JISS Journal of Indonesian Social Science

Vol. 5, No.1, January 2024
E-ISSN: 2723-6692
P-ISSN: 2723-6595
http://jiss.publikasiindonesia.id/

Obstacles and Solutions in Law Enforcement Against the Crime of Electronic Data and Information Falsification

Faisal Santiago, Endro Satoto
Universitas Borobudur, Indonesia
Email : faisalsantiago@borobudur.ac.id, endro91@gmail.com

KEYWORDS
criminal act; falsification of data and information; electronic transactions

ABSTRACT
The criminal act of falsifying data via the internet is included in the category of cybercrime and still faces obstacles in law enforcement. The formulation of the problem in this research is about the factors that cause criminal acts of falsifying information data and electronic transactions, law enforcement against perpetrators of criminal acts of falsifying information data and electronic transactions, as well as the obstacles faced in law enforcement against perpetrators of criminal acts of falsifying information data and electronic transactions, and how to overcome them. The author uses an empirical juridical approach, using primary and secondary data. Data analysis uses qualitative analysis. The research results show that: Law enforcement against perpetrators of criminal acts of falsifying information data and electronic transactions is divided into three, namely preemptive, preventive, and repressive. The obstacles faced in law enforcement against perpetrators of criminal acts of falsifying information data and electronic transactions are divided into internal obstacles, namely the limited number of investigators, high operational costs, and lack of optimal coordination between the police and other related parties. Meanwhile, external obstacles include the lack of evidence obtained from the victim, the majority of witnesses not knowing who the person was, when, what they were using, and the reason the account was created, and a lack of legal awareness from the public.

1. Introduction

The Republic of Indonesia is a state of law (rechtsstaat), namely a state in which all attitudes, behavior, and actions, whether carried out by the authorities or by its citizens, must be based on law.(Kranenburg dan Sabroedin B, 2017) The Indonesian rule of law is a state based on Pancasila and the 1945 Constitution of the Republic of Indonesia, an agreement to form a state government, protect the entire nation and all bloodshed, promote the general welfare, and make the life of the nation

intelligent. The Indonesian rule of law is a modern rule of law, in connection with which the government's main task is to improve the welfare of its people. That is why the modern Law State is also called the Welfare State (Hartono & Maryanto, 2018).

One form of crime that often occurs in society is fraud and embezzlement. For individuals, this criminal act is not that difficult to carry out. Fraud can be carried out simply by using good communication skills so that someone can convince other people. The crime of fraud is a crime that involves personal possession of objects or items. Fraud is a form of sell-out. The general characteristic of a sale of promises is that the person has made a mistake, and therefore he is willing to give up the goods or money. According to Tri Andrisman, the crime of fraud is a "material delict", meaning that for it to be perfect, consequences must occur.(Tri Andrisman., 2011)

Along with the development of computerized technology, criminal acts of fraud have transformed following digital developments, namely the criminal act of falsifying data in electronic transactions. Globalization has driven the birth of the era of information technology development. The phenomenon of data falsification in information technology has spread in almost all parts of the world. It includes developing countries such as Indonesia, which cannot be separated from the existence of certain individuals who misuse technological sophistication to gain personal or group profits in violation of statutory regulations (Rachman, 2019).

Efforts to anticipate the bad possibilities posed by the Internet have been made by the Government of the Republic of Indonesia together with the DPR with the promulgation of Law Number 19 of 2016 concerning Information and Electronic Transactions. Article 3 of the ITE Law, it is states that "The use of information technology and electronic transactions is carried out based on the principles of legal certainty, benefit, prudence, good faith and freedom to choose technology or be technology neutral.(R. Soesilo, 1994).

One of the negative impacts of the development of computerized technology is data falsification. Falsification of this data can be in the form of personal documents (documents that concern individual interests, for example, profile photos, activity documentation, birth certificates, family cards, STTB, charters, KTPs, driver's licenses, marriage certificates, etc.); commercial documents (documents related to commerce, for example, checks, bonds, receipts, money orders, shares, etc.) (Purba, 2022).

