Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Criminal Liability of Perpetrators who Intentionally and Unauthorized Alteration of Electronic Documents Based on the Electronic Information and Transactions Law (Study of Central Jakarta District Court Decision Number 724/Pid.Sus/2023/PN Jkt.Pst)

Beti Septiana Sari[1], Abunawas[2], Jamiatur Robekha[3]
IBLAM College of Law, Campus A, Jl. Kramat Raya No. 25, Senen, Central Jakarta

Article Info

Keywords:
Accountability,
changing electronic documents,
intentionally,
without authorization.

ABSTRACT

An electronic document is electronic information created, forwarded, sent, received, or stored in digital, electromagnetic, optical, or similar format, which can be viewed, displayed, and/or heard through a computer or electronic system. This document can be in the form of text, sound, images, or various other formats that convey meaning. The crime of altering electronic documents that causes harm to another person can be categorized as a cybercrime, particularly related to the manipulation of electronic information. The research method used is the normative juridical method, namely research that prioritizes library data, namely research on secondary data. The secondary data can be in the form of primary, secondary, or tertiary legal materials. Based on the research results, the author concludes that criminal liability for perpetrators of criminal acts intentionally and without authority to change electronic documents belonging to others that result in harm to others, can be enshrined by the Electronic Information and Transactions Law (UU ITE). The ITE Law regulates criminal sanctions for various actions related to electronic data manipulation. The relevant articles in the ITE Law related to illegal alteration of electronic documents include Article 27, Article 30, Article 32, Article 35, and Article 65. These articles regulate: a) Article 27: Prohibition on distributing, transmitting, and/or making accessible electronic information that contains content that violates morality, gambling, insults, or defamation; b) Article 30: Prohibition on unauthorized access to other people's computers or electronic systems; c) Article 35: Prohibition on falsifying electronic data; d) Article 65: Prohibition on using personal data that does not belong to them. Meanwhile, the sanctions, the perpetrator can be subject to criminal sanctions in the form of imprisonment and/or a fine, the amount of which varies depending on the article violated and the level of loss caused.

Corresponding Author:
Beti Septiana Sari
IBLAM College of Law, Campus A, Jl. Kramat Raya No. 25, Senen, Central Jakarta

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

INTRODUCTION

The development of information technology is currently advancing rapidly. This has certainly made banking easier for people. The internet itself was first discovered in 1969 and has been a favorite since the 1990s in Indonesia, although not as rapidly as it is now. It wasn't until the 2010s that Indonesia experienced rapid internet development and the convenience it offers. Recently, we've heard about the concept of the 4th Industrial Revolution, which utilizes data, blockchain technology, and artificial intelligence. However, Japan has already introduced the concept of Society 5.0, a new concept that is considered capable of replacing the previous four versions, which only focused on the production of goods or services.

In today's modern digital era, everything can be done from home or anywhere, simply by using a mobile phone or internet-enabled device like a smartwatch or laptop, which are becoming increasingly diverse and versatile. This convenience has both positive and negative impacts, with everything being made easier, including negative consequences, and the emergence of new types of crime as the times evolve.

Use of the internet as a means of information has become a new fashion among society which has resulted changes in the way of working and living habits in society. With the development of information that spreads so quickly gives rise to various legal problems. The free nature of the internet has resulted in many people exploit it to gain profit even though it is against the law. This technology-based crime is carried out through the use of media. found on the internet or commonly called cyber crime.

Electronic document crimes, also known as cybercrimes, are crimes involving the manipulation, misuse, or falsification of information and documents stored electronically. These crimes can range from digital signature forgery and data theft to the distribution of illegal content, document forgery, and online fraud.

An electronic document is electronic information created, forwarded, sent, received, or stored in digital, electromagnetic, optical, or similar formats, which can be viewed, displayed, and/or heard via a computer or electronic system. This document can be in the form of text, sound, images, or various other formats that have meaning.

