JURNAL ILMIAH DUNIA HUKUM
Volume 7 Issue 2 April 2023
ISSN Print: 2528-6137 | ISSN Online: 2721-0391

Legal Politics of Electronic Documents in State Finances As Legal Evidence

Rizky Dian Bareta[1], Triyono[2], Rahmat[3]
[1] *Directorate General of Treasury, Ministry of Finance*
[2] *Computer Science, The Pennsylvania State University*
[3] *Leiden Law School, Leiden University*

* *Correspondence e-mail: qq.bareta@gmail.com*

Submission
2022-Oct-31
Review
2022-Dec-12
Accepted
2023-Apr-13
Publish
2023-Apr-27

Abstract

Disruption of digital technology as part of the industrial revolution 4.0 forces changes in human culture to keep up with the times, including in public institutions. Regulating the digitalization of state finances has risks, including electronic evidence in court that is very likely to occur, given that corruption in state finances is still rampant, requiring legal evidence in court. This research is normative research by examining the existence of regulations related to electronic documents in state finances and explaining how electronic documents are formed. In this study, it can be concluded that regulations regarding electronic evidence have been adequately accommodated, although there is still an asymmetry in the classification of electronic evidence itself. Regulations governing electronic documents in the field of state finances still refer to laws regarding electronic information and transactions. These regulations are considered complete, although, in several regulations in the field of state finance, adjustments are still required to support the use of electronic documents in state finances. Electronic signatures are divided into certified and uncertified signatures, but certified signatures make the presence of an ideal electronic document. This research can be used as input for policymakers in implementing electronic documents in state finance.

Keywords: *electronic documents; state finances; electronic signature; electronic evidence; corruption*

How to Cite: Bareta, Rizky Dian, Triyono, Rahmat. "Legal Politics of Electronic Documents in State Finances As Legal Evidence" Jurnal Ilmiah Dunia Hukum Vol. 7, No. 2 (2023).

1. Introduction

State Finance, according to Law Number 17 of 2003 are all rights and obligations of the state that can be valued in money, as well as everything either in the form of money or in the form of goods that the state can own in connection with the implementation of these rights and obligations.

Meanwhile, in some literature, it is stated that state finances are wealth managed by the government, which includes money and goods owned; owned valuable paper; rights and obligations that can be valued in money; third-party funds collected based on potential owned and/or guaranteed by either the

central government, regional government, business entities, foundations or other institutions.[1]

State finances are closely related to corruption because corruption is always based on state financial losses. The crime of corruption is a crime that is regulated by a separate law, namely Law Number 31 of 1999, in conjunction with Law Number 20 of 2001. Because of this, corruption is classified as a special crime, namely crimes regulated outside the Criminal Code.[2]

Corruption, according to Law Number 31 of 1999 juncto Law Number 20 of 2001, means that everyone who unlawfully commits an act of enriching himself or another person or a corporation that can harm state finances or the country's economy.

In the general Indonesian dictionary by Pius A. Partanto and M. Dahlan Al Bahrry, corruption is defined as a bad act such as cheating, fraud, abuse of office for self-interest, and is easily bribed.[3]

Sayed Hussein Alatas's book "Corruption and the Disting of Asia" states "that actions that can be categorized as corruption are bribery, extortion, nepotism, and abuse of trust or position for personal gain."[4]

There is no clear definition of electronic evidence in the law. Still, it is explained in Law Number 11 of 2008 concerning Electronic Information and Transactions that activities through electronic media systems, also called cyberspace, even though virtual, can be categorized as a real legal action or act. Juridically, activities in cyberspace cannot be approached with conventional legal standards and qualifications because if this method is followed, there will be too many difficulties and things that escape law enforcement. Activities in cyberspace are virtual activities that have a genuine impact even though the evidence is electronic.

Electronic documents based on Article 1 number 4 of Law Number 11 of 2008 concerning Information and Electronic Transactions are stated as any Electronic Information that is created, forwarded, sent, received, or stored in analog,

---

[1]Sahya Anggara, *Administrasi Keuangan Negara* (Bandung: CV Pustaka Setia, 2016).
[2]Suhendar Suhendar, "Penyidikan Tindak Pidana Korupsi Dan Kerugian Keuangan Negara Dalam Optik Hukum Pidana," *Pamulang Law Review*, 2019, https://doi.org/10.32493/palrev.v1i1.2849.
[3]Suherman, "Pola Mutasi, Reward & Punishment vs Fraud," *Djkn*, 2017.
[4]Suhendar Suhendar and Kartono Kartono, "Kerugian Keuangan Negara Telaah Dalam Perspektif Hukum Administrasi Negara Dan Hukum Pidana," *Jurnal Surya Kencana Satu : Dinamika Masalah Hukum Dan Keadilan*, 2020, https://doi.org/10.32493/jdmhkdmhk.v11i2.8048.

digital, electromagnetic, optical, or the like, which can be seen, displayed, and/or heard through a Computer or Electronic System, including but not limited to writing, sound, pictures, maps, designs, photos or the like, letters, signs, numbers, Access Codes, symbols or perforations that have meaning or significance or can be understood by people who are able to understand it.

Changes in the world in the industrial revolution 4.0 caused quite significant changes in the life of society, nation and state. The invention of the internet itself became the main driving factor of globalization. Globalization has made various developments and advances in the world of technology and information rapid, as evidenced by the massive advances in communication technology, driving changes that occur as a whole, are felt collectively, and affect many people so that they affect our lifestyle and the environment around us.[5]

The internet is predicted to be one of the main driving forces in various aspects of life, including the economic aspect. The main reason that the internet can become a driving force is its function which provides convenience in conducting transactions, especially financial transactions.[6] Even though the internet, words can simultaneously affect a global economy.[7]

The culture of using information technology then penetrates governance. It has been proven that information technology-based government services emerged, such as online passports, the People's Online Aspirations and Complaints Service (LAPOR) and so on. Government services in state finance are no exception, such as the State Revenue Module, the State Treasury and Budget System, and most recently, the Institutional Level Financial Application System.