The criminal act of falsifying data via Internet media is included in the category of cybercrime, which can be carried out either by a person (individual) or as an organization (coordinated). According to Lamintang, cybercrime is a term that refers to criminal activity in which a computer or computer network is the tool, target, or place where the crime occurs. The existence of cybercrime has become a threat to stability, making it difficult for the government to compensate for criminal techniques carried out using computer technology, especially internet and intranet networks. In its implementation, cybercrime allows for formal offenses and material offenses.(P.A.F Lamintang dan Djisman Samosir, 2010).

The latest data shows that, from 2017 to 2022, the CekRekening.id service from the Ministry of Communication and Information has received approximately 486,000 reports from the public related to information crimes and electronic transactions. Of the 486,000, the type of fraud that dominates is online transaction fraud approximately 405,000 reports. "After that, it was followed by fictitious online investment fraud with a total of approximately 19,000 and online buying and selling fraud with 12,000 reports," said the person in charge of the ITE Criminal Complaints Service.(P.A.F Lamintang dan Djisman Samosir, 2010).

This case of data falsification began with the defendant deliberately, and without right or against the law, manipulating, creating, changing, eliminating, and destroying Electronic Information and/or Electronic Documents to assemble the information considered authentic data, to pursue profit. personal donations and fundraising, which is mostly done through social media. Then, the defendant created an Instagram social media account and chose the figure of a celebrity who was considered to have many fans and often appeared on television shows. The suspect's actions will be

subject to sanctions under Article 45 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (Arsanudin, 2016).

Barriers to proof in criminal cases, due to advances in technology, especially information technology, regarding the issue of how technological products, especially electronic data, are positioned as evidence, considering that the proof system in Indonesia currently still uses legal provisions that do not include electronic data as false. one type of valid evidence (Natasha et al., 2023). The use of evidence based on Article 184 paragraph (1) of the Criminal Procedure Code, which is felt to be less effective in achieving proof of cyber crimes, for example in a case of "data falsification" in electronic transactions, is very difficult to present witnesses as formulated in Article 27 paragraph 1 KUHAP, witnesses, especially victim-witnesses, are limited to only knowing and feeling the consequences of the criminal act, not the process of the act that gave rise to the felt consequences, even though to track down the perpetrator of the criminal act, there must first be a report from the victim to the authorities for further investigation (Wibisono, 2021). According to Sitompul, without a report, it is very unlikely that a cybercrime case has occurred. (Josua Sitompul., 2012).

2. Materials and Methods

The method used in writing this applied paper is a descriptive-analytical method, namely by using data that clearly describes problems directly in the field, then analysis is conducted, and then conclusions are drawn to solve a problem. The data collection method is through observation and literature study to obtain solutions to problems in preparing this paper. In line with the research objectives to be achieved, the domain of this research is included in the realm of qualitative research, thus a qualitative approach method will be used. According to Soerjowinoto et al., qualitative methods are methods that emphasize the process of researchers' understanding of problem formulation to construct a complex and holistic legal phenomenon. (Petrus Soerjowinoto, 2006).

3. Result and Discussion

Law Enforcement Against Perpetrators of Criminal Acts of Falsification of Information Data and Electronic Transactions, Obstacles and Solutions.

The act of forgery is classified as a crime of fraud if a person describes an item (c.q. a letter) as if it were genuine, even though he does not have the truth or truth. Because of the description of this data, other people are deceived and believe that the situation described in the goods/letters/data is genuine. Forgery of writing/data occurs if the content or data is incorrect.(Chazawi, 2002).

The various types of counterfeiting acts contained in the Criminal Code include:

a. apart from recognizing the principle of the right to guarantee the truth/authenticity of data/letters/writings, the act of falsifying said data/letters/writings must be "carried out with malicious intent"
b. because the evil purpose is considered too broad, it must be implied that the perpetrator must have the "intention/purpose" to create the perception that something that is faked is genuine.