The crime of altering electronic documents that causes harm to others can be categorized as a cybercrime, particularly one related to the manipulation of electronic information. Perpetrators can be prosecuted under the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), as well as other relevant laws and regulations.

The Criminal Code (KUHP) does not regulate in detail the crime of manipulating electronic documents so that they can be considered as authentic data. However, Article 263 paragraphs (1) and (2) of the Criminal Code states that:

> (1) Whoever makes a false letter or falsifies a letter which can give rise to a right, obligation or release from debt, or which is intended as evidence of something with the intention of using or ordering another person to use or ordering another person to use the letter as if its contents were true and not falsified, is threatened if the use can

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

cause a loss, due to the falsification of the letter, with a maximum prison sentence of six years;

(2) Anyone who intentionally uses a fake or falsified letter as if it were genuine, if the use of the letter can cause loss, shall be subject to the same penalty.

His actions in changing and manipulating electronic documents are regulated in Article 51 paragraph (1) in conjunction with Article 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions. In short, this article prohibits any person from intentionally and without rights or unlawfully manipulating, creating, changing, deleting, or destroying electronic information/electronic documents, so that the information is considered as if it were original. The perpetrator can be subject to criminal sanctions of imprisonment and fines.

In this study the author provides an example of a case related to a criminal act intentionally and without the right to change another person's electronic documents which resulted in losses for others whose case has been decided by the Central Jakarta District Court with decision Number 724 / Pid.Sus / 2023 / PN Jkt.Pst. In this case the defendant is Windia Dede Chandra Bin Alex Chandra, who in the trial was proven legally and convincingly guilty of committing a criminal act intentionally and without the right to change another person's electronic documents which resulted in losses for others, so that the panel of judges sentenced the defendant to imprisonment for 1 (one) year and 7 (seven) months and a fine of Rp. 10,000,000.00 (ten million rupiah).

The author's concern in this study is related to the regulation of criminal acts of intentionally and without rights to change electronic documents belonging to other people and the application of criminal sanctions against perpetrators of criminal acts of intentionally and without rights to change electronic documents belonging to other people which results in losses to other people. Based on the description above, the author determines the title of this study is CRIMINAL LIABILITY OF PERPETRATORS OF INTENTIONAL AND WITHOUT RIGHTS TO CHANGE ELECTRONIC DOCUMENTS BASED ON THE ELECTRONIC INFORMATION AND TRANSACTIONS LAW (Study of Central Jakarta District Court Decision Number 724 / Pid.Sus / 2023 / PN Jkt.Pst). The formulation of the problem in this study is 1) How is the regulation of criminal acts of intentionally and without rights to change electronic documents belonging to other people? 2) How is the criminal liability for perpetrators of criminal acts of intentionally and without rights to change electronic documents belonging to other people which results in losses to other people?

The form of research used in writing the thesis entitled: "criminal liability for perpetrators of intentional and unauthorized changes to electronic documents based on the Electronic Information and Transactions Law", is normative juridical, namely analyzing the relationship between applicable laws and regulations with legal theories and the practice of implementing positive law concerning the issues discussed. This research will analyze legal issues, facts, and other legal phenomena related to the legal approach, then obtain a comprehensive picture of the problem to be studied. This descriptive analytical research will

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

only describe the state of the object or problem and is not intended to draw or draw generally applicable conclusions regarding criminal liability for perpetrators of intentional and unauthorized changes to electronic documents based on the Electronic Information and Transactions Law.

RESULTS AND DISCUSSION

Regulations on the Criminal Act of Intentionally and Without Authority to Change Electronic Documents Belonging to Another Person

Criminal acts related to changing electronic documents belonging to others are comprehensively regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law Number 19 of 2016 and most recently by Law Number 1 of 2024. This regulation is the main legal basis for protecting the integrity and authenticity of electronic information in today's digital era.

