Protection And Legal Security System For Digital Signature Users As Consumers In The Indonesian Legal System

[1]Tami Rusli, [2]Zainab Ompu Jainah, [3]Erlina B
Email: [1]tami.rusli@ubl.ac.id, [2]zainab@ubl.ac.id, [3]erlina@ubl.ac.id
Universitas Bandar Lampung, Indonesia

Article Info
Received:2023-11-17
Revised:2024-01-20
Accepted:2024-06-26

Keywords:
Legal Protection; Digital Signature; Consumer

Abstract
This research aims to find legal protection against digital signature users as consumers associated with the principle of justice. This research uses a normative juridical approach by focusing on secondary data. The research specification used is descriptive-analytical. The research stages were carried out through library research and field research as support. Data collection techniques were carried out through document studies and interviews. While data analysis is carried out in a qualitative, juridical manner. The results showed that since the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), the legal force and legal certainty of electronic information, electronic documents, and electronic signatures as valid evidence in electronic transactions such as e-commerce and e-business have the same legal force and legal certainty as the original. As a suggestion, in an effort to increase the effectiveness of the enactment of Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE), it is necessary to immediately issue a Government Regulation (PP) as an implementing regulation so as not to cause confusion for the community and, of course, the government itself in its law enforcement.

I. Introduction

The globalization of information has made Indonesia part of the world community, so it is necessary to establish uniform arrangements for information management and electronic transactions in various regulations to equalize perceptions, definitions, and the scope of the area of validity of the electronic transaction process at the national level to optimize, evenly, and spread information technology development. Free trade and rapid technical and industrial advances have affected many industries. Electronic transactions are

rising in banking and commerce. Cyberspace performs legal operations autonomously and inconsistently. Globalization and foreign living affect this. International social life should enhance national and international legislation[1].

Indonesia's development goals are stated in the Preamble of the Fourth Amendment to the 1945 Constitution: to protect the nation and Indonesia, promote the general welfare, educate the nation's life, and participate in a world order based on independence, lasting peace, and social justice in a complex globalized world. As stated by Mochtar Kusumaatmadja in [2], law is a means of reforming society, meaning that the existence of order in development or reform efforts is something that is desired or even considered absolutely necessary.

Changes in the law serve society, keeping it moving smoothly and fulfilling its interests. If the interests of society change, the law must be renewed, and laws that are incompatible with its duty of service must be discarded or abandoned [3]. As Alvin Toffler's opinion is quite popular, the current world changes towards the fourth wave (the present fourth wave of globalization), which brings changes in information technology advances (without any borders or distances) [4] . In the global development towards relatively high knowledge-based economic growth, Indonesia in the cyberworld (cyberspace) has become an important part of the global communication and information system [5]. The development of the world of internet technology has characteristics, including invisibility and unlimited territory, that allow everyone to communicate between countries [6]. The process of rapid legal change is required by a developing society if the change is to be carried out in an orderly manner. Since change and order are the dual aims of a growing society, the law must be used to achieve both[7].

Changes in today's society are so rapid, one of which is in the field of information technology, which is developing so sophisticatedly that only computers and telephone devices can reach the world, which has now become our

[1] Efa Laela Fakhriah, "Perkembangan Alat Bukti Dalam Penyelesaian Perkara Perdata Di Pengadilan Menuju Pembaruan Hukum Acara Perdata," *ADHAPER: Jurnal Hukum Acara Perdata* 1, no. 2 (2015): 135–53.

[2] Wahyu Nugroho and Agus Surono, "Rekonstruksi Hukum Pembangunan Dalam Kebijakan Pengaturan Lingkungan Hidup Dan Sumber Daya Alam," *Jurnal Hukum Lingkungan Indonesia* 4, no. 2 (2018): 77–110.

[3] Bambang Indra Gunawan, "Penerapan E-Mail Sebagai Bukti Elektronik Dalam Sengketa Hukum Perdata Di Indonesia," *Jurnal Lex Justitia* 2, no. 1 (2020): 1–15.

[4] Sunaryati Hartono, *Bhinneka Tunggal Ika Sebagai Asas Hukum Bagi Pembangunan Hukum Nasional* (Citra Aditya Bakti, 2016).

