminal sanctions to violations. Its provisions create liability that does not depend solely on general civil law, and they fill the gap that Government Regulation No. 80 of 2019 left with respect to sanctions.

Considered through Kelsen's theory, the provider's responsibility arises from a legal duty (to secure data), and the sanction follows when that duty is breached. Since the duty stems from statutes, the responsibility is legal in nature. In terms of the two theories on official responsibility, the personal-fault approach places the burden on the individual whose act caused the loss, whereas the service-fault approach places it on the institution. For e-commerce, the institutional approach is more appropriate, because data leaks typically result from institutional failures in policy, technology, and staffing rather than from the acts of one person. This is consistent with the doctrines of corporate and vicarious liability.

The responsibility of the entrepreneur in e-commerce thus comprises guaranteeing the security of the system and of consumers' personal data, supplying products that match their description, and compensating for damage or non-conformity of goods. It also includes a broader ethical dimension: a business actor has to build a safe and trustworthy ecosystem by giving clear and accurate information and by protecting the security of payment systems.

Discussion of Challenges

Although the legal framework is now stronger, several challenges remain. The first is information asymmetry: consumers rarely understand how their data are processed, and standard-form clauses drafted unilaterally by business actors tend to favour the drafter. The second is proof.

Consumers must show a causal link between a breach and their loss, yet the evidence lies within the provider's systems. The presumption of liability and the recognition of electronic evidence help, but they need to be applied consistently by courts and complaint bodies. The third is jurisdiction: e-commerce is cross-border, and enforcement is difficult when the business actor is located abroad, although the regime is designed to apply to actors who transact with Indonesian consumers. The fourth is implementation. The PDP Law requires supporting regulations and an effective supervisory institution to operate as intended, and providers must translate its obligations into concrete internal procedures.

These findings are in line with earlier studies that stress the importance of personal data protection to consumer satisfaction and trust in online marketplaces (Aryani & Susanti, 2022), the need for a comprehensive legislative formulation (Sinaga, 2020), the framing of personal data protection as a privacy right (Kusnadi, 2021), and the need to renew consumer protection regulation in the digital business era (Novita & Santoso, 2021). The present study adds an integrated analysis of how these regimes work together and how liability can be constructed when protection fails.

CONCLUSION

This study concludes, first, that Indonesian law protects consumers' personal data in e-commerce through a layered framework that comprises the Constitution, the UUPK, the EIT Law, Government Regulation No. 80 of 2019, and, most importantly, the PDP Law. This framework has both preventive characteristics, through information, consent, and security duties, and repressive characteristics, through compensation and sanctions. The enactment of the PDP Law in 2022 replaced fragmented sectoral rules with a comprehensive standard and strengthened legal certainty for consumers and business actors.

Second, e-commerce providers can be held liable for the leakage of personal data on several complementary grounds: default, unlawful acts under Article 1365 of the Civil Code, the compensation obligation in Article 19 of the UUPK, the responsibilities of electronic system operators under the EIT Law and its implementing regulations, and the specific obligations and sanctions of the PDP Law. The presumption of liability and the institutional (service-fault) approach are especially suitable for easing the consumer's burden of proof.

Based on these findings, the study recommends that:

- e-commerce providers adopt sound personal data protection practices, including secure systems, internal data governance procedures, clear information to consumers about how their data will be used, and prompt notification when a breach occurs;
- the government and supervisory authorities complete the implementing regulations of the PDP Law and enforce it consistently, so that sanctions and compensation mechanisms are effective in practice;
- courts and consumer dispute bodies apply the UUPK, the EIT Law, and the PDP Law in an integrated manner, including the presumption of liability, to address the consumer's evidentiary difficulties; and
- consumers be educated to read privacy terms, to limit the data they disclose, and to use available complaint and dispute settlement channels.

Because this study is normative and based on legal materials, future research could add empirical analysis of court decisions, supervisory practice, and consumers' experiences after the PDP Law became fully applicable.