An act of forgery can be punished if there is a violation of collateral/trust in cases where:

1) The perpetrator has the intention/purpose of depicting an untrue situation as if it were true using data that is not genuine as if it were genuine so that other people believe that the data is authentic and therefore other people are deceived.
2) The element of intent/intention does not need to include the element of benefiting oneself or others (in contrast to various types of fraudulent acts).
3) However, the act must cause a general danger, specifically in falsifying data/letters and so on, formulated with the public "possible loss" related to the nature of the data/letters.

On a network, data copying can be done easily without having to obtain permission from the data owner. Only a small part of the information and data on the internet cannot be "retrieved" by internet users. Theft is no longer just taking tangible goods/materials but also includes taking data

illegally. The term manipulating data is known as The Trojan horse which has the following meaning:(Hamzah, 2010).

"An act that changes data or instructions in a program, deletes, adds, makes data or a program unreachable for personal/group interests." The Trojan Horse can now be carried out online (via a network system). This makes it possible for someone to commit criminal acts of forgery targeting companies or banking database systems that use network technology.

The perpetrator in this criminal act utilized the function of the internet as a public medium which he misused for his own or his group's interests. Information technology currently makes it possible for parties (including the press) to commit this offense. The use of websites as a publication tool on the internet is considered very effective. In fact, in the future, the probability that the publication function of the internet become the most important mediator of information.(Hamzah, 2010).

If it is related to the offenses in the Criminal Code, then data diddling can be categorized as an act without the authority to falsify letters/fabricate letters. In Article 35 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, it is implied that acts of data falsification are included in:

"Every person intentionally and without right or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are treated as if they were authentic data."

The sanctions for perpetrators of criminal acts of falsifying electronic data and information are regulated in Article 45 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, as follows:

Article 45

(1) Every person who intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain content that violates decency as intended in Article 27 paragraph (1) shall be punished by a maximum imprisonment 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).
(2) Any person who intentionally and without authorization distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing gambling content as intended in Article 27 paragraph (2) shall be punished with a maximum imprisonment of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).
(3) Every person who intentionally and without right distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing insulting and/or defamatory content as intended in Article 27 paragraph (3) shall be punished with a maximum prison sentence of 4 (four) years and/or a maximum fine of Rp. 750,000,000.00 (seven hundred and fifty million rupiah).
(4) Any person who intentionally and without authority distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents containing extortion and/or threats as intended in Article 27 paragraph (4) shall be punished by imprisonment. A maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).
(5) The provisions as intended in paragraph (3) constitute a complaint offense.

Article 45A

(1) Every person who intentionally and without right spreads false and misleading news which results in consumer losses in Electronic Transactions as intended in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of IDR 1,000,000. 000.00 (one billion rupiah).
(2) Any person who deliberately and without right disseminates information aimed at causing feelings of hatred or enmity towards certain individuals and/or community groups based on ethnicity, religion, race, and inter-group (SARA) as intended in Article 28 paragraph (2) shall be

sentenced to imprisonment for a maximum of 6 (six) years and/or a fine of a maximum of IDR 1,000,000,000.00 (one billion rupiah).

Article 45B

Every person who intentionally and without authorization sends Electronic Information and/or Electronic Documents containing threats of violence or intimidation aimed at personally as intended in Article 29 shall be punished by imprisonment for a maximum of 4 (four) years and/or a fine of a maximum Rp. 750,000,000.00 (seven hundred and fifty million rupiah).

Countermeasures for criminal acts of data falsification in information and electronic transactions are divided into three, namely preemptive, preventive, and repressive, including:

a. Preemptively.