[5] Abdul Muis, *Indonesia Di Era Dunia Maya: Teknologi Informasi Dalam Dunia Tanpa Batas* (Remaja Rosdakarya, 2021).

[6] Tuti Andriani, "Sistem Pembelajaran Berbasis Teknologi Informasi Dan Komunikasi," *Sosial Budaya* 12, no. 1 (2016): 117–26.

[7] H Yacob Djasmani, "Hukum Sebagai Alat Rekayasa Sosial Dalam Praktek Berhukum Di Indonesia," *Masalah-Masalah Hukum* 40, no. 3 (2011): 365–74.

daily life[8]. The internet has now provided many benefits to the user community both for communication and business transactions. Information technology continues to follow such rapid development with modern facilities that it has changed the society that usually uses paper transactions (paper) to use digital (paperless). Originally, the internet was only used as the center of communication and information media, but now it can be used as a medium for trade transactions (e-commerce) by means of an agreement.

To achieve certain goals based on the evidence owned, of course, cannot be separated from who must be responsible, in this case, civil liability. E. Saefullah Wiradipradja argues that transaction activities carried out by business actors must be accountable. Responsibility is a word in the Indonesian language that has been generally used in society. Among legal experts, both practitioners and theorists, responsibility is termed "responsibility" in consideration of values and a broad sense of social justice, both from a moral and social life perspective [9]. In relation to civil liability, he argues that the modern concept of civil liability states in general that the element of fault in a person who causes harm to another person is an absolute requirement for the existence of a tort [10].

As a human invention, information technology, of course, always has weaknesses in its technical system. In addition, information technology also has uncertainties in terms of legal certainty [11]. In fact, legal theory explains that the law is a reflection of the values prevailing in society. Regarding this, Daud Silalahi argues as follows:

> *"Law, as a social rule, cannot be separated from the values that apply in a society; even the law itself is a reflection of the values that apply in society. Consequently, a good law is a law that is in accordance with the living law in society, which is also in accordance with or is a reflection of the values that prevail in that society."* [12] At present, many countries have had and made legal regulations relating to the issue of activities using information technology; for example, Singapore has had the Electronic Transaction Act 1998, the United States has had the Digital Signature Act 1999, and the European Union has had the EU Directives on

[8] Budi Rahardjo, "Pernak Pernik Peraturan Dan Pengaturan Cyber Space Di Indonesia," *Aditama, Jakarta*, 2003.

[9] H E Saefullah, "Beberapa Masalah Pokok Tentang Tanggung Jawab Pengangkutan Udara," *Bandung: Pusat Penelitian Universitas LPPM-Universitas Islam*, 2015.

[10] H.E. Saefullah Wiradpiradja, "Masalah Tanggungjawab Pengangkutan Udara Dalam Rangka Pembentukan Undang-Undang Angkutan Udara Nasional Yang Baru" (Unpad Bandung, 2019).

[11] Abdul Halim Barkatullah, *Hukum Transaksi Elektronik Di Indonesia: Sebagai Pedoman Dalam Menghadapi Era Digital Bisnis e-Commerce Di Indonesia* (Nusamedia, 2019).

[12] Daud Silalahi, SPHN VIII, and BADAN PEMBINAAN HUKUM NASIONAL, "Pembangunan Berkelanjutan Dalam Rangka Pengelolaan (Termasuk Perlindungan) Sumber Daya Alam Yang Berbasis Pembangunan Sosial Dan Ekonomi," in *Makalah Disampaikan Pada Seminar Pembangunan Hukum Nasional VIII, Tema Penegakan Hukum Dalam Era Pembangunan Berkelanjutan Diselenggarakan Oleh Badan Pembina Hukum Nasional Departemen Kehakiman Dan Hak Asasi Manusia RI Denpasar*, 2003, 14–18.

Electronic Commerce 1999. In addition to the existence of these legal regulations, it can be said that, in terms of information technology, these countries already have a certain level of maturity.

The Law on Electronic Information and Technology, specifically Article 5 paragraphs (1) and (4), establishes the legal status of electronic information and documents. Paragraph 1 states that electronic information, electronic documents, and their printouts hold validity as legal evidence. However, paragraph 4 outlines exceptions to this provision. It states that the regulations pertaining to electronic information and documents, as mentioned in paragraph (1), do not apply to letters that are required by law to be in written form, or to letters and documents that must be in the form of a notarial deed or a deed executed by specific legal procedures.

