Journal of Law Perspectives Review
Volume 2, Nomor 1, 2026, Hal: 61-70
https://doi.org/10.64670/jlpr.v2i1.74

Catalyst Journal

Journal of Law Perspectives Review

Journal Homepage: journal.catalystindo.org

# Criminal Liability for Electronic Document Forgery: A Case Study of PT. Toyobo Japan

Sophia Lequin Theovani Purba[1], Thomas Poltak Sianturi[2], Theodora Verina Josephine Rouli Situmorang[3], Rosmalinda[4], Annisa Hafizhah[5*]

[1,2,3,4,5] Fakultas Hukum, Universitas Sumatera Utara Jl. Universitas No.19, Padang Bulan, Kec. Medan Baru, Kota Medan, Sumatera Utara 20155

ARTICLEINFO

*Received:* 29 December 2025
*Accepted:* 24 January 2026
*Available Online:* 28 January 2026

*Keywords:*
Electronic Document Forgery; Criminal Liability; Information and Electronic Transactions Law; Criminal Code; Cybercrime.

Correspondence
*Name: Sophia Lequin Theovani Purba
E-mail:



ABSTRACT

This study aims to explain the legal regulation of electronic document forgery in Indonesia as well as the form of criminal liability in the case of electronic document forgery of PT Toyobo Japan. Forgery of electronic documents is regulated through the general provisions of the Criminal Code and special provisions in the Electronic Information and Transactions Law that provide a legal basis for the act of creating, altering, and distributing counterfeit digital documents. This study uses a normative juridical method with a legislative approach and a case approach, based on the analysis of primary and secondary legal materials. The results of the study showed that the perpetrators deliberately created fake email accounts and manipulated payment instruction documents to illegally divert funds. These acts meet the elements of intentionality, responsible ability, unauthorized access, and the creation of false electronic documents as stipulated in the Criminal Code and the ITE Law. Thus, the perpetrators can be held criminally responsible as the main perpetrator or participate based on the applicable legal provisions.

## Introduction

Along with the development of the times and the rapid advancement of technology, including in the field of administration, people now have much easier access to carry out various administrative activities. However, this convenience also poses new challenges related to security and trust in the authenticity of documents, especially as the digital age allows important documents to be replicated or manipulated with advanced technologies such as image engineering, forgery software, and 3D printing. This condition has led to an increase in cases of document forgery in Indonesia, ranging from fake identities to other important documents. Therefore, juridical analysis of document forgery is very important to understand the applicable legal basis, the role of law enforcement officials, and effective prevention and handling measures. This effort requires cooperation between the government, law enforcement agencies, and the private sector to formulate policies and strategies that are able to overcome the rampant crime of document forgery.

The crime of falsifying documents carried out through internet media is included in the

category of cybercrime, which can be committed by both individuals and groups in an organized manner. Cybercrime, or cybercrime, refers to various criminal activities that use computers as the main means. Document forgery through digital media can include the forgery of various personal documents such as birth certificates, family cards, marriage certificates, diplomas, ID cards, driver's licenses, and other population documents. In addition, counterfeiting can also target commercial documents such as checks, bonds, stocks, money orders, receipts, and the like.

From a criminal law perspective, electronic document forgery is categorized as a formal offense that is generally considered completed when the perpetrator commits the act of altering, falsifying, or producing electronic documents with the intention of using them as if they were authentic. Falsification of documents, including in electronic form, is understood as a criminal act that damages public trust and disrupts the integrity of state administration, so that the perpetrators can be held criminally responsible both as individuals and as corporations. According to Article 1 number 4 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), electronic documents are any electronic information that is created, forwarded, transmitted, received, or stored in analog form, which can be viewed, displayed, and/or heard through a computer or electronic system, including but not limited to writing, sounds, images, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have a meaning or significance or can be understood by a person who is able to understand them.