The COVID-19 pandemic in early 2020 forced the Government to accelerate the use of information technology further and increase the dependence on information technology, even though the goals were more or less the same as the previous goals. The COVID-19 pandemic has made information technology very important.[8] This is evidenced by virtual meeting rooms and cloud computing, which makes it possible to maintain the productivity of workers who work from home in carrying out their work and in the learning process

[5] Ashad, *Teori Modernitas Dan Globalisasi* (Sidoarjo: Kreasi Wacana, 2014).
[6] A Raharjo, *Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, *Citra Aditya Bakti*, 2002.
[7]John Naisbitt, "Global Paradox: The Bigger the World Economy, the More Powerful Its Smallest Players," *Choice Reviews Online*, 1994, https://doi.org/10.5860/choice.31-5537.
[8]Rita Komalasari, "Manfaat Teknologi Informasi Dan Komunikasi Di Masa Pandemi Covid 19," *TEMATIK*, 2020, https://doi.org/10.38204/tematik.v7i1.369.

used by students who do school from home. Several regions launching information technology-based innovations, such as West Java, launched Sambara as a motor vehicle tax administration. This information system has been used since 2018. The COVID-19 pandemic has had a very significant impact on the use of this application.[9]

More broadly, state finances cannot be separated from corruption and state losses. The 2020 Indonesian Corruption Perceptions Index (CPI) released by Transparency International (Transparency International, released 28 January 2021) places Indonesia in 102nd place out of 180 countries in the world with a score of 37 points out of 100 points. Of the 31 countries in the Asia Pacific region, the average score is 45 points out of 100 points. Indonesia has made improvements, so there has been an increase of 5 points since 2012. However, this does not necessarily indicate that Indonesia is getting cleaner from corruption. Transparency International stated in a release that there were no significant developments in handling anti-corruption in the Asia Pacific.[10]

There are still many corruption cases in Indonesia, which means that the state financial sector will often be in contact with the law in a corruption trial. In a criminal case trial, especially corruption, there must be proof that someone can be found guilty. With the use of information technology, especially concerning electronic documents on state finances, its use will undoubtedly be possible to be confronted in a corruption trial as legal evidence.

State finances have not yet adopted electronic documents, so in criminal courts adjudicating corruption cases, until now, electronic documents have not been used as evidence. However, in criminal trials, electronic evidence has been massively used. This is because there is still a legal vacuum for using electronic documents in state finances.

Two legal systems are predominantly adhered to in the world, namely Civil Law and Common Law. The legal system adopted by countries in Continental Europe is based on Roman law called the Civil law system. The Civil Law system has several characteristics, including codification, and independent

[9]Sri Fitria Mulyadi, Dadan Kurniansyah, and Made Panji Teguh Santoso, "Implementasi Penerapan Aplikasi Sambara Dalam Administrasi Wajib Pajak Pada Masa Pandemi Covid-19 Di Kabupaten Karawang," *Jurnal Ilmu Pemerintahan Suara Khatulistiwa*, 2021, https://doi.org/10.33701/jipsk.v6i2.1887.

[10]Adi Heryadi, Ilham B Tarigan, and Weni Astuti, "Memahami Indeks Persepsi Korupsi (IPK) Indonesia Dan Kontribusi Polisi Militer Untuk Meningkatkan IPK," *DHARMA BAKTI*, 2022, https://doi.org/10.34151/dharma.v5i1.3928.

judges, so that laws become the primary source of law, and the judicial system has an inquisitorial nature. [11]

Indonesia adheres to civil law so that laws and regulations become the supreme commander in a civil law adherent country. Based on the rules of law and regulations, it is realized that legal developments will always lag behind technological developments. Because of this, the adage "Het Recht In Achter de Feiten Aan" emerges, meaning that "the law is always teetering behind events or events that appear in real society."[12]

In several previous studies, the existence of formal requirements for electronic documents has been examined, one of which is research entitled The Power of Proofing Electronic Information Evidence in Electronic Documents and Their Printed Results in Proof of Crimes, explained by Nur Laili Isma and Arima Koyimatun, which discusses the power proving electronic information evidence on electronic documents and their printed results in proving a crime. This research is a normative juridical research in which it is concluded that the position of electronic information evidence and electronic documents and their printed results is an extension of documentary evidence and instructions based on Article 184 of the Criminal Procedure Code. In criminal procedural law, there is no hierarchy of evidence, but the existence of electronic information evidence and electronic documents must clearly explain a criminal case.[13] Another study conducted by Johan Wahyudi discussed Electronic Documents as Evidence in Proof in Court. This study demonstrates the legal relationship between legal subjects through the internet media. This legal relationship has a reasonably high legal risk, so it is necessary to have clear rules of the game in carrying out legal relations between legal subjects through the internet media. This is accommodated in the ITE Law.[14]

There are formal and material requirements for the use of electronic documents. This study examines the legal politics of using electronic documents in state finances from a formal and material perspective.

---

[11]Fajar Nurhardianto, "Sistem Hukum Dan Posisi Hukum Indonesia," *Jurnal Tapis*, 2015.
[12]Romli Atmasasmita, *Hukum Kejahatan Bisnis Teori Dan Praktik Di Era Globalisasi* (Jakarta: Prenadamedia Group, 2014).
[13]Arima Isma, Nur Laili; Koyimatun, "Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana," *Jurnal Penelitian Hukum*, 2014.
[14]Johan Wahyudi, "Dokumen Elektronik Sebagai Alat Bukti Pada Pembuktian Di Pengadilan," *Perspektif*, 2012, https://doi.org/10.30742/perspektif.v17i2.101.

