UNMAS DENPASAR

INTERNATIONAL PROCEEDING

INTERNATIONAL CONFERENCE FACULTY OF LAW UNIVERSITY OF MAHASARASWATI DENPASAR

"Law, Investment,Tourism And Local Wisdom"

Denpasar, 1st December 2021

Juridical Review of the Crime of Using Photos and Images Legal Hijacking of Other People's Social Media Accounts Number 19 of 2016 concerning Information and Electronic Transactions

I Nyoman Sunarta

Faculty of Law, Mahasaraswati University Denpasar,

Email: advokatsunarta@gmail.com

Abstract

Indonesian Law Number 19 of 2016 aboutInformation and Electronic Transactions (UU ITE) was born by considering the demands of the needs of information technology users, which aims to provide legal protection for information technology users who are considered the most vulnerable group to crime spread on social media, one of which is the crime of using photos and hijacking other people's social media accounts. At present, there are many cases of photo theft that are used to commit fraud and make social media a facility for these crimes, but efforts to prevent the development of these crimes are only focused on written legal texts without any systematic effort to realize what was the initial goal. This research aims to determine the juridical review of the crime of using photos and hijacking other people's social media accounts according to Indonesian Law Number 19 of 2016 about Information and Electronic Transactions. This research is a normative juridical research with secondary data. The research method uses literature study by collecting legal materials and information in the form of primary, secondary, and tertiary legal materials. To get a clear explanation, the data were then arranged systematically and analyzed using descriptive methods

Keywords: Indonesian Law about Information and Electronic Transaction, Piracy, Law Enforcement

I. INTRODUCTION

I.1 Background Of The Problem

The rapid development of globalization of information technology has made it a phenomenon interesting life, where people who use information technology in communication is no longer limited by time and place (borderless). Anytime and wherever people who use these technology devices can establish communication, obtain information, and disseminate information to others. Technology globalization

This position places the Indonesian people as part of the world community of users communication and information technology.1 The ease and sophistication of today's technology increasingly widespread and increasingly needed by all circles. Globalization of information technology

has also engineered the lives of Indonesian people into the cyber era with internet facilities

which presents cyberspace with its virtual reality offering to the public various expectations and conveniences. Information and communication technology is currently being leads to a convergence that facilitates human activities as creators, developers and users of the technology itself. One of them can be seen from the rapid development of internet media. Internet as a medium and Electronic communication has been widely used for various activities, including for e-mail browsing (browsing, surfing), looking for news, sending messages to each other via e-mail, and

trade.

The benefits of technology and information can be felt both in the education and the economy and others, matters relating to development of science, science and so on which can easily be accessed access, so that billions and even trillions of information can be received quickly. In

field of work, the management of very large amounts of data can be managed by good, fast, effective and efficient and minimize errors.In the economic field, promotions and potentials in improving people's welfare done quickly without limitation of place or region and reach all layers society both nationally and internationally. However, technological developments and This information not only provides benefits but also causes serious problems can harm the public, such as misuse of data, theft of personal data, sales of personal data, fraud and others.

Around 2008 an innovation in the internet field began to emerge in the form of a social networking site, namely www.facebook.com or better known as Facebook.Facebook is a virtual world where users can interact with each other other users from all over the world. In the Facebook social network there are several display of user's personal information such as profile photo, photo upload, personal data not even Rarely do people also flaunt their private lives in these accounts for shown and shared with other users who can access each other's uploads Facebook users who have become relations or friends to exchange information.

The exchange of information carried out within the Facebook social network allows

Users can share files, videos, and even photos of themselves. However lack of supervision in the exchange of information in the Facebook space, causing there is freedom without control by Facebook users when they want to make an exchange information. So it is often found that there are abuses and violations that carried out by irresponsible Facebook users. 4 Examples are many Facebook users who abuse it by taking photos and data Other users to commit criminal acts of fraud. Against abuse freedom of internet users in accessing and obtaining other people's personal data, it can be concluded that there are system weaknesses, and lack of supervision, so that someone's personal data can be misused and cause harm to the owner of the data. Misuse, theft, sale of personal data is a violation of law in the field of information technology and can also be categorized as violation of human rights, because personal data is part of human rights humans to be protected. In this regard, there are several examples of cases in misuse of personal data, including:

1) Capture data and hijack other users' accounts;
2) Distribute files, photos and videos without the permission of the actual owner;
3) Using other people's personal data to commit crimes;
4) Stealing other people's photos on social media and misused to commit fraud

Unauthorized use of other people's photos, without the owner's permission, and hijacking Social media accounts are criminal offenses. Misuse of personal data is an act that fulfills the elements of a criminal act such as an element of a criminal act theft and elements of criminal acts of fraud and other criminal acts both in terms of elements objective and subjective elements. With the fulfillment of these elements, the sanctions administrative sanctions, civil sanctions and criminal sanctions are not sufficient to accommodate criminal abuse of personal data which is actually a form of crime that perfect. Based on the explanation of the background above, then what becomes The problem to be researched is

I.2 Research Objectives

1. How is the law enforcement process against the perpetrators of stealing other people's photos and being wrong?
use it to commit fraud in an effort to provide legal certainty for
victim?
2. What are the obstacles experienced by law enforcers in dealing with criminal cases?
crimes related to information technology in accordance with Law No 19 of 2016 concerning Information and Electronic Transactions?