The use of information, media, and communication technology has changed the behavior of society and human civilization globally. These developments have brought a number of significant positive impacts, especially in the social, economic, and cultural fields, although they are still accompanied by the potential for abuse in the form of criminal acts such as electronic document forgery (Wall, 2017). The case of electronic document manipulation involving Japan's PT Toyobo shows how digital crime can be operated in a structured and difficult-to-detect mode. The perpetrators in the case falsified PT Trias Sentosa's digital identity through the creation of fake emails and manipulated electronic documents. This action tricked PT Toyobo Japan so that the company diverted payments to accounts controlled by the perpetrators.

This incident illustrates that the threat of electronic document forgery has the potential to cause a large amount of financial loss, especially when the aggrieved party is abroad and the transaction occurs across jurisdictions. Various studies show that the increasing intensity of information technology use is not always balanced with an adequate level of digital security literacy. This makes companies and individuals vulnerable to being trapped in the form of social engineering and manipulation of electronic documents. In addition, the system of proof of digital crimes has its own complexity because it relies on electronic traces, metadata, and the ability of law enforcement authorities to conduct digital forensic analysis.

In the context of Indonesian law, electronic documents have been recognized as legitimate evidence. However, such legitimacy demands stronger protection mechanisms, especially in terms of authentication and data integrity. When electronic documents are manipulated, it not only violates legal norms, but also undermines public trust in the electronic transaction system. Therefore, it is important to ensure that regulations related to data security, electronic transactions, and

manipulative actions in the digital space can be effectively enforced.

Research on criminal liability for electronic document forgery is relevant in order to understand how the state responds to the growing digital crime. It is also important to see the extent to which the legal system is able to provide a sense of justice for victims, while creating legal certainty in electronic activities. In addition, this paper is expected to enrich the literature on law enforcement against technology-based crimes by formulating problem 1. What is the legal arrangement regarding electronic document forgery in Indonesia? And 2. What is the form of criminal liability that can be imposed on the perpetrators of electronic document forgery in the case of PT Toyobo Japan?

A number of previous studies have examined the crime of electronic document forgery from various perspectives. Several studies have focused on the normative aspects regarding the application of provisions in the Electronic Information and Transaction Law and its relevance to the provisions of forgery in the Criminal Code, especially related to the elements of unlawful acts and electronic evidence as valid evidence. Other research focuses more on the technical dimension of digital proof, such as the use of digital forensics in identifying metadata manipulation and electronic traces. In addition, there are also studies that discuss cybercrime in general, including the mode of social engineering in email-based fraud and manipulation of cross-border transactions.

However, most of these studies are still general and have not specifically examined criminal liability in the context of concrete case studies involving cross-jurisdictional corporations such as the case of PT Toyobo Japan. There has not been much research that integrates normative analysis of elements of criminal responsibility with the construction of the role of perpetrators, both as main perpetrators and participants, in electronic document falsification schemes that are structured and involve the misuse of corporate identity.

Thus, there is a *research gap* in the aspect of in-depth analysis regarding the construction of criminal liability in the case of electronic document forgery with a transnational dimension, especially in examining the cumulative application of the provisions of the Criminal Code and the ITE Law to modus operandi based on the manipulation of corporate digital identities. This research seeks to fill this gap by presenting a more comprehensive and contextual juridical analysis of the case of PT Toyobo Japan, so as to make a theoretical and practical contribution to the development of cyber criminal law in Indonesia.

## Methods

Legal research is the process of finding scientific truth about a legal issue through the application of scientific methods that are structured in a planned, systematic, and logical manner. Its main goal is to provide answers to legal events and solve issues that arise, both in the realm of theory and practice. This research uses an analysis method (normative qualitative analysis), which is an approach that relies on legal materials in the form of laws and regulations, court decisions, contracts or agreements, legal theories, and expert opinions. This method was chosen because the discussion of electronic document forgery and criminal liability in the case of PT Toyobo Japan requires an analysis of applicable legal norms, including provisions in the Criminal Code, the Electronic Information and Transaction Law (ITE Law), as well as other regulations related to electronic documents, cybercrime, and criminal liability. In its implementation, this study uses two types of

approaches. First, a statutory approach to review the regulations regarding the falsification of electronic documents in the Criminal Code and the ITE Law. Second, a case approach to assess how the legal provisions are applied in the case of electronic document forgery involving PT Toyobo Japan.