Specifically, Article 32 paragraph (1) of the ITE Law states that any person who intentionally and without authority or unlawfully changes, adds, reduces, deletes, or transfers electronic information and/or electronic documents belonging to another person may be subject to criminal penalties. This crime is seen as a form of violation of a person's ownership rights and data integrity in the digital space. Article 48 of the ITE Law is the criminal article of this provision, by stipulating a maximum prison sentence of 8 years and/or a maximum fine of IDR 2 billion. In fact, if the act causes disruption to the electronic system, the penalty can increase to 10 years in prison and/or a maximum fine of IDR 5 billion.

The ITE Law also provides protection for two main types of electronic information: personal data and public electronic information. Protection of personal data is now strengthened with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The PDP Law aims to guarantee individual privacy rights, build trust in digital activities, and prevent data misuse by irresponsible parties. This protection covers the entire data lifecycle, from collection, processing, storage, distribution, and destruction. Furthermore, the PDP Law establishes principles for personal data protection, such as legal certainty, prudence, transparency, and accountability of data controllers.

Meanwhile, public electronic information is protected with the aim of maintaining information stability in government systems and public institutions, avoiding data manipulation that could cause public unrest, and preventing cybercrimes such as hacking of government websites and falsification of state information. Security of public electronic information is supported by technical regulations, such as Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and Regulation of the Minister of Communication and Information Technology Number 20 of 2016, which regulates the governance of personal data protection in electronic systems.

Within the broader context of criminal law, the new Criminal Code (Law No. 1 of 2023) also addresses cybercrimes. Articles 332 to 335 stipulate criminal penalties for

perpetrators who unauthorizedly access, damage, or misuse electronic systems, including those owned by the state, financial institutions, and banking institutions. The new Criminal Code carries a maximum penalty of 12 years' imprisonment and a substantial fine (category VII), depending on the extent of the loss and the object of the attack.

If the act of altering electronic documents is carried out with the aim of damaging the reputation or defaming another person, the perpetrator can be charged with additional articles. In addition to Article 32 in conjunction with Article 48 of the ITE Law, the perpetrator can be subject to provisions in the PDP Law (specifically Articles 65 to 67) as well as Article 310 of the old Criminal Code and similar articles in the new Criminal Code. The old Criminal Code differentiates between oral and written defamation with different criminal penalties. Meanwhile, defamation committed through electronic media or the internet is regulated in Article 27 paragraph (3) and Article 27A of the ITE Law, with a maximum prison sentence of 4 years and/or a maximum fine of IDR 750 million. However, it is important to note that in some circumstances, defamation is not criminally punishable if the statement is made in the public interest or as a form of self-defense.

Overall, regulations regarding the crime of altering electronic documents demonstrate the state's commitment to protecting citizens' rights in the digital age. These regulations are crucial not only for imposing sanctions on cybercriminals but also for ensuring the security, reliability, and public trust in the use of information and communication technology.

Criminal Liability for Perpetrators of Criminal Acts Who Intentionally and Without Rights Change Electronic Documents Belonging to Another Person Which Causes Loss to Another Person

The crime of intentionally and without authorization altering another person's electronic documents is a form of cybercrime expressly regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016. Such acts are punishable by law if they cause harm to another party. Such actions violate the right to information and personal data protection, and threaten trust in digital transactions.

The ITE Law includes a number of important articles that form the basis for criminal liability, including:

a. Article 30, which prohibits illegal access to electronic systems;
b. Article 32, which regulates the prohibition on changing, adding, reducing, transmitting or deleting electronic information without authority;
c. Article 3, which prohibits the falsification of electronic data to make it appear legitimate;
d. Article 36, which emphasizes the legal threat if changes to the data cause losses; and
e. Article 65 , regarding misuse of personal data.

To prosecute the perpetrator criminally, there are four important elements that must be fulfilled, namely:

1. There is an act of changing electronic information,

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

2. Done without the rights or permission of the legitimate owner of the data,
3. Done intentionally (malicious intent or full awareness of the act), and
4. Causing harm to others.