2. Research Method

This study used qualitative research methods. This type of research is grounded theory which is explained in an analytical descriptive form where the research gives an overview of the state of the object under study. This research is normative legal research. In general, the problem approach used in writing normative legal research consists of 5 (five) approaches, namely the statutory approach, conceptual approach, historical approach, case approach, and comparative approach.[15] Meanwhile, in this study, the statutory approach was used. The statutory regulation approach is carried out to examine interrelated regulations to analyze their suitability and consistency.[16] This conceptual approach is used to clarify the ideas contained in laws and regulations.[17]

This study's data types include primary legal sources from statutory regulations and court decisions. Primary sources of law that are mainly used are those that regulate state finances, sources of law that handle information and electronic transactions, and laws that regulate evidence. Secondary legal sources that explain primary legal sources are taken from articles, magazines, and literature books. Tertiary legal sources are taken from legal and language dictionaries, which can explain primary and secondary legal sources.

3. Research Results and Discussion

Indonesia is one of the countries that adhere to civil law, so that law becomes the main foundation in the life of the nation and state. This has been emphasized in Article 1, paragraph (3) of the Constitution of the Republic of Indonesia, which states that "Indonesia is a state based on law". Therefore the formation of law must be responsive to changes that occur in society, one of which is to accommodate changes in the use of technology and the behavior of its users. However, in the formation of law, of course, it cannot be separated from the rules that have been determined, including the rules of non-contradiction and the principle of integrity. In the logic of law science, the principle of non-contradiction is known, which means that one legal rule and another must be synchronous and harmonious and not contradictory (principle of integrity).[18]

---

[15]S Soekamto and S Mamudji, *Penelitian Hukum Normatif (Suara Tinjauan Singkat)*, *Jakarta: Rajawali Pers*, 2015.
[16]S Nasution, "Metode Penelitian," *Jakarta: Rineka Cipta*, 2002.
[17]Bahder Johan Nasution, "Metode Penelitian Ilmu Hukum," in 2, 2016.
[18]Munir Fuadi, *Teori-Teori Besar Dalam Hukum (Grand Theory)*, *Kencana Prenadamedia Group*, 2014.

3.1. Legal politics of electronic documents as legal evidence in court

State finances have arrangements in the package of state finance laws, namely Law Number 17 of 2003, Law Number 1 of 2004, and Law Number 15 of 2004. The package of laws on state finance contains guidelines in the form of flowcharts. The standard state finances start at the planning, implementation, and accountability stages of state finances. However, no single substance in the laws on state finances regulates legal evidence if there is a case related to state finances. The existence of the *Lex Specialis derogate legi Generalis* rule of law means that specific laws take precedence over general laws, causing the rules governing legal evidence in state financial fraud to be regulated in the lex specialis, which regulates criminal law, namely the Criminal Code.

The proof attempts to convince the judge to examine the case to obtain certainty about the truth of a legal event.[19] At the same time, the purpose of the proof is to describe an event so that the truth is obtained.[20]

In proving there are several proof systems, among others:[21]

a. The evidentiary system is based on positive law;
b. The evidentiary system is based solely on the conviction of the judge; and
c. The evidentiary system is based on the judge's conviction for logical reasons.

Article 184 of Law Number 8 of 1981 concerning the Criminal Procedure Code indicates that the evidence is valid. Article 184, paragraph (1) of the Criminal Procedure Code states that valid evidence is:

a. Witness statement;
b. Expert testimony;
c. Letters;
d. Hints;
e. Defendant's testimony.

Article 164 HIR states the means of evidence: written evidence, witness evidence, presumptions, confessions, and oaths. The provisions of the

[19]Dkk Imron, *Hukum Pembuktian*, *Jurnal Hukum & Pembangunan*, 2017.
[20]Martiman Prodjohamidjojo, *Komentar Atas KUHAP: Kitab Undang-Undang Hukum Acara Pidana* (Jakarta: Pradnya Paramitha, 1984).
[21]Chella Maiyuni, "KUHP," *Journal of Chemical Information and Modeling*, 2013.

Criminal Code and the Civil Code grammatically do not mention electronic evidence's existence.

One of the electronic pieces of evidence is electronic documents. Electronic documents have been regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions. Special arrangements regarding electronic documents are regulated in 1 chapter, namely Chapter III, Information, Documents and Electronic Signatures, which contains 8 Articles starting from Article 5 to Article 12.

Article 5 and elucidation to Article 5 of the ITE Law regulate electronic documents as legal evidence. This article stipulates that electronic documents and/or printouts are valid legal evidence before a court as an extension of the procedural law in force in Indonesia, both civil, criminal and administrative procedural law. However, electronic documents do not apply to legally regulated documents and must be in written form and for notary deeds or deed-making officials.

Several laws, for example, the Company Documents Law, the Terrorism Law, the Corruption Eradication Law, and the Money Laundering Law, regulate electronic evidence.

Arrangements for evidence in Law Number 20 of 2001 concerning Amendments to Law Number 31 of 1999 concerning the Eradication of Corruption Crimes explained that electronic evidence is an extension of Article 188 of Law Number 8 of 1981 into Article 26A. Article 188 of the Criminal Procedure Code explains the evidence indicating the various evidence listed in Article 184. This means that electronic evidence can be used, but only as evidence. The provisions in Article 188 of the Criminal Procedure Code, which place electronic evidence as directive legal evidence, give power to judges to use their subjectivity. If electronic documents are used as evidence, there is still legal uncertainty.