Preemptive efforts carried out by the Cyber Unit/Unit III Sub Directorate V, Special Criminal Investigation Directorate of the Regional Police were carried out utilizing appeals to the public, counseling, and placing banners and stickers in strategic places to be read. The police form good cooperation with the community to find bright spots more easily regarding legal issues that exist in the community, especially regarding criminal acts of falsifying information data and electronic transactions.

b. Preventive role

It is a preventive role to prevent criminal acts of falsifying information data and electronic transactions. There are several activities carried out by the Police preventively in dealing with criminal acts of data falsification in information and electronic transactions, including Socialization Activities in the Community.

Socialization activities are held every Saturday. After providing outreach to the public, it was continued by conducting questions and answers regarding the theme raised, namely overcoming law enforcement against criminal acts of falsifying data in information and electronic transactions. Apart from that, the public is allowed to provide suggestions and criticism.

c. Repressively.

The repressive role in criminal acts of falsifying information data and electronic transactions is carried out through investigations and investigations.

1. Investigation.

An investigation is a series of investigative actions to search for and discover an incident that is suspected of being a criminal act of falsifying data in information and electronic transactions to determine whether or not an investigation can be carried out according to the method regulated in the Criminal Procedure Code (Article 1 point 5 of Law No. 8 of 1981 concerning the Book of Criminal Procedure Law).

2. Investigation.

The investigation process that has been carried out by investigators regarding the criminal act of falsifying information data and electronic transactions, then the investigation process is carried out regarding this incident. The investigation is a series of actions by investigators for criminal acts of falsification of information data and electronic transactions which are regulated by law to search for and collect evidence of criminal acts of falsification of information data and electronic transactions to arrest suspects of criminal acts of its falsification.

Broadly speaking, the process of law enforcement involves all legal subjects in every legal relationship. Anyone who carries out normative rules or does or does not do something based on the norms of the applicable legal rules means that he has implemented or upheld the legal rules. Meanwhile, narrowly from the aspect of the subject, law enforcement can be interpreted as the efforts of certain law enforcement officials to be able to guarantee and ensure that the legal rules run as stated in the regulations. This is to ensure the upholding of the law, if necessary, law enforcement officials are permitted to use coercive measures.

The point of view of law enforcement is based on its object, namely from the legal aspect, law enforcement is understood to also include broad and narrow meanings. In a broad sense, law enforcement also includes the values of justice contained in the sound of formal rules or the values of justice that live in society. This is different in the narrow sense, then law enforcement is only limited to enforcing formal and written regulations issued by the institution authorized to issue these regulations. However, the field of law enforcement is not as beautiful as described by the legal theories and regulations that regulate it. There is more than one law enforcement problem, can discuss deeper about law enforcement and to get a clearer picture of the problem, we need to pay attention to what factors can influence the effectiveness of law enforcement.

Obstacles in Law Enforcement Against Perpetrators of Criminal Acts of Falsification of Information Data and Electronic Transactions and Their Solutions.

A constraint is a problem that causes an activity cannot run due to influencing factors. The author divides internal constraints and external constraints.

a. Internal Obstacle

1) The number of members investigating the crime of data falsification in electronic information and transactions, Cyber Unit/Unit III, Sub-Directorate V, Special Police Criminal Investigation Directorate is limited.

   The number of investigative members is very insufficient, especially with the need to have skills in the cyber field such as technology and information systems skills, as well as coding skills as the main prerequisite for identifying and tracking perpetrators of criminal acts of data falsification in information and electronic transactions.

2) Operational costs for providing data servers and IT-based training

   The available competencies are inadequate. The operational costs of providing a data server for the criminal act of falsifying data in information and electronic transactions provided by the state are considered to be very low. Efforts to investigate the perpetrators of criminal acts of falsifying data in information and electronic transactions require special servers and programs to reveal and track the whereabouts of perpetrators of criminal acts of falsifying data in information and electronic transactions. Of course, this requires costs that are not cheap. Moreover, with the limited capabilities of investigators and the need to participate in several special trainings related to mastering IT-based competence, this increases the financial burden on the Cyber Unit/Unit III Sub Directorate V, Special Police Criminal Investigation Directorate.