I.3 Research Method

The type of research in this case is normative legal research because the focus of the study is
departing from norms, regulations, legal theories therefore
has the task of systematizing positive law, the research method uses
literature study by collecting legal materials and information in the form of legal materials
primary, secondary, and tertiary. To get a clear explanation, the data is then
systematically compiled and analyzed using descriptive methods. Search techniques
legal materials using document study techniques, as well as study analysis using qualitative analysis.

II. DISCUSSION

II.1 The process of law enforcement against the perpetrators of theft of other people's photos and in the wronguse it to commit fraud in an effort to provide legal certainty for the victim

Because social networking services provide facilities for their users to share files, videos and even photos of each other easily, people Those who use these facilities often unknowingly commit negligence.

The omission in question, for example, unknowingly, the users of the social network have share their personal photos, videos and current location. At this time many people
compete to show his personal life on social media with the aim of
exhibit themselves and the activities that are being and/or have been carried out,
but not many people are aware of the negative impact of social media itself.

There are several negative impacts of social media, namely: 1) Decreased productivity,
2) Easy spread of fake news (hoax), 3) The rise of crime on social media, 4)

Loss of one's privacy, 5) Cause conflict. Cases that often occur today
There are many irresponsible people who easily steal
someone's photo from social media, then create a new account using their name, photo,
or the identity of another person to commit fraud by pretending to be
owner of the true identity, with the mode of borrowing money or doing
extortion of the victims themselves. This is very detrimental to social users
the media, especially the Indonesian people. These actions fall into the category of
against the law, therefore can be punished based on Article 30 paragraph (3) of the Law
Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) as referred to in
which has been amended by Law Number 19 of 2016 concerning Amendments to
Law Number 11 of 2008 concerning Information and Electronic Transactions states: "(1) Any person knowingly and without rights or against the law
access Computers and/or Electronic Systems belonging to other Persons in any way. (2)
Everyone knowingly and without rights or unlawfully accesses the Computer
and/or Electronic Systems in any way for the purpose of obtaining
Electronic Information and/or Electronic Documents. (3) Everyone intentionally and
without right or against the law accessing Computers and/or Electronic Systems by
any way by breaking, breaking through, overtaking, or breaking into the system
security." If a criminal incident occurs or there is a report of an
the crime, the officer who receives the report immediately conducts an investigation
to determine to what extent the truth of the incident. The report can be
This is done in writing which must be signed by the complainant and can also be submitted
orally.6 This is regulated in Article 43 paragraph (1) of Law Number 19 Years
2016 concerning Amendments to Law Number 11 of 2008 concerning Information and
Electronic Transactions stating: "Other than Republican State Police Officer Investigators

Indonesia, certain Civil Servant Officials within the Government within the scope of
duties and responsibilities in the field of Information Technology and Electronic Transactions
given special authority as an investigator as referred to in the Act
concerning the Criminal Procedure Code to conduct criminal investigations in the field of
Information Technology and Electronic Transactions", and regarding the investigation process
regulated in Article 43 paragraph (5), namely: "Civil Servant Investigators as referred to in
in paragraph (1) has the authority to: a. receive a report or complaint from someone about
the existence of a crime in the field of Information Technology and Electronic Transactions; b.
summons any person or other party to be heard and examined as
suspect or witness in connection with an alleged crime in the field of Technology Electronic Information and Transactions; c. carry out an examination of the veracity of the report or information relating to criminal acts in the field of Information Technology and
Electronic Transactions; d. conduct inspections of Persons and/or Business Entities
who should be suspected of committing a crime in the field of Information Technology and Transactions
Electronic; e. carry out inspections of related tools and/or facilities
with Information Technology activities suspected of being used to commit acts
crime in the field of Information Technology and Electronic Transactions; f. To do
search of certain places suspected of being used as places for
commit criminal acts in the field of Information Technology and Electronic Transactions; g.
carry out sealing and confiscation of tools and/or facilities for Technology activities
Information that is allegedly used in a manner that deviates from the provisions of the laws and regulations; h. create a data and/or Electronic System related to criminal acts in
in the field of Information Technology and Electronic Transactions so that they cannot be accessed; i. ask