In 2020, through Law Number 11 of 2020, the DPR passed the Omnibus Law on the Job Creation Law, which provides regulations regarding electronic documents regarding changes to Law Number 30 of 2014 concerning Government Administration. However, later a contradiction arose between the Corruption Law and the Job Creation Law concerning the position of electronic evidence as a piece of legal evidence; where the Corruption Law classifies electronic evidence as a guide, the Job Creation Law provides equal legal force between electronic and written decisions.

So that it can be interpreted that electronic documents, according to the Job Creation Law, are equated with documentary evidence as explained in Article 187 of the Criminal Procedure Code. This has significant implications for the strength of legal evidence.

Electronic evidence in court has not been explicitly regulated, causing legal uncertainty at trial, even though the use of electronic evidence in society has been massive. Differences of opinion regarding electronic evidence have been debated for a long time. Even in 2016, Setya Novanto questioned the statement of electronic evidence as contained in the ITE Law. The problem was then poured into Constitutional Court Decision Number 20/PUU-XIV/2016. This decision later became one of the backgrounds and one of the materials included in the amendments to the ITE Law in 2016.

Indonesia indeed adheres to the concept of Civil Law where the judge's decision is independent based on the applicable provisions and does not recognize jurisprudence in legal decisions. However, in its development, there is a legal vacuum or multiple interpretations of law, so there is the possibility of using jurisprudence, with conditions:[22]

a. Decisions on an event whose law is not yet clearly regulated in legislation;
b. The decision must already be a permanent decision;
c. It has been repeatedly decided with the same decision in the same case;
d. Fulfills a sense of justice;
e. The Supreme Court justified the decision;
f. Contains *obiter dicta* and *ratio decidendi*.

This jurisprudence can be deemed necessary and can be a way out of confusing arrangements, but this jurisprudence can only be used as a guide for judges. So that with this jurisprudence, it is hoped that there will be no disparities in legal decisions and treatment of electronic evidence, one of which is regarding the use of electronic evidence. Until now, there has been no precise regulation regarding its use.

[22]Center for Legal and Judicial Research and Development of the Supreme Court of the Republic of Indonesia, *Kedudukan Dan Relevansi Yurisprudensi Untuk Mengurangi Disparitas Putusan Pengadilan* (Jakarta: Puslitbang Hukum dan Peradilan MA RI, 2010).

3.2. Legal politics of electronic documents in state finances

The package of state finance laws, Law No. 17/2003 on State Finance, Law No. 1/2004 on State Treasury and Law No. 15/2004 on Audit of State Financial Management and Responsibility, does not regulate state finance technology. The package of laws regulates concepts and business processes in state finance following the state financial cycle from planning to accountability.

In 2008, Law Number 11 of 2008 concerning Information and Electronic Transactions allowed state finances to use electronic documents. This regulates the existence of electronic documents and their legal requirements as legal evidence.

Article 5, Article 6, and Article 7 of the ITE Law also regulate the requirements for electronic documents, including the use of an electronic system that follows the provisions and document information that can be accessed, displayed, guaranteed for its integrity, and can be accounted for. Article 10 of the ITE Law provides reliability certification requirements for business actors conducting electronic transactions. Neither in this ITE Law nor in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 Concerning Information and Electronic Transactions do not mention the definition of a business actor, nor is the definition of a business actor found in the Big Indonesian Dictionary. However, when referring to Law Number 7 of 2014 concerning Trade, "Business Actors are every individual Indonesian citizen or business entity in the form of a legal entity or not a legal entity that is established and domiciled within the jurisdiction of the Unitary State of the Republic of Indonesia that carries out business activities in Commerce." This can be interpreted if the government, as the organizer of electronic transactions, is not obliged to have a reliability certificate.

Articles 11 and 12 of the ITE Law provide regulations regarding electronic signatures. Article 1 point 12 of the ITE Law states, "Electronic Signature is a signature consisting of Electronic Information attached to, associated with or related to other Electronic Information that is used for verification and authentication." Article 11 of the ITE Law explains that electronic signatures have legal force if certain conditions are met. There are 6 (six) conditions as described in Article 11 paragraph (1) of the ITE Law. Still, in general, the conditions require that an electronic signature is valid if it

guarantees the data integrity of electronic documents. Article 12 of the ITE Law regulates the security of electronic signatures.

Strengthening the ITE Law in the context of digitization in the public or government domain, Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems has been established. Generally, it is explained that the principles in SPBE are effectiveness, integration, continuity, efficiency, accountability, interoperability and security. In connection with secure electronic documents, the security principles are explained in the form of confidentiality, integrity, availability, authenticity, and undeniability (*nonrepudiation*).

At the level of implementation of legal politics, the provisions for electronic signatures in the ITE Law are regulated through Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. The PP was repealed and replaced with Government Regulation Number 71 of 2019 concerning Electronic Systems and Transactions (PSTE) implementation. PP PSTE provides several more detailed arrangements regarding electronic signatures. The Law and PP do not offer formal requirements for certificates in electronic signatures but provide material requirements regulated in Article 11 of the ITE Law and Article 59 of PP PSTE, explaining that electronic seals are included in the scope of electronic signatures used by business entities. Electronic signatures have legal force and legal consequences as long as they meet the requirements:

a. Electronic signature creation data is only related to specific signers;
b. The electronic signature creation data is in the power of the authorized signatory;
c. The authorized signatory knows changes to electronic signatures;
d. The integrity of electronic information related to electronic signatures can be maintained;
e. There is a way to identify the signer; and
f. There is a sign that the signatory has given consent.