Making deeds using modern devices both in the form of hardware and software not only saves personnel costs but is also expected to produce deed products that are faster and more accurate, as stated by H. Franken. Several things are quite positive with the use of modern devices, including the means of storing texts, the ease of processing a text in making changes, the ease of compiling texts using standard texts, the ease of entering data in existing texts, administrative efficiency, the sophistication of office organization, and the speed of communication outside the office [13].

The changes that have occurred in the use of modern devices in the notary's office have not been followed by changes in the procedures for making notarial deeds, including the implementation of deeds made both in the presence and by the notary in the presence of the confrontants, who must affix their signatures, as well as the witnesses and the notary, and the implementation of the reading of the deed, where the notary must read the deed to the confrontants and witnesses. In an authentic deed, the notary guarantees the presence of (the) confronters at a certain place on a certain date if it is true that (the) confronters provide information as stated in the deed or if the circumstances mentioned in the deed have occurred and it is signed by (the) confronters. If it is to be made electronically, according to Van Esch in [14] , the information from the confronters can be made through an electronic statement with an information system; the notary cannot determine from which place the electronic statement was made, but the notary can determine where the electronic statement was received.

Article 2 of the Law on Electronic Information and Transactions states that anyone who commits a legal act, whether in Indonesia or abroad, has legal consequences and harms Indonesia. The article above states that this legislation applies to legal activities outside Indonesia by Indonesian and foreign people or legal organizations that have legal implications in Indonesia, including the use of

[13] Herlien Budiono, *Kumpulan Tulisan Hukum Perdata Di Bidang Kenotariatan* (PT. Citra Aditya Bakti, 2018).
[14] Mariam Darus Badrulzaman, *Aneka Hukum Bisnis* (PT. Alumni, Bandung, 2005).

information technology for electronic information and electricity Economic, strategic data, national dignity, defense and security, state sovereignty, persons, and legal entities are harmed by Indonesia. Protection and Legal Security System Against Digital Signature Users as Consumers in the Indonesian Legal System was the author's background study.

2. Research Method

The approach used in this research is normative-juridical, namely that the law is conceptualized as norms, rules, principles, or dogmas through national legislation, which is related to consumer digital signatures. The study specification is descriptive-analytical to describe consumer digital signature protection facts. Then analyzed in order to obtain an overview of legal protection efforts against consumer digital signatures. The research stage begins with library research to obtain primary legal materials, secondary legal materials, and tertiary legal materials. To complement library research using secondary data, this research also conducted field research, which was analyzed descriptively and qualitatively to obtain various inputs and opinions of experts and policymakers related to information technology regulation [15].

The research data collection technique is carried out by document study, using secondary data in the form of primary, secondary, and tertiary legal materials to be inventoried, studied, researched, and analyzed so that it can be used as a theoretical basis for examining primary data sources. and Data collection techniques are also carried out by interviewing resource persons with a list of questions related to agreements that use digital signatures, the results of which are used to strengthen library data. The analysis of data collected from literature studies and interviews is carried out in a qualitative, juridical manner, which is poured out in the form of descriptions and concepts based on existing regulations, and then conclusions are drawn. The research was conducted at the Faculty of Law Library, University of Bandar Lampung. Meanwhile, to obtain primary data, field research was conducted by conducting interviews with experts and policymakers related to the regulation of information technology as a resource.

3. Results and Discussion

Electronic Information and Transaction Law (ITE Law) as Cyber Law in Indonesia

ITE Law Number 11 of 2008 governs all constraints, principles, and legal norms linked to electronic information and transactions via 13 chapters and 54 provisions. The Draft Law on Information Technology (RUU IT) by the Centre

[15] Soerjono Soekanto, "Soerjono Soekanto Dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat" (Cet, 2020).

for Information Technology Law Studies, Faculty of Law, Padjajaran University, and the Draft Law on Digital Signatures and Electronic Transactions by the Institute for Law and Technology Studies, University of Indonesia, formed this legislation. The Law on Electronic Information and Transactions (ITE) binds enterprises and internet users. The enactment of this legislation is encouraging and has been long awaited by many to come out of international ostracization. Unfortunately, the public is so focused on the prohibition of internet pornography in the ITE Law (Electronic Information and Transaction Law) that they forget the essence of the ITE Law itself. The ITE Law is a daring legal product that introduces various new legal ideas that have frequently produced polemics for parties involved in electronic transactions using telecommunications media and information technology, such as the internet and computers.