One form of crime closely related to the alteration of electronic data is phishing. Phishing is a form of crime committed by tricking victims into handing over sensitive information such as usernames, passwords, or financial data. Perpetrators typically impersonate official institutions and use tools such as fake email addresses or websites. In this context, phishing perpetrators have violated criminal law principles because they knowingly violate the law and have mens rea, or an element of guilt.

According to Roeslan Saleh, criminal responsibility arises from actions that are reprehensible both legally and socially. Meanwhile, Moeljatno emphasized that criminal responsibility contains three main elements: (1) the perpetrator's ability to take responsibility, (2) the existence of an unlawful act with an inner attitude in the form of intent or negligence, and (3) the absence of justification or forgiveness.

Intention or mens rea in criminal law can be reviewed in three forms:

1. Intention as a goal, where the perpetrator really wants a certain result to occur;
2. Intention with awareness of certainty, namely the perpetrator is aware that the consequences of his actions will definitely occur even though that is not the main goal;
3. Intentional intent with awareness of the possibility, namely the perpetrator imagines that there is a possibility of consequences arising, but still continues with his actions.

Regarding interception or wiretapping, the ITE Law also regulates the prohibition in Article 31 paragraph (1) and Article 47, which threatens perpetrators with a maximum prison sentence of 10 years and a fine of up to IDR 800 million. Interception is the act of listening to, recording, or monitoring electronic information without permission. In law enforcement, it is important to prove the perpetrator's *mens rea* , namely malicious intent in accessing information that should be confidential or private.

Case: Central Jakarta District Court Decision Number 724/Pid.Sus/2023/PN Jkt.Pst

A concrete case of this can be seen in the Central Jakarta District Court's ruling in criminal case No. 724/Pid.Sus/2023/PN Jkt.Pst. Defendant Windra Dede Chandra was found guilty of illegally and unauthorizedly altering a bank customer's electronic data.

Initially, the defendant, who worked for an IT services company, was tasked with repairing Bank Artha Graha Internasional customer data. However, using a high-level user (superuser) that was supposed to be used for limited purposes, the defendant created two fictitious accounts to manipulate customer data: DDANU.1 and DDANU.2. He then changed the customers' phone numbers and email addresses to fake data to gain access to mobile banking services.

After successfully accessing the victim's mobile banking account, the defendant transfeVrred Rp60,135,000 through QRIS transactions and virtual accounts. All of these actions were carried out without the account holder's permission or knowledge, clearly violating the law.

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

The judge stated that the elements of a criminal act as per Article 32 paragraph (1) and Article 36 of the ITE Law in conjunction with Article 51 paragraph (1) had been fulfilled. The perpetrator was sentenced to 1 year and 7 months in prison and a fine of Rp. 10 million, subsidiary to 1 month in prison. This decision emphasizes that the act of illegally changing electronic documents and causing harm to others is a serious crime that can be prosecuted with strict criminal sanctions.

CONCLUSION

The criminal offense of intentionally and without authorization to change another person's electronic documents is regulated in the Electronic Information and Transactions Law (UU ITE). Specifically, the relevant article is Article 32 paragraph (1) of the ITE Law, which regulates criminal sanctions for any person who intentionally and without authorization or unlawfully changes, adds, reduces, transmits, damages, removes, moves, or hides electronic information and/or electronic documents belonging to another person or the public. The perpetrator can be threatened with a maximum prison sentence of 10 years and/or a maximum fine of IDR 5 billion. Changes to electronic documents are carried out with the aim of making the document considered authentic data. The goals can vary, for example to deceive, falsify identity, or gain profit from the changed document. Protection of electronic documents is very important because more and more transactions and information are carried out electronically. Changes to electronic documents can be detrimental to individuals, organizations, and even the state. Meanwhile, changing another person's electronic documents intentionally and without authorization is a criminal offense regulated in the ITE Law. The perpetrator can be threatened with imprisonment and a fairly heavy fine. It is important to always be careful and respect the rights of others when using electronic documents.