Article 60 PP PSTE stipulates that electronic signatures serve as identity and maintain the integrity of electronic information. Electronic signatures are divided into certified electronic signatures and non-certified electronic signatures. A certified electronic signature is an electronic signature made by an Indonesian electronic certificate provider service and made using an

electronic certifying device and fulfilling the requirements for the validity of an electronic signature.

An uncertified electronic signature is only explained by an uncertified electronic signature that does not use the services of an electronic certificate provider in Indonesia. The legal consequences are in the form of a different proof strength compared to a certified electronic signature. This provision does not provide further regulation of uncertified electronic signatures. This means that non-certified electronic signatures are legally recognized with a different legal proof value from certified electronic signatures. In addition to the strength of proof, an uncertified electronic signature must also fulfill the requirements stated in Article 59, paragraph (3) PP Number 71 of 2019. The fulfillment must supplement these requirements:

a. Electronic time service (Article 67 paragraph (3));
b. Registered electronic delivery service (Article 69 paragraph (4));
c. Website authentication (Article 71 paragraph (5)); and
d. Preserving electronic signatures and/or seals (Article 72 paragraph (3)).

This means that electronic documents as valid legal evidence do not have formal requirements for electronic signature certification, but the requirements contained in the Law and PP are material for electronic signatures as part of electronic documents.

Tracing from several statutory provisions regarding electronic documents, it was later found arrangements regarding electronic documents in Law Number 30 of 2014 concerning Government Administration. Chapter VII of the Implementation of Government Administration states that an electronic decision is contained in 1 (one) article, namely Article 38. The article and the explanation of the article regulate the recognition of electronic decisions so that these decisions are valid and have the same legal force as written decisions. The procedure for using electronic decisions refers to the ITE Law. However, if there is a difference between an electronic and a written decision, the written decision shall prevail. The exception for decisions in electronic form are decisions that result in a burden on state finances. This means that in state finances, decisions of treasury officials must be in written form so that the possibility of using

electronic documents in state finances is closed since the presence of the Law on Government Administration.

However, Article 38 has been amended through Law Number 11 of 2020 concerning Job Creation. The amendment to Article 38 of the Law on Government Administration stipulates that the legal force of decisions is electronic, equating with the legal force of written findings. It is also regulated that if decisions are made electronically, written choices are no longer made. This is regulated to maintain legal certainty over the decision, so there is no longer a dualism of decisions. The regulation that prohibits decisions in electronic form for decisions that burden state finances is no longer regulated. This gives fresh air to state finances that the use of electronic documents in state finances is no longer limited.

What is of concern is that the Job Creation Law is only 2 (two) years old with the Constitutional Court's Decision regarding the Formal Test for the Job Creation Law (Decision Number 91/PUU-XVIII/2020), with points in the form of:

1. Declare the "Formation Process" of the Job Creation Bill to be unconstitutional, but this law will remain in effect until the law is changed 2 (two) years after the decision (25 November 2023).
2. If by 25 November 2023, the new law has not been made, then the current Job Creation Law will no longer be valid, and everything that the Job Creation Law has amended will become valid again.
3. Asking the government to suspend all actions/policies that are strategic and have broad implications is also not justified to issue "new" implementing regulations related to the Job Creation Law. Questions that may arise: Is the existing PP still valid? Yes, because the formation process is considered unconstitutional, the law and all existing regulations remain valid. Only new implementing regulations and other strategic policies are not permitted.

The MK decision needs to be given more attention because if there is no improvement in the Job Creation Law according to the MK decision, it will return to the substance of the arrangements in the previous Law Number 30 of 2014. This means that in state finances, treasury official decisions must again be in written form.

In the field of state finance, there is Government Regulation (PP) Number 45 of 2013 in conjunction with Government Regulation Number 50 of 2018

as an implementation of legal politics regarding state finances. The PP has adapted the use of technology in state finances through integrated system settings in the chapter on managing the state financial information system. Still, the PP has not yet adapted electronic documents. Arrangements for electronic documents in the scope of state finance, especially in implementing the budget, are regulated in Minister of Finance Regulation Number 204/PMK.05/2020 concerning the Piloting of Payment Procedures in the Context of Implementing the State Revenue and Expenditure Budget through Government Payment Platforms. The provision stipulates that electronic data, transactions and/or documents for electronic financial administration are ratified using an electronic signature. Still, there is no mention of the certification of the electronic signature. However, the PMK states that electronic data and electronic documents on electronic financial administration that are legalized with an electronic signature are valid evidence, although the legal requirements are not displayed. Since electronic documents and their legal requirements are regulated explicitly in the ITE Law, and PP PSTE, electronic documents and electronic signs for financial administration still refer to PP Number 71 of 2019.

So that it can be interpreted that the scope of the use of electronic documents in state finances is only regulated in PMK Number 204/PMK.05/2020, which provides a legal umbrella for the benefit of digital documents in a particular product in state finances, namely products produced by Agency Level Application Systems (SAKTI) within the scope of the Government Payment Platform.

3.3. The concept of electronic documents that can be used as legal evidence in court

As explained in number 1 and number 2, the material requirements of electronic documents as legal evidence are subject to the Criminal Code and laws governing information and electronic transactions, while as part of a civil law country that requires a legal basis as a formal requirement, the use of electronic documents in the scope of state finances has been regulated, although still within a limited scope.

The legal rules of *Lex Specialis derogate legi Generalis* provide a mandate to laws governing information and electronic transactions to determine the material requirements of an electronic document to be used as an extension of legal evidence as regulated in the Criminal Code law.