The legal breakthrough ITE Law encourages the growth of information and technology (IT), industry, and the public interest to realize law's role as a social engineering instrument [16] . This law contains several matters, namely jurisdictional issues, protection of personal rights, principles of e-commerce, principles of unfair business competition and consumer protection, principles of intellectual property rights (IPR) and international law, and principles of cybercrime.

Since the enactment of the ITE Law, there has been automatic legal protection and guarantees of legal certainty and justice for the community in general and users, managers, and distributors of electronic information in particular. In connection with that, various groups in the community mention that the ITE Law is basically a cyber law that is expected to regulate all affairs of the internet (cyber) world, including giving punishment to cyber crime perpetrators, protecting the rights of individual consumers as users, regulating electronic transactions, regulating various activities carried out by the cyber space community, and so on [17].

Protection and legal security system for consumer digital signatures

In connection with the development of information technology, business transactions are increasingly taking place electronically. However, the development of information technology has also created new opportunities for crime. It has also complicated law enforcement's investigation and prosecution of the crime. Thus, irresponsible people must be prevented from accessing

[16] Muhammad Junaidi, Kadi Sukarna, and Bambang Sadono, "Pemahaman Tindak Pidana Transaksi Elektronik Dalam Undang-Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Budimas: Jurnal Pengabdian Masyarakat* 2, no. 2 (2020).

[17] Barkatullah, *Hukum Transaksi Elektronik Di Indonesia: Sebagai Pedoman Dalam Menghadapi Era Digital Bisnis e-Commerce Di Indonesia*.

electronic information. Such security is particularly important for highly private electronic information[18].

In an environment where transactions take place using paper documents, it is generally easy to overcome the problems. However, if the parties conduct their transactions paperless or based on electronic documents, the threat of the aforementioned problems becomes very great. Not only can changes made to electronic documents be made without leaving visible signs, but the documents can be "re-played" in such a way that the transaction will appear to be a bona fide transaction. In this regard, e-commerce requires a security system that can protect the parties to the transaction. The reliability of such a system should be at least equal to the reliability of the security system for paper transactions that are replaced by e-commerce systems.

The security system for electronic communications must be able to provide protection against things such as alteration, addition, or destruction by irresponsible parties of data and information, both during storage and during the transmission process by the sender to the recipient; and the actions of irresponsible parties who try to obtain confidential information, either directly from its storage or when transmitted by the sender to the recipient (eavesdropping efforts). In this regard, the electronic communication security system must accommodate security needs relating to aspects of :

1. Confidentiality

   Data confidentiality involves protecting it from unauthorized parties. Information should be protected against unauthorized outside parties, hackers, and interception or tampering while transmission over communication networks is in progress. The trick is to make the information "unintelligible" by those authorized or irresponsible. To render information "incomprehensible", the content must be altered such that without knowing the transformation process, it cannot be comprehended.
2. Integrity

   Integrity concerns data protection against efforts to modify the data by irresponsible parties, either while the data is stored or while the data is sent to other parties. The security system must be able to ensure that when the information is received by the recipient, it appears the same as when it was stored or sent. The security system that is built must make it possible to find out if the original content of the information sent has been modified, added to, or deleted. The system must also be able to prevent the information from being "re-played", For example, a fresh copy of the data is sent again using the authorization that was originally used when the original message was sent.
3. Authorization

[18]Mariam Darus Badrulzaman, *Aneka Hukum Bisnis*.

Authorization concerns the monitoring of access to certain information. Certain transactions may only be accessible by certain parties, while other transactions are not. Authorization is intended to limit actions by parties who are not authorized to do something within the information network environment. These restrictions depend on the security level of the party concerned. This limitation concerns the extent to which a party authorized to access said matter is authorized to do the following enter data or information, reading data or information, modify, add, or delete data or informationd. Export or import data or informatione. Print data or information.