3) Insufficient coordination between investigators from Cyber Unit/Unit III Sub Directorate V, Special Criminal Investigation Directorate of the Police with cellular operators or internet service providers.

Currently, the police have implemented countermeasures in the form of a bilateral agreement between the Cyber Unit/Unit III Sub Directorate V, the Police Special Criminal Investigation Directorate, and all cellular telephone service providers. electronically it is still difficult to trace and prove because the identities used by perpetrators often change and use different KTPs.

b. The external obstacles faced by investigators of the Crime of Data Falsification in Information and Electronic Transactions, Cyber Unit/Unit III, Sub Directorate V, Special Police Criminal Investigation Directorate, include:

1) Minimal evidence obtained from the victim.
2) The majority of witnesses did not know who the person was, when, what they were using, and why the account was created.
3) Lack of legal awareness from the public. This is because the amount of material loss due to falsification of data in electronic information and transactions is often small in nominal amounts so that the victim is reluctant to report the incident to the police, even though the victim or the public should be obliged to report every incident of the criminal act of falsifying data in

information and electronic transactions to the police. whatever material losses he experienced for police data.

4) Lack of information from witnesses questioned in cases of falsification of electronic data and information. The lack of information from witnesses regarding criminal acts of data falsification in electronic information and transactions will make it difficult for the Cyber Unit/Unit III Sub Directorate V, Special Police Criminal Investigation Directorate to collect evidence and facts about what happened which are listed on websites, accounts or online media the perpetrator.

Efforts or solutions made to overcome the obstacles faced in law enforcement against perpetrators of criminal acts of falsifying information data and electronic transactions begin with internal and external improvements, namely:

a. Internal efforts.

Namely by accepting new members in the Cyber Unit/Unit III Sub Directorate V, Special Criminal Investigation Directorate of the Police who are expected to be able to overcome the IT-based competency gap and are expected to answer the challenges of disclosing and tracking the hiding place of the perpetrator of the criminal act of falsifying data in current information and electronic transactions. The perpetrator is in online mode and is carrying out fraudulent acts using other people's data/identity to carry out his crime.

b. External efforts.

The external efforts undertaken are:

a. Carrying out legal outreach efforts to the public regarding the importance of law enforcement against criminal acts of falsifying information data and electronic transactions.
b. Analyze other comparative evidence such as photos, telephone/cellphone numbers, e-mails, and friendships. Tracking OTP code/account.

4. Conclusion

Based on the provisions of Article 1 Number 5 of Law Number 18 of 2017 concerning the Protection of Indonesian Migrant Workers. Protection of Indonesian Migrant Workers means all efforts to protect the interests of Prospective Indonesian Migrant Workers and/or Indonesian Migrant Workers and their families in ensuring the fulfillment of their rights in all activities before work, during work, and after work in legal, economic and social aspects.

Law enforcement against criminal acts of data falsification in electronic information and transactions is divided into three, namely preemptive, preventive, and repressive. Preemptive efforts carried out by the Cyber Unit/Unit III Sub Directorate V, Special Criminal Investigation Directorate of the Police are usually carried out through appeals to the public, counseling, and placing banners and stickers in strategic places to be read. The preventive role is a preventive role so that criminal acts of falsification of information data and electronic transactions do not occur, namely in the form of Socialization Activities in the Community. Meanwhile, it plays a repressive role in criminal acts of falsifying internal data

information and electronic transactions through investigative and investigative actions. However, most cases of electronic data and information falsification are resolved through mediation/non-penal measures which are considered more fair effective, and efficient.