The main principle in electronic documents is that electronic documents contain electronic information. Electronic information can be distinguished, but electronic information cannot be separated from electronic documents. Electronic information is data or a collection of data that can be in any form, and electronic documents are a means or place of electronic information. Electronic information, for example, is who signed it, when it was signed, the purpose for which the information was sent, and so on. Electronic documents are files in various forms, for example, pdf. Electronic information and electronic documents if there is a dispute or violation of the law requiring evidence, then the information and documents can be used as electronic evidence (digital evidence).

The expansion in Article 26A of Law Number 20 of 2001 is an electronic evidence arrangement regulated in Article 5, paragraph (1) of the ITE Law. Article 5, paragraph (1) UU ITE divides the regulation into two parts. First, Electronic Information and/or Electronic Documents. And the second is the printout of the Electronic Information and/or the printout of an Electronic Document. Article 5, paragraph (4) is a formal requirement in which electronic documents do not apply to matters regulated in that paragraph. The material requirements for electronic documents are regulated in Article 6, Article 15, and Article 16 of the ITE Law. Electronic Information and Documents must fulfill guarantees of authentication, integrity, and availability.

As an analogy to electronic signatures as manual signatures, as also stated in the elucidation of Article 11 of the ITE Law, as with manual signatures, these signatures are also used to ensure that the electronic documents exchanged are signed by the authorized signatory and are guaranteed from changes to the information in them. Article 59 of Government Regulation Number 71 of 2019, as mentioned in the previous chapter, states six requirements for electronic signatures to have legal force and legal consequences, which fulfill the three aspects above.[23]

The digital signature formation algorithm consists of 2 related processes, as shown in Figure 2, namely the signature generation and verification processes. The first process occurs when the signatory signs the electronic document, while the second occurs when the recipient receives the

[23]National Institute of Standards and Technology, "Digital Signature Standard (DSS)," *Federal Information Processing Standards Publication*, 2009.

electronic document. The verification process will result in a decision that the documents obtained are intact or have changed during the trip.

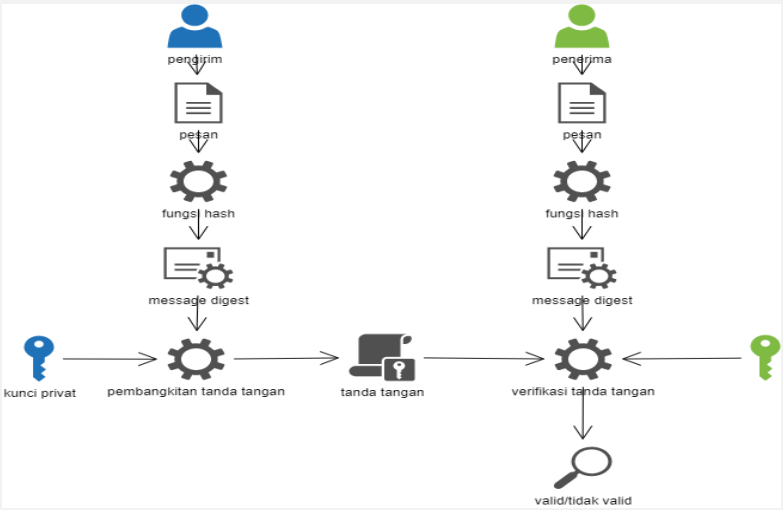

Figure 1. Digital Signature Process

The process begins when the signer generates the signature of the information to be sent. This process involves using a private key owned and controlled by the signer. In addition to having a private key, the signer also has a public key which is a partner of the private key and is created simultaneously in the key generation process with an asymmetric cryptographic algorithm. The public key can be known and attached to the transmitted document beside the signatory. The recipient will later use this key to carry out the document verification process when received. These two keys are unique and only owned and controlled by a particular signer. Apart from that, Article 61 of Government Regulation Number 71 of 2019 also requires that other parties do not easily know this data. To prevent misuse by other parties, articles 11 and 12 of the ITE Law and article 61 of PP PSTE require that the private key remain secret and possess the signatory is the owner of the key pair. This algorithm is designed to distinguish any changes in information that occur. For this purpose, this algorithm uses cryptographic techniques by utilizing a hash function for the information sent. The function will return a hash value as the associated information changes.[24] So that any changes related to electronic signatures and information sent can be known by message

[24]"Digital Signature Standard," in *Safeguarding Critical E-Documents*, 2015, https://doi.org/10.1002/9781119204909.app1.

recipients who comply with the provisions of article 11 of the ITE Law and 59 paragraph (3) letters c and d PP PSTE.

The recipient must gain confidence that the owner of the public key used to verify is the correct owner of the document. The owner's identity and public key can be attached to the electronic document. In line with this, article 62, paragraph (5) provides guidance that the electronic signature attached uses data for making electronic signatures made by the electronic certificate operator and includes the time of signing. The verifier can ensure that the document is correct from the sender if the hash value of the information received is the same as the hash information attached and encrypted with the owner's private key. If the encryption can be opened with the recipient's public key, the recipient is confident that the document with its public key comes from its owner.

In addition, the implementation of Public Key Infrastructure (PKI) on electronic signatures can be used to determine the signature of a document. An electronic signature alone is not sufficient to obtain owner information. The application of PKI to electronic signatures supports the property of nonrepudiation when it fulfills three things as well as in line with articles 60 and 61 PP PSTE, namely: [25]

1. The public key used at the verification stage is bound to the identity of the signer in the certificate issued by the issuer of the electronic certificate so the issuer can verify that authentication.
2. Changes in information and signatures can be detected due to using cryptography in digital signatures.
3. The signer cannot deny signing the document because, in theory, only he knows the private key used to sign the document.