## Results and Discussion

### Legal Regulations Regarding Electronic Document Forgery in Indonesia

The era of information technology development that has blown in the last 2 decades which has a significant speed has resulted in the development of information technology has now penetrated all lines of life of the world people. Including Indonesia, it has spurred the development of technology in the community both in cities and villages so that all members of society must master information technology in order to be able to keep up with the times (Veronika J. K, (2022).

The Government of Indonesia has counteracted this era by enacting Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) which then in its course experienced the first amendment to Law (UU) Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions to the second amendment to Law (UU) Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Transactions Electronic Transactions. In the explanation of the ITE Law, it is emphasized that "The use of Information Technology, media, and communication has changed both the behavior of society and human civilization globally". The development of information and communication technology has also caused world relations to become borderless and caused social, economic, and cultural changes to take place so rapidly (Council, 2021).

Forgery of electronic documents carried out through social media or digital platforms includes different types of documents that can be grouped based on their purpose and use. First, there is the falsification of personal documents related to individual interests, such as birth certificates, family cards, education certificates, award certificates, identity cards (KTP), driver's licenses (SIM), marriage certificates, and other personal identity documents. Second, counterfeiting can also be related to commercial documents or business documents related to business transactions and business activities, such as checks, bonds, receipts, money orders, stocks, and other financial instruments (Gemilang, 2024).

In addition to these two main categories, there are also other documents that can be forged in the context of international transactions and large-scale businesses, including letters of introduction, sales invoices, bills of lading, blanks or official forms, and letters of credit (payment guarantee documents in international transactions). Each type of forged document has a different potential legal impact, depending on the type of document, the purpose of the forgery, and the harm caused to the parties involved. By utilizing information technology and social media, forgery perpetrators can easily create, modify, distribute, and disseminate such forged documents to various parties with a very wide range (Basu, 2018; Albrecht at., al. 2017). Article 1 paragraph (4) of the ITE Law explains that Electronic Documents are any Electronic Information that is created, transmitted, transmitted, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard through a Computer or Electronic System, including but not

limited to writing, sound, images, maps, designs, photographs or the like, letters, signs, etc. numbers, Access Codes, symbols or perforations that have a meaning or significance or can be understood by a person who is able to understand them (Sjahdeini, 2019).

The crime of forgery of letters is specifically regulated in Chapter XII of the Criminal Code (KUHP) which contains Articles 263 to 278, which regulates various forms and aspects of the crime of forgery of letters. Normatively, the definition of letter forgery is defined in Article 263 paragraph (1) of the Criminal Code as the act of making documents or letters that are not original or converting existing letters into fake letters. The forged document or letter must be a document that has the legal ability to give rise to a right, engagement or release of debt, or a document intended as evidence of a certain event or circumstance. The element of error in the crime of forgery of letters according to Article 263 paragraph (1) of the Criminal Code is the intention or intention of the perpetrator to use or instruct others to use the fake letter as if the content is true and genuine, without forgery. In addition, another important element is that the use of the fake letter must be able to cause harm to others or be detrimental to the parties who believe in the authenticity of the letter. Thus, Article 263 paragraph (1) of the Criminal Code criminalizes the act of forgery of letters by creating, altering, or manipulating documents with the aim of harming other parties through the use of fake letters presented as genuine and trustworthy documents (Sitanggang & Saputra, 2024).

Document forgery carried out using social media will be used by the ITE Law as a legal instrument. In Article 26 paragraph (1) of the ITE Law, it says that "unless otherwise specified by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned". In this law, falsification of electronic documents is defined as the act of creating, altering, reproducing, distributing, disseminating, and/or using counterfeit electronic documents without rights or against the law (Article 35 and Article 51 of the ITE Law). The electronic document has legal force equivalent to conventional documents and can be valid evidence in legal proceedings (Article 5 Paragraph 1 of the ITE Law). In addition, the ITE Law regulates unauthorized access to computers and electronic systems that can be used to forge electronic documents (Article 31). The legal regulation of electronic document forgery in Indonesia is mainly guided by the ITE Law as a special regulation that protects the integrity of electronic documents and criminalizes all forms of forgery and manipulation of documents in digital form, as well as supported by the Criminal Code regulations for general criminal aspects related to forgery and fraud.