Criminal liability for perpetrators of criminal acts who intentionally and without authority change electronic documents belonging to others resulting in losses to others, can be ensnared by the Electronic Information and Transactions Law (ITE Law). The ITE Law regulates criminal sanctions for various actions related to electronic data manipulation. The relevant articles in the ITE Law related to illegal changes to electronic documents include Article 27, Article 30, Article 32, Article 35, and Article 65. These articles regulate: a) Article 27: Prohibition on distributing, transmitting, and/or making accessible electronic information that has content that violates morality, gambling, insults, or defamation; b) Article 30: Prohibition on unauthorized access to another person's computer or electronic system; c) Article 35: Prohibition on falsifying electronic data; d) Article 65: Prohibition on using personal data that does not belong to him. Meanwhile, the sanctions, the perpetrator can be subject to imprisonment and/or a fine, the amount of which varies depending on the article violated and the level of loss caused. As in the Central Jakarta Court Decision Number 724/Pid.Sus/2023/PN Jkt.Pst, the panel of judges referred to Article 36 in conjunction with Article 32 paragraph (1) in conjunction with Article 51 paragraph (1) of the Republic of

Jurnal Info Sains : Informatika dan Sains
Volume 15, Number 01, 2025, DOI 10.54209/infosains.v15i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Indonesia Law Number 19 of 2016 concerning Amendments to the Republic of Indonesia Law Number 11 of 2008 concerning Electronic Information and Transactions.

SUGGESTION

Although Article 32 of the ITE Law already regulates this crime, suggestions for further regulation may include: a) Expanding the Scope of the Article: Expanding the scope of the article to cover all forms of electronic data manipulation, including changes made indirectly through a system or network; b) Clearer Definition: Providing a clearer definition of "without rights" and "against the law" in the context of electronic data manipulation. This is to avoid multiple interpretations and ensure fairness in law enforcement. c) Increasing Criminal Sanctions: Increasing criminal sanctions for perpetrators, especially in cases that result in significant losses or involve sensitive data. Currently, the maximum criminal penalty is 8 years' imprisonment and/or a maximum fine of IDR 2 billion, but these sanctions may need to be adjusted to developments in technology and cybercrime. The public is urged to be more careful in protecting their electronic documents and electronic systems; Electronic system service providers need to improve security systems to prevent hacking and data manipulation; Law enforcement needs to take firm action against perpetrators of electronic crimes to provide a deterrent effect.

REFERENCES

Arief, Barda Nawawi. *Mayantara Crimes.* Jakarta: Raja Grafindo Persada, 2007, p. 19

Delvyan Putri Surya Ningrum, Jamiatur Robekha, Legal Analysis in Cyber Crime Cases Against Internet Banking in Indonesia, *Journal of Education, Social and Humanities* , Vol.2, No.4, June 2023, P. 765

https://www.google.com/search?client=firefox-be&q=dokumen+elektronik/diakses-1-Juli-2025

https://www.google.com/search?client=firefox-be&q=elektronik+document+related+crimes/accessed-1-Juli-2025

Ina Heliany, Wonderful Digital Tourism Indonesia and the Role of the Industrial Revolution in Facing the Era of the Digital Economy 5.0, Destinesia Journal of Hospitality and Tourism, Vol. 1, No. 1, September 2019, p. 22

Article 263 paragraphs (1) and (2) Criminal Code

Article 51 paragraph (1) in conjunction with Article 35 of Law Number 19 of 2009 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

Central Jakarta District Court Decision Number 724/Pid.Sus/2023/PN Jkt.Pst

Soerjono, Soekanto, *Introduction to Legal Research* , Jakarta: UI Press, 2010, p. 81

Sry Wahyuni, Elwidarifa Marwenny, *Legal Review of the Criminal Act of Threats in the Electronic Information and Transactions Law (Case Study of the Koto Baru District Court),* Uir Law Review, Vol 4 Issue 2, 2020, pp. 15-24