Electronic signatures do not guarantee an electronic document's confidentiality but the integrity of changes. Information may be forged by someone pretending to be the sender using a different key pair. The owner of the original information may deny the document that the recipient has received because the information contained in it has been falsified. They

[25]J. L Hernandez-Ardieta, *Enhancing The Reliability of Digital Signature as Non-Repudiation Evidence Under a Holistic Treat Model* (Leganes: University Carlos III of Madrid, 2011).

also say the solution is to use a certificate from a trusted certificate issuer.[26]

Electronic certificates can also be issued by parties trusted by both parties who exchange information. This step can reduce the risk of key forgery by other parties while sending information to the recipient. An electronic certificate can contain a public key and information about the owner, the issuer of the certificate, and the period of the certificate before being revoked, where the public key can be verified through the publisher's signature. The certificate issuer is the party that acts as an intermediary and serves as a digital notary who ensures that the signature in an electronic document is genuine and valid. Furthermore, article 61, paragraph 4 says that the certificate issuer must also ensure that the signatory's data is safe from disclosure, alteration and unauthorized access, as well as stipulating the obligation of the Electronic Certification Operator to maintain the security and confidentiality of the data creation process. On the other hand, mastery over the data and its confidentiality is the responsibility of the signatory as the data owner.

The certificate may be revoked before the expiry date by the certificate holder or for other reasons. Article 52 of Government Regulation Number 71 of 2019 states that the authority to revoke and block this certificate rests with the electronic certification operator. Certificates included in the certificate revocation list can no longer be used by holders. Article 62, paragraphs 1 and 2 of PP 71 of 2019 state the need for a mechanism to ensure that the electronic signature verification data is still valid and within the power of the signatory. Related parties must know this information. They can use this information to verify documents originating from the certificate holder that has been revoked.

The description is an explanation associated with a certified electronic signature. In this regard, Government Regulation 71 of 2019 divides electronic signatures into certified and non-certified. Certified signatures are required to fulfill legality in the eyes of the law and use electronic certificates from Indonesian electronic service providers. On the other hand, this regulation also states that uncertified signatures are a means of authentication and verification. In general, uncertified electronic signatures still have the possibility of falsifying information.

[26]Stallings W. & Brown. L, *Computer Security, Principles And Practice, 3rd Ed* (Upper Saddle River: Pearson, 2015).

This is coupled with the need for a party that both parties trust in exchanging information. The signature is not certified. Moreover, the electronic signature is only produced and issued by one of the parties, which means that both the signatory and the maker of the electronic signature are the same party. The similarity between the party making the signature and the user of the signature, coupled with the unavailability of a system to identify the signer and that he has given consent, makes the principle of nonrepudiation vague. Referring to the Government Regulation on the Implementation of Electronic Systems and Transactions, the application of uncertified electronic signatures can have legal validity as long as it meets the requirements in Article 59, paragraph 3. Related to the principle of non-denial in the use of uncertified electronic signatures, following the mandate of the provision, the provision of a system that facilitates the identification of electronic information signatories and a mechanism that can show that the signatory has approved the electronic document becomes a necessity. The absence of this causes the electronic signature to be invalid in the eyes of the law.

4. Closing

4.1. Conclusions

As for this research, it can be concluded that electronic documents as electronic evidence in trials have been accommodated in several laws. KUHAP and HIR grammatically do not regulate the existence of electronic evidence, but the regulation of electronic evidence has been regulated long ago. Even the Corruption Law in 2001 had defined electronic evidence's existence before the ITE Law's birth. However, in several settings, there is an asymmetry in the position of electronic evidence where in one law, it provides a position as directive evidence; on the other hand, there are laws that provide an equivalent position to documentary evidence. The Job Creation Law, as the last law that regulates electronic documents, should be a permanent reference for judges, and the substance of the law makes electronic documents as evidence, as stated in Article 184 of the Criminal Procedure Code.

Meanwhile, regarding the legal basis of electronic documents in state finance, it can be concluded that it is quite complete. Business processes in state finance still refer to the package of state financial laws, both Law Number 17 of 2003 and Law Number 1 of 2004, by adopting the regulation of electronic documents in Law Number 11 of 2008 in conjunction with

Law Number 19 of 2016 and Law Number 30 of 2014 in conjunction with Law Number 11 of 2020. Electronic document arrangements have been represented by PP Number 71 of 2019, which was later adopted by PMK Number 204.05/2020 to become the legal basis for using electronic documents in state finances. Even though PP Number 45 of 2013 juncto PP Number 50 of 2018 has not adapted the existence of these electronic documents. What is of concern is the Constitutional Court's decision which annulled the Job Creation Law, which caused the sustainability of electronic documents in state finances to be threatened. In addition, it is necessary to pay attention to the material requirements for electronic signatures as one of the legal requirements for electronic documents as valid legal evidence in the ITE Law and PP PSTE.

The material requirements regarding electronic documents regulated in regulations in the field of electronic information, such as Government Regulation Number 71 of 2019, have provided quite complete arrangements regarding the exchange of information in electronic transactions, which must fulfill the three elements of authentication, information integrity and nonrepudiation. This Government Regulation has also regulated provisions regarding electronic certification, which is implemented in a way that supports these three elements. On the other hand, using uncertified electronic signatures accommodated under this government regulation still leaves the risk of forgery by other parties while sending information from sender to recipient and fulfilling the principle of nonrepudiation. Not to mention if it is added that the signature maker and signature user are from the same party and the absence of a system that is used as an approval identification function in the form of an electronic signature.