**Forms of Criminal Liability That Can Be Imposed on Perpetrators of Electronic Document Forgery in the Case of PT Toyobo Japan**

Information technology today has a dual nature, where on the one hand it provides great benefits in improving human welfare, progress, and civilization, but on the other hand it also has the potential to be used as a means to carry out unlawful actions. Along with the development of technology, a new legal regime has emerged known as cyber law or telematics law, which regulates and supervises legal activities related to cyberspace and information technology. Cyber law or *Cyber Law* It is a term used internationally to describe the legal regime related to the use and use of information and communication technology. In its development, the term telematics law emerged as

a result of the integration of three branches of law, namely telecommunications law, media law, and informatics law, which created a comprehensive legal framework. In addition, there are various other terminologies that are also used to refer to the same legal regime, including the law of information technology, cyber law (*Virtual World Law*), and the law of the Mayantara, all of which refer to the same understanding. (April, 2024).

These terms are evolving and used because legal activities today are no longer limited to conventional activities, but also include activities carried out through computer systems and communication systems, both on a local and global scale through the Internet. These activities are carried out by utilizing information technology based on computer systems, which are electronic systems that are virtual and cannot be seen physically directly (Nudirman, 2018).

In Indonesian criminal law, criminal liability is a core concept that explains when and how a person can be held accountable for criminal acts. Two fundamental elements must be present simultaneously for criminal liability to be applied: guilt (schuld) and capacity to be responsible (imputability). Guilt is defined as the psychological connection between the perpetrator and the act or the impact of the act, which manifests in two main categories. First, intentionality (dolus), which occurs when the perpetrator acts with full knowledge and intention that the act violates legal norms or produces prohibited consequences. Second, negligence (culpa), which occurs when the perpetrator commits an act without the intention of violating the law, but his carelessness causes a violation of the law (Makhali, 2023).

In the case of PT Toyobo Japan, three perpetrators named Reza Hernanda, Syahrudin Noor, and Denny Anggriawan have committed intentional unlawful acts. They created fake email accounts and sent out ungenuine payment orders with the aim of harming PT Toyobo Japan. So that the second element of criminal liability is fulfilled, namely accountability (Putra & Wibowo, 2022). Accountability is a person's ability to be responsible, which means that the perpetrator must be mentally and physically healthy, know that his or her actions are against the law, and not in special circumstances that eliminate responsibility such as mental illness or immaturity. The three suspects in this case are adults with normal mental states, so they have the full capacity to be responsible and there is no legal obstacle that abolishes their responsibility (Fitriani & Santoso, 2019; Yulianti, 2018).

Syahrudin Noor's role in this case is as an account coordinator who is responsible for identifying and coordinating the company's accounts that will be used to receive profits from criminal acts. In the aspect of criminal liability, Syahrudin Noor carried out coordination activities deliberately and had a full understanding of the purpose of using the account, so that his status could be determined as participating in a criminal act (*participation*) that helps and facilitates the execution of the main perpetrator (Iskandar, 2021). Denny Anggriawan has a position as the owner of PT Kalimantan Kuasa Karya and at the same time the holder of a company account that receives the transfer of funds from the proceeds of criminal acts. From the perspective of criminal liability, Denny Anggriawan acted deliberately and with full awareness that the funds received were the result of illegal activities, so that they could be categorized as the main perpetrators (dader) who obtained material benefits directly from crimes. Thus, the differentiation of roles among the defendants reflects varying degrees of involvement in separately organized and divided crime schemes. Article 55 of the Criminal Code stipulates that "Whoever commits, who orders to do, or participates in

committing an act, is convicted as a criminal offender". This normative formulation indicates that in criminal liability for crimes committed collectively, the legal system does not make significant material differentiations between direct perpetrators and perpetrators, so that all perpetrators involved in criminal acts are fully responsible for the entire unlawful act. Article 56 of the Criminal Code further regulates that individuals who "give orders to commit an act or provide an opportunity to commit such an act, shall be punished for participating in the criminal act". The provisions of this article have important relevance in the case of PT Toyobo because it indicates that criminal liability is not only limited to the person who physically performs the act, but also includes those who provide the facilities, opportunity, or direction for the execution of the act. Therefore, Denny Anggriawan as the owner of a fictitious company and the giver of the order can be considered as an individual who gave an order to commit or provide an opportunity for the act of forgery of electronic documents (Joseph & Hasibuan, 2022).