The obstacles faced in law enforcement against perpetrators of criminal acts of data falsification in information and electronic transactions are:

a. Internal Constraints are:

1) The number of members investigating the crime of data falsification in electronic information and transactions, Cyber Unit/Unit III, Sub-Directorate V, Special Police Criminal Investigation Directorate is limited.
2) Operational costs for providing data servers and available IT competency-based training are inadequate.
3) Insufficient coordination between investigators from Cyber Unit/Unit III Sub Directorate V, Special Criminal Investigation Directorate of the Police with cellular operators or internet service providers.

b. External constraints are:

1) Minimal evidence obtained from the victim.
2) The majority of witnesses did not know who the person was, when, what they were using, and why the account was created.
3) Lack of legal awareness from the public.
4) Lack of information from witnesses questioned in cases of falsification of electronic data and information.

Efforts to overcome the obstacles faced in law enforcement against criminal acts of data falsification in information and electronic transactions are:

a. Internal efforts by recruiting new members to the Cyber Unit/Unit III Sub Directorate V, Special Criminal Investigation Directorate of the Police.
b. External efforts, namely:

1) Carrying out legal outreach efforts to the public regarding the importance of law enforcement against criminal acts of falsifying information data and electronic transactions.
2) Analyze other comparative evidence such as photos, telephone/cellphone numbers, e-mails, and friendships. Tracking OTP code/account security code.

5. References

Arsanudin, L. O. (2016). *PENEGAKAN HUKUM DALAM PEMANFAATAN TANAH UNTUK KEPENTINGAN PEMBANGUNAN REAL ESTATE DI KOTA SEMARANG*. Fakultas Hukum UNISSULA.

Chazawi, A. (2002). *Pelajaran Hukum Pidana*. PT Raja Grafindo Persada.

Hamzah, A. (2010). *Asas-Asas Hukum Pidana*. Rineka Cipta.

Hartono, D., & Maryanto, M. (2018). Peranan Dan Fungsi Praperadilan Dalam Penegakan Hukum Pidana Di Polda Jateng. *Jurnal Daulat Hukum*, *1*(1).

Josua Sitompul. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Tata Nusa.

Kranenburg dan Sabroedin B. (2017). *Ilmu Negara Umum*.

Natasha, C., Akli, Z., & Johari, J. (2023). PENEGAKAN HUKUM TERHADAP PELAKU TINDAK PIDANA PENYEDIAAN DAN PENGGUNAAN ALAT SWAB ANTIGEN BEKAS DI BANDARA INTERNASIONAL KUALANAMU. *JURNAL ILMIAH MAHASISWA FAKULTAS HUKUM UNIVERSITAS MALIKUSSALEH*, *5*(3).

P.A.F Lamintang dan Djisman Samosir. (2010). *Delik-delik Khusus Kejahatan yang Ditujukan Terhadap Hak Milik dan lain-lain Hak yang Timbul dari Hak Milik*. Tarsito.

Petrus Soerjowinoto, D. (2006). *Buku Panduan Metode Penulisan Karya Hukum (MPKH) dan Skripsi*. Fakultas Hukum,UNIKA Soegijapranata.

Purba, B. J. (2022). HAMBATAN PENEGAKAN HUKUM DALAM PELAKSANAAN JOINT INVESTIGASI DIREKTORAT JENDERAL BEA DAN CUKAI DAN DIREKTORAT JENDERAL PAJAK. *HERMENEUTIKA: Jurnal Ilmu Hukum*, *6*(1), 104–111.

R. Soesilo. (1994). *Kitab Undang-Undang Hukum Pidana (KUHP), serta KomentarKomentar Lengkap Pasal Demi Pasal*. Politea.

Rachman, B. A. (2019). *Efektivitas Penegakan Hukum Oleh Satuan Lalu Lintas Melalui Tilang Terhadap Masyarakat Yang Melanggar Lalu Lintas Di Wilayah Hukum Polres Pekalongan*. Universitas Islam Sultan Agung.

Tri Andrisman. (2011). *Delik Tertentu dalam KUHP*. Unila Press.

Wibisono, K. A. (2021). *Penegakan Hukum Terhadap Tindak Pidana Illegal Mining Di Wilayah Hukum Polda Kalimantan Tengah*. Universitas Islam Sultan Agung (Indonesia).