REFERENCES

- Amiruddin, & Asikin, Z. (2004). *Pengantar metode penelitian hukum* [Introduction to legal research methods]. PT Raja Grafindo Persada.
- Arief, D. M., & Gultom, E. (2005). *Cyber law: Aspek hukum teknologi informasi* [Cyber law: Legal aspects of information technology]. Refika Aditama.
- Aryani, A. P., & Susanti, L. E. (2022). Pentingnya perlindungan data pribadi konsumen dalam transaksi online pada marketplace terhadap kepuasan konsumen [The importance of protecting consumers' personal data in online marketplace transactions for consumer satisfaction]. *Jurnal Ahmad Dahlan Legal Perspective*, 2(1).
- Asshiddiqie, J. (2008). *Pokok-pokok hukum tata negara Indonesia pasca reformasi* [Principles of Indonesian constitutional law after the reform]. Bhuna Ilmu Populer.
- Indrati S., M. F. (2002). *Ilmu perundang-undangan: Jenis, fungsi, dan materi muatan* [The science of legislation: Types, functions, and content]. Kanisius.
- Kelsen, H. (2006). *Teori hukum murni* [Pure theory of law] (R. Mutaqien, Trans.). Nuansa & Nusa Media.
- Kusnadi, S. A. (2021). Perlindungan hukum data pribadi sebagai hak privasi [Legal protection of personal data as a privacy right]. *Al Wasath: Jurnal Ilmu Hukum*.
- Marzuki, P. M. (2006). *Penelitian hukum* [Legal research]. Kencana.
- Matsuura, J. H. (2002). *Security, rights, and liabilities in e-commerce*. Artech House.
- Nasution, A. Z. (2001). *Perlindungan hukum konsumen* [Legal protection of consumers]. Grasindo.
- Novita, Y. D., & Santoso, B. (2021). Urgensi pembaharuan regulasi perlindungan konsumen di era bisnis digital [The urgency of renewing consumer protection regulation in the digital business

- era]. *Jurnal Pembangunan Hukum Indonesia*, 3(1).
- Perdana, A., et al. (2014). Penyelesaian wanprestasi dalam perjanjian jual beli melalui media elektronik [Settlement of default in sale and purchase agreements through electronic media]. *Jurnal Ilmu Hukum*, 2.
- Rahardjo, S. (2002). *Sosiologi hukum: Perkembangan, metode, dan pilihan masalah* [Sociology of law: Development, methods, and choice of problems]. Muhammadiyah University Press.
- Ridwan HR. (2016). *Hukum administrasi negara* [State administrative law]. Rajawali Pers.
- Setiawan, R. (2008). *Pokok-pokok hukum perikatan* [Principles of the law of obligations]. Bina Cipta.
- Sibuea, H. P. (2010). *Asas negara hukum, peraturan kebijakan & asas-asas umum pemerintahan yang baik* [Principles of the rule of law, policy regulations, and general principles of good governance]. Erlangga.
- Sinaga, E. M. C. (2020). Formulasi legislasi perlindungan data pribadi [Legislative formulation of personal data protection]. *Jurnal RechtsVinding*, 9(2).
- Sjahdeini, S. R. (2001). *Hukum cyber: Sistem pengamanan e-commerce* [Cyber law: E-commerce security systems].
- Soekanto, S., & Mamudji, S. (2012). *Penelitian hukum normatif: Suatu tinjauan singkat* [Normative legal research: A brief review] (14th ed.). PT Raja Grafindo Persada.
- Sofian, A. (2021). *Hukum perlindungan konsumen di Indonesia* [Consumer protection law in Indonesia]. Sinar Grafika.
- Subekti. (2003). *Hukum perjanjian dan penerapannya* [Contract law and its application]. PT Raja Grafindo Persada.
- Thohari, A. (2016). *Hak konstitusional dalam hukum tata negara Indonesia* [Constitutional rights in Indonesian constitutional law]. Erlangga.
- Titik Triwulan, & Febrian, S. (2010). *Perlindungan hukum bagi pasien* [Legal protection for patients]. Prestasi Pustaka.
- Constitution of the Republic of Indonesia of 1945.
- Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata*).
- Law No. 8 of 1999 on Consumer Protection.
- Law No. 39 of 1999 on Human Rights.
- Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016.
- Law No. 27 of 2022 on Personal Data Protection.
- Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions.
- Government Regulation No. 80 of 2019 on Trading Through Electronic Systems.
- Regulation of the Minister of Communication and Informatics No. 20 of 2016 on Personal Data Protection in Electronic Systems.