Article 31 of the ITE Law regulates unauthorized access to computers and electronic systems. This article states that "Every Person intentionally and without rights or unlawfully accesses the Computer and/or Electronic System belonging to another Person". In the case of PT Toyobo Japan, the three perpetrators gained unauthorized access to create fake email accounts that resembled official accounts from PT Trias Sentosa and PT Toyobo Japan, so that their actions met all the elements listed in Article 31 of the ITE Law. The three suspects have legal responsibility for unauthorized access to the email system with a criminal threat in the form of imprisonment of up to 6 (six) years and/or a fine of up to a maximum of Rp 600,000,000.00 (six hundred million rupiah). Article 35 of the ITE Law combined with Article 51 paragraph (1) of the ITE Law is the most relevant provision to ensnare the perpetrators of electronic document forgery in this case. Article 35 of the ITE Law stipulates that "Every Person deliberately and without the right to produce, make, reproduce, distribute, disseminate, and/or use Counterfeit Electronic Documents". In the case of PT Toyobo, the perpetrator created a fake email account that was identical to the official email of PT Trias Sentosa and PT Toyobo Japan, and created a fake payment instruction document containing an order to transfer payments from a legitimate account to an account belonging to the perpetrator. This act clearly meets the elements regulated in Article 35 of the ITE Law, namely producing, making, and using fake electronic documents. Denny Anggriawan as the main perpetrator will receive the most severe crime, followed by Reza Hernanda and Syahrudin Noor as participants with consideration of their level of involvement and the application of the principle of criminal proportionality. Thus, the case of PT Toyobo Japan provides a practical illustration of how Indonesian criminal law integrates various legal norms to ensure that every perpetrator of cybercrime gets appropriate, fair, and appropriate criminal accountability in accordance with their actions and role in organized crime.

## Conclusion

The legal arrangement regarding the forgery of electronic documents in Indonesia is basically based on the Criminal Code as a general provision on the forgery of letters and the ITE Law as a special rule that regulates the forgery of documents in digital form. The Criminal Code through Articles 263–278 affirms that forgery occurs when a person creates or alters documents so that they

appear as if they are original and can cause losses. Meanwhile, the ITE Law expands the scope of counterfeiting to the electronic realm, where Article 35 and Article 51 criminalize the act of making, reproducing, distributing, and using counterfeit electronic documents. The ITE Law also complements legal protection through Article 31 which ensnares perpetrators who access electronic systems without rights, so that overall national regulations have provided a comprehensive basis to overcome electronic document forgery in the digital era.

The form of criminal liability for the perpetrators of electronic document forgery in the case of PT Toyobo Japan shows the application of the principle of error (dolus or intentionality) and accountability that allows the three perpetrators to be held fully accountable. Reza Hernanda, Syahrudin Noor, and Denny Anggriawan knowingly created fake email accounts, produced fake electronic documents, and directed payment streams to obtain unlawful profits. Based on Articles 55 and 56 of the Criminal Code, all perpetrators—both the main perpetrators and those who help — are responsible as perpetrators of criminal acts. In addition, their actions met the elements of Article 31 and Article 35 of the ITE Law related to illegal access and the creation of false electronic documents. Thus, all perpetrators can be criminally charged according to the level of their role, where Denny Anggriawan as the main perpetrator receives the threat of the heaviest punishment, followed by two other perpetrators as parties who participated in the crime.