4. Availability

   Information stored or transmitted through communication networks must be available at any time if needed. The protection system must be able to prevent the occurrence of causes that could hinder the availability of the required information. Operational errors, errors related to the application of the software used (software application), problems involving hardware (hardware problems), and viruses are some of the reasons that can make the required information unavailable when needed.

5. Authenticity

   The capacity of a person, organization, or machine to authenticate the identity of the information owner is called authentication. All parties involved in a transaction must feel safe and certain that the communication that occurs through the network between the parties is correct; that is, it is true that the parties are dealing with the parties that are actually desired and correct regarding the information exchanged between them.

6. Non-repudiation of origin or non-repudiation

   Non-repudiation of origin or non-repudiability protects a party who subsequently rejects a transaction or communication activity. Non-repudiation systems must authenticate data authenticity and delivery to an impartial third party.

7. Auditability

   The data must be recorded in such a way that all the necessary confidentiality and integrity requirements have been fulfilled, namely that the transmission of the data has been encrypted by the sender and decrypted by the recipient as appropriate.

Cryptography provides the security specified above. The Oxford Advanced Learner's Dictionary defines cryptography as "the art of writing or solving codes"—ciphers. Cryptography involves encryption and decryption. Encryption is the process of making information unintelligible to unauthorized readers. Decryption is the process of reversing the encryption so that the information can be read again. Traditionally, cryptography is performed by the sender using a secret code or secret key to encrypt the information. Using the same secret code

or secret key, the recipient of the information decrypts it. There are two types of cryptography systems, namely the symmetric system, also called the secret key cryptosystem, based on a single secret key used by both parties, namely the sender uses the key to encrypt (encryption) while the recipient uses the key to decrypt (decryption), and the asymmetric cryptosystem, also called the public key cryptosystem, which is based on the use of a pair of keys. The two keys are the private key and the public key.

In the life of transactions that use paper (paper-based transactions), as we have known so far, in many cases the documents used for transactions are signed by, for, or on behalf of the parties to the transaction. The main purpose of affixing the signature is to prove that the document really originates from or has been approved by the person who affixes the signature (one of whom is a consumer). After the advent of computers and the internet, a problem arose: how can the parties involved in e-commerce transactions affix their respective signatures as authentication of the electronic documents created between them. Could there be a way for the parties to replace the signature function on paper when they carry out their transactions electronically. Implementation of solutions to security problems in the field of information technology, as stated above, and solving the problem of affixing signatures to electronic documents in e-commerce transactions are solved by using cryptography techniques as described above. In addition to securing it by encrypting the message sent, the sender can also include a digital signature from the sender of the message in question along with the message itself.

The word "signature" in this context is very misleading. A signature in this context is not a "digitized image of a handwritten signature". It is not a signature that is affixed by a person with his or her hand to paper documents, among other things, as is commonly done. A digital signature is obtained by first creating a message digest, or hash, which is a mathematical summary of the document to be sent through cyberspace. The inclusion of a digital signature on an electronic document by the sender is to provide more certainty to the recipient regarding the authentication of the sender of the electronic document. Thus, the recipient of the electronic document or message is not uncertain about who the actual sender of the electronic document or message is.

The function of a digital signature is the same as that of a person's fingerprint. A digital signature is a tool to identify a message that is sent. In other words, the affixing of a digital signature, in addition to aiming to ensure that the message is not sent by someone else but indeed sent by the sender in question, also aims to be used as legally strong evidence that the contents of the message that has been sent by the sender have been approved by the sender. The RSA algorithm is commonly used for digital signatures. Digital Signature Algorithm (DSA), developed by the US National Institute of Standards and Technology, is also

popular. DSA offers different security properties than RSA, although their implementation methods are comparable.