4.2. Suggestions

Based on these conclusions, the authors propose several suggestions, namely the need for amendments to Government Regulation Number 45 of 2013 by accommodating the existence of electronic documents in state finances, bearing in mind that Indonesia adheres to civil law, so there is a need for a strong legal umbrella in the administration of electronic documents in state finances. In addition, in technical implementation legal politics, it is necessary to have a Minister of Finance Regulation which provides regulations regarding electronic documents in its implementation. Electronic documents produced by electronic systems in

state finance are electronic documents with certified signatures following applicable regulations so that electronic documents produced normatively meet formal requirements as electronic documents.

The last suggestion, this research can be a trigger for further empirical research by conducting research on the fulfillment of material requirements for electronic documents generated from the Agency Level Application System (SAKTI) or conducting comparative legal research that compares laws in other countries regarding the use of electronic documents, especially in the field of state finance.

REFERENCES

Ashad. *Teori Modernitas Dan Globalisasi*. Sidoarjo: Kreasi Wacana, 2014.

Center for Legal and Judicial Research and Development of the Supreme Court of the Republic of Indonesia. *Kedudukan Dan Relevansi Yurisprudensi Untuk Mengurangi Disparitas Putusan Pengadilan*. Jakarta: Puslitbang Hukum dan Peradilan MA RI, 2010.

"Digital Signature Standard." In *Safeguarding Critical E-Documents*, 2015. https://doi.org/10.1002/9781119204909.app1.

Fuadi, Munir. *Teori-Teori Besar Dalam Hukum (Grand Theory)*. *Kencana Prenadamedia Group*, 2014.

Hernandez-Ardieta, J. L. *Enhancing The Reliability of Digital Signature as Non-Repudiation Evidence Under a Holistic Treat Model*. Leganes: University Carlos III of Madrid, 2011.

Heryadi, Adi, Ilham B Tarigan, and Weni Astuti. "Memahami Indeks Persepsi Korupsi (IPK) Indonesia Dan Kontribusi Polisi Militer Untuk Meningkatkan IPK." *DHARMA BAKTI*, 2022. https://doi.org/10.34151/dharma.v5i1.3928.

Imron, Dkk. *Hukum Pembuktian*. *Jurnal Hukum & Pembangunan*, 2017.

Isma, Nur Laili; Koyimatun, Arima. "Kekuatan Pembuktian Alat Bukti Informasi Elektronik Pada Dokumen Elektronik Serta Hasil Cetaknya Dalam Pembuktian Tindak Pidana." *Jurnal Penelitian Hukum*, 2014.

John Naisbitt. "Global Paradox: The Bigger the World Economy, the More Powerful Its Smallest Players." *Choice Reviews Online*, 1994. https://doi.org/10.5860/choice.31-5537.

Komalasari, Rita. "Manfaat Teknologi Informasi Dan Komunikasi Di Masa Pandemi Covid 19." *TEMATIK*, 2020. https://doi.org/10.38204/tematik.v7i1.369.

Maiyuni, Chella. "KUHP." *Journal of Chemical Information and Modeling*, 2013.

Martiman Prodjohamidjojo. *Komentar Atas KUHAP: Kitab Undang-Undang Hukum Acara Pidana*. Jakarta: Pradnya Paramitha, 1984.

Mulyadi, Sri Fitria, Dadan Kurniansyah, and Made Panji Teguh Santoso. "Implementasi Penerapan Aplikasi Sambara Dalam Administrasi Wajib Pajak Pada Masa Pandemi Covid-19 Di Kabupaten Karawang." *Jurnal Ilmu Pemerintahan Suara Khatulistiwa*, 2021. https://doi.org/10.33701/jipsk.v6i2.1887.

Nasution, Bahder Johan. "Metode Penelitian Ilmu Hukum." In *2*, 2016.

Nasution, S. "Metode Penelitian." *Jakarta: Rineka Cipta*, 2002.

National Institute of Standards and Technology. "Digital Signature Standard (DSS)." *Federal Information Processing Standards Publication*, 2009.

Nurhardianto, Fajar. "Sistem Hukum Dan Posisi Hukum Indonesia." *Jurnal Tapis*, 2015.

Raharjo, A. *Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. *Citra Aditya Bakti*, 2002.

Romli Atmasasmita. *Hukum Kejahatan Bisnis Teori Dan Praktik Di Era Globalisasi*. Jakarta: Prenadamedia Group, 2014.

Sahya Anggara. *Administrasi Keuangan Negara*. Bandung: CV Pustaka Setia, 2016.

Soekamto, S, and S Mamudji. *Penelitian Hukum Normatif (Suara Tinjauan Singkat)*. *Jakarta: Rajawali Pers*, 2015.

Stallings W. & Brown. L. *Computer Security, Principles And Practice, 3rd Ed*. Upper Saddle River: Pearson, 2015.

Suhendar, Suhendar. "Penyidikan Tindak Pidana Korupsi Dan Kerugian Keuangan Negara Dalam Optik Hukum Pidana." *Pamulang Law Review*, 2019. https://doi.org/10.32493/palrev.v1i1.2849.

Suhendar, Suhendar, and Kartono Kartono. "Kerugian Keuangan Negara Telaah Dalam Perspektif Hukum Administrasi Negara Dan Hukum Pidana." *Jurnal Surya Kencana Satu : Dinamika Masalah Hukum Dan Keadilan*, 2020. https://doi.org/10.32493/jdmhkdmhk.v11i2.8048.

Suherman. "Pola Mutasi, Reward & Punishment vs Fraud." *Djkn*, 2017.

Wahyudi, Johan. "Dokumen Elektronik Sebagai Alat Bukti Pada Pembuktian Di PengadilaN." *Perspektif*, 2012. https://doi.org/10.30742/perspektif.v17i2.101.