**Acknowledgments**

Praise be to God Almighty for all the graces, blessings, and guidance that have been given so that the writing of this scientific journal can be completed properly. The author would also like to express his deepest gratitude to Mrs. Dr. Rosmalinda, SH, LLM, as the supervisor of the Legal Writing Engineering course, who has provided guidance, direction, and very valuable input in the process of writing this journal. Mother's patience and dedication in guiding writers is a strong motivation to continue to develop in the field of legal scientific writing. The author also does not forget to thank Mrs. Annisa Hafizhah, SH, MH, who has made significant contributions through constructive suggestions and feedback that is very helpful in improving the quality of this journal. The author realizes that this journal is still far from perfect, and therefore the author is open to receiving constructive criticism and suggestions from various parties for the improvement of the quality of scientific work in the future. Hopefully this journal can be useful for the development of science, especially in the field of criminal law and electronic document protection.

**Bibliography**

Albrecht, C., Albrecht, W. S., & Dunn, J. (2017). Fraud risk assessment and the detection of fraudulent financial reporting in international trade. *Journal of International Accounting Research, 16*(3), 1–22. https://doi.org/10.2308/jiar-51820

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. Begawan Abioso , 15 (1).

Basu, S. (2018). International trade fraud and documentary manipulation in the digital era. *Journal of Financial Crime, 25*(4), 1052–1067. https://doi.org/10.1108/JFC-06-2017-0056

Fitriani, N., & Santoso, B. (2019). Pertanggungjawaban pidana dalam tindak pidana siber

berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Jurnal Hukum IUS QUIA IUSTUM*, *26*(2), 317–335.

Gemilang, Herdino Fajar. (2024). Meninjau ilmu digital forensik terhadap bukti elektronik dalam tindak pidana informasi dan transaksi elektronik. Perahu (Penerangan Hukum): Jurnal Ilmu Hukum 12.2.

Iskandar, Boby, and Eren Arif Budiman. (2021). Kebijakan Formulasi Hukum Pidana Tentang Penanggulangan Tindak Pidana Terorisme Siber (Cyber Terorism) Di Indonesia. Jurnal Hukum Ius Publicum 2.1.

Makhali, Imam. (2023). Bentuk Pertanggung Jawaban Pidana Bagi Pelaku Tindak Pidana Mayantara. Transparansi Hukum 6.1.

Nudirman, Munir. (2018). Pengantar Hukum Siber Indonesia, Jakarta, Raja Grafindo Persada.

Putra, R., & Wibowo, A. (2022). Pertanggungjawaban pidana pelaku penipuan berbasis email (business email compromise) dalam transaksi internasional. *Jurnal Ilmu Hukum*, *18*(2), 211–228.

Raden, Digdayana, Aditya, Bilal. (2021). Pembuktian Tindak Pidana Pemalsuan Dokumen Elektronik. Diss. Universitas Muhammadiyah Yogyakart.

Sitanggang, A. S., F. Darmawan, dan D. Saputra. (2024). Hukum Siber Dan Penegakan Hukum Di Indonesia: Tantangan Dan Solusi Memerangi Kejahatan Siber. Jurnal Pendidikan Dan Teknologi Indonesia, vol. 4, no. 3.

Sjahdeini, S. R. (2019). Legal implications of electronic documents and digital evidence in Indonesian cyber law. *Indonesia Law Review*, *9*(2), 245–260.

Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity landscape. *Information & Communications Technology Law*, *26*(2), 137–165. https://doi.org/10.1080/13600834.2017.1298503

Veronika Juliana, Kanter. (2022). Penerapan Sanksi Pidana Pelaku Pemalsuan Dokumen Yang Dilakukan Melalui Media Sosial. Lex Crimen 11.2.

Yulianti, D. (2018). Unsur kesengajaan dan kesalahan dalam pertanggungjawaban pidana menurut KUHP dan perkembangannya. *Jurnal Hukum & Pembangunan*, *48*(4), 789–805.

Yusuf, Dm, Mohd, And Rizwan Hasibuan. (2022). Tindak Pidana Cyber Crime Dan Sanksinya Dalam Undang-Undang Informasi Dan Transaksi Elektronik. ANDREW Law Journal 1.2.