Making a digital signature goes through two stages. The first stage is to create a message digest, and the next stage is to encrypt the message digest with the sender's private key. Meanwhile, to verify the digital signature, one must ensure that the digital signature is indeed proof of the identity of the actual sender of the message, meaning that it was not someone else who sent the message. Because digital signatures are created using the original text of the message sent as input for the encryption algorithm used, if the message is changed, even if only a few changes are made, it is impossible to decrypt the digital signature correctly. If the results of the decryption are incorrect, it means that the message has been modified at the time of sending, knowing that the digital signature has been forged by copying the digital signature from one message to another. In using a digital signature, there are two parties: the certificate authority (CA) and the subscriber (consumer). This relationship shows the link between the CA as a service provider and the subscriber as a consumer. As a service provider, CA must guarantee the rights of subscribers (consumers), including: [19] 1. Privacy

CA, as a data provider, is obliged to maintain the confidentiality of subscriber (consumer) identities from unauthorized parties. The CA may only confirm that the certificate owned by the subscriber (consumer) is correct and is recognized by the CA. In several developed countries, personal data is protected by law (the Data Protection Act). The law in question contains data protection principles that must be obeyed by people who store or process information using computers that concerns people's lives and computer bureaus that provide services for those who wish to The processing of information is similarly controlled and is subject to registration according to the law. Individuals whose personal information is stored on a computer are given rights of access and rights to obtain records for correcting and deleting incorrect information. They can also file a complaint with the Data Protection Register (which is appointed by law) if they are not satisfied with the way people or organizations collect information, and according to certain circumstances, individuals (consumers) have the right to compensation.

Adequate security measures must be taken against unauthorized access to, alteration, distribution, or destruction of personal data, as well as against unexpected loss of personal data. An individual (consumer) will be given the right to:

a. Within a reasonable period of time without delay and without charge; given an explanation by the data user about whether his party controls personal data where the individual (consumer) concerned becomes the

[19] Ahmad M Ramli, "Cyber Law Dan Haki: Dalam Sistem Hukum Indonesia," 2014.

data subject; and for access to such data that is controlled by the data user.

b. If deemed necessary, correct or delete the data.

The last principle relates to safeguards, and threats to this are of two types:

a. security from unauthorized access; and
b. With regard to copy backups, data centers containing personal (consumer) data

Still related to the issue of guaranteeing privacy in relation to private keys is the requirement that there be a guarantee that the CA does not try to find the public key pair from the subscriber (consumer). The CA has a great chance of being able to find the pair key from the subscriber (consumer) because the CA has a more sophisticated computer to find it. In addition, there must be a guarantee that the creator of the card containing the private key will not share or duplicate it. This is very logical because the card maker, besides knowing the public key, also knows the private key because he is the creator. To guarantee this, it is necessary to have a notary system that guarantees it.

2. Accuracy

This principle contains the notion of "accuracy" between what is requested and what is obtained. That what the subscriber (consumer) gets is in accordance with what he asks for based on the information he receives. Accuracy of information (correct information without deception) is also a principle of accuracy.The CA is also obliged to provide all information related to the offer or request submitted to the subscriber (consumer). Indirectly, the subscriber (consumer) has the right to obtain a licensed CA, which means that when the subscriber (consumer) accesses the CA, there is a presumption that the CA is a legitimate and licensed CA, and the subscriber (consumer) must be protected from fraudulent CA deviations.

3. Property

Subscribers (consumers) must be protected from any irregularities that may occur due to their entry into this system. This means that the subscriber (consumer) has the right to be protected from all forms of tapping, copying, and theft. If this happens, the CA is obliged to compensate the loss suffered by the subscriber (consumer).

4. Accessibility

Every individual is entitled to equal treatment in terms of access and information. This means that every subscriber (consumer) can enter this system if they fulfill the requirements, and they can use this system without any obstacles. Subscribers (consumers) also have the right to have their opinions and complaints heard.

In relation to the use of digital signatures, CAs in a stronger position should be able to guarantee the rights of subscribers (consumers). Especially in

the adhesion agreement between CA and the subscriber (consumer). The proposed agreement should not be one-sided, so that the subscriber (consumer) has no bargaining power. To cover the risk of defective products, the CA can insure the risk. This is to reduce the burden that must be borne by the CA if one day there is a subscriber (consumer) who sues the CA because he feels harmed.

4. Conclusion

Since the enactment of Law Number 11 of 2008 on Electronic Information and Transactions (ITE), the legal force and legal certainty of electronic information, electronic documents, and electronic signatures as valid evidence in electronic transactions such as e-commerce and e-business have the same legal force and legal certainty as the original. However, this legislation is still in the form of basic norms, and to elaborate its implementation, Government Regulation (PP) is required, which needs to be harmonised with Government Regulation (PP) supporting the implementation of Law Number 36 of 1999 on Telecommunication. As a suggestion in an effort to increase the effectiveness of the enactment of Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE), it is necessary to immediately issue a Government Regulation (PP) as an implementing regulation so as not to cause confusion for the public and, of course, the government itself in law enforcement.

Refrences

Andriani, Tuti. "Sistem Pembelajaran Berbasis Teknologi Informasi Dan Komunikasi." *Sosial Budaya* 12, no. 1 (2016): 117–26.

Barkatullah, Abdul Halim. *Hukum Transaksi Elektronik Di Indonesia: Sebagai Pedoman Dalam Menghadapi Era Digital Bisnis e-Commerce Di Indonesia*. Nusamedia, 2019.

Budiono, Herlien. *Kumpulan Tulisan Hukum Perdata Di Bidang Kenotariatan*. PT. Citra Aditya Bakti, 2018.

Djasmani, H Yacob. "Hukum Sebagai Alat Rekayasa Sosial Dalam Praktek Berhukum Di Indonesia." *Masalah-Masalah Hukum* 40, no. 3 (2011): 365–74.

Fakhriah, Efa Laela. "Perkembangan Alat Bukti Dalam Penyelesaian Perkara Perdata Di Pengadilan Menuju Pembaruan Hukum Acara Perdata." *ADHAPER: Jurnal Hukum Acara Perdata* 1, no. 2 (2015): 135–53.

Gunawan, Bambang Indra. "Penerapan E-Mail Sebagai Bukti Elektronik Dalam Sengketa Hukum Perdata Di Indonesia." *Jurnal Lex Justitia* 2, no. 1 (2020): 1– 15.

H.E. Saefullah Wiradpiradja. "Masalah Tanggungjawab Pengangkutan Udara Dalam Rangka Pembentukan Undang-Undang Angkutan Udara Nasional Yang Baru." Unpad Bandung, 2019.

Hartono, Sunaryati. *Bhinneka Tunggal Ika Sebagai Asas Hukum Bagi Pembangunan Hukum Nasional*. Citra Aditya Bakti, 2016.

Junaidi, Muhammad, Kadi Sukarna, and Bambang Sadono. "Pemahaman Tindak Pidana Transaksi Elektronik Dalam Undang-Undang No 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik." *Budimas: Jurnal Pengabdian Masyarakat* 2, no. 2 (2020).

Mariam Darus Badrulzaman. *Aneka Hukum Bisnis*. PT. Alumni, Bandung, 2005.

Muis, Abdul. *Indonesia Di Era Dunia Maya: Teknologi Informasi Dalam Dunia Tanpa Batas*. Remaja Rosdakarya, 2021.

Nugroho, Wahyu, and Agus Surono. "Rekonstruksi Hukum Pembangunan Dalam Kebijakan Pengaturan Lingkungan Hidup Dan Sumber Daya Alam." *Jurnal Hukum Lingkungan Indonesia* 4, no. 2 (2018): 77–110.

Rahardjo, Budi. "Pernak Pernik Peraturan Dan Pengaturan Cyber Space Di Indonesia." *Aditama, Jakarta*, 2003.

Ramli, Ahmad M. "Cyber Law Dan Haki: Dalam Sistem Hukum Indonesia," 2014.

Saefullah, H E. "Beberapa Masalah Pokok Tentang Tanggung Jawab Pengangkutan Udara." *Bandung: Pusat Penelitian Universitas LPPM-Universitas Islam*, 2015.

Silalahi, Daud, SPHN VIII, and BADAN PEMBINAAN HUKUM NASIONAL. "Pembangunan Berkelanjutan Dalam Rangka Pengelolaan (Termasuk Perlindungan) Sumber Daya Alam Yang Berbasis Pembangunan Sosial Dan Ekonomi." In *Makalah Disampaikan Pada Seminar Pembangunan Hukum Nasional VIII, Tema Penegakan Hukum Dalam Era Pembangunan Berkelanjutan Diselenggarakan Oleh Badan Pembina Hukum Nasional Departemen Kehakiman Dan Hak Asasi Manusia RI Denpasar*, 14–18, 2003.

Soekanto, Soerjono. "Soerjono Soekanto Dan Sri Mamudji, Penelitian Hukum Normatif Suatu Tinjauan Singkat." Cet, 2020.