information contained in the Electronic System or information generated by Electronic System to Electronic System Operators related to acts crime in the field of Information Technology and Electronic Transactions; j. ask for expert help needed in the investigation of criminal acts in the field of Information Technology and Electronic Transactions; and/or k. stop criminal investigations in the field of Information Technology and Electronic Transactions in accordance with legal provisions criminal procedure.To uncover criminal acts related to Electronic Information and Electronic Transactions, Investigators may cooperate with investigators from other countries to share information and evidence. While in terms of making arrests and detention, investigators through the public prosecutor are obliged to request a determination from the head of the court local country within twenty-four hours. In Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions contains the punishment given on the perpetrators of criminal acts, namely: "(1) Any person who fulfills the elements as referred to in Article 30 paragraph (1) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 600,000,000.00 (six hundred million rupiah). (2) Every People who meet the elements as referred to in Article 30 paragraph (2) shall be punished with a maximum imprisonment of 7 (seven) years and/or a maximum fine of IDR 700,000,000.00 (seven hundred million rupiah). (3) Everyone who meets the elements of as referred to in Article 30 paragraph (3) shall be punished with imprisonment for a maximum of 8 (eight) years and/or a maximum fine of Rp.800,000,000.00 (eight hundred million rupiah)". with the intent to unlawfully benefit oneself or another person, by using a false name or false dignity, by deceit, or a series lies, moves others to hand things over to him, or in order to give debts or write off receivables are threatened for fraud by

imprisonment for a maximum of four years".

8Victims of crime are important to protect,

First, because society is considered as a form of belief system that

(system of institutionalized trust). This trust is integrated through norms

expressed in institutional structures, such as the police, prosecutors,

court, and so on. The occurrence of a crime against the victim can be meaningful

the destruction of the belief system, so that the regulation of criminal law and law

other matters concerning the victim will serve as a means of restoring the system

that belief. Second, there are arguments for social contract and solidarity because the state

it can be said to monopolize all social reactions to crimes that forbid

personal actions. Therefore, if there are victims of crime,

then the state must pay attention to all victims by improving services

as well as rights arrangements. Third, victim protection which is usually associated with wrongdoing

one goal of punishment, namely conflict resolution. Resolution of the resulting conflict

by the existence of a crime will restore balance and bring a sense of peace

in society. Victims whose photos and identities are used by fraud perpetrators

is the party who suffers the most and is harmed, therefore it is necessary to have

a protection from the state. Victims' rights must be seen as a form of treatment

the same for everyone before the law (equality before the law). However, unfortunately

The ITE Law does not clearly regulate the protection provided to victims

for the occurrence of the crime. The ITE Law only explicitly regulates the rights

victims in the event of a criminal act in an electronic transaction, including fraud

through the internet, namely the right to settle cases and punish people who have

commit a criminal act. So that if there is misuse of personal data who is also an Indonesian citizen, it will be resolved through Indonesian law

and carried out in courts in the jurisdiction of Indonesia

resolve criminally, the injured victim can solve the problem

by filing a civil suit which is carried out in accordance with the provisions of Legislation. In addition, the parties can also resolve disputes through arbitration, or other alternative dispute resolution institutions in accordance with the provisions of the legislation. The settlement of the dispute is regulated in Article 39 of Law Number 19 of 2016 concerning Amendments to the Law Number 11 of 2008 concerning Information and Electronic Transactions.

II.2 Constraints experienced by law enforcers in handling criminal cases crimes related to information technology in accordance with Law Number 19 of 2016 concerning Information and Electronic Transactions

The Indonesian government has taken steps in an effort to dealing with cybercrimes that use technology as a crime. However, it should be realized that the legal instruments and legislation must also be adjusted with the type of crime, therefore in 2008 the Indonesian government has enact special laws to deal with cybercrimes that known as the Law on Information and Electronic Transactions (UU ITE). Invite The law is expected to be able and able to protect the public from threats cyberspace caused by technology, so it will provide security guarantees information and communication technology users. Besides that, this law will be able to ensnare cybercriminals such as credit card fraud, ATM card burglary, pornography, copyright infringement and other crimes using information technology. Even though the law is official legalized, on the other hand it is not comparable to human resources. The thing that What is meant is law enforcement officers who understand the mayantara law (cyber) and also the limited number of information technology experts such as in agencies Police. Based on the facts from the statistical results obtained by the author, the crime rate in cyberspace in Indonesia is increasing day by day. The results of the research

conducted by Dimitri Mahayana, director of the Telematics Research Institute Sharing Vision
who conducted a study in 2013 stated that Indonesia could get
42,000 cyber attacks per day. This tends to undermine security
companies and the State. He said the data showed significant vulnerabilities
needs to be improved, including through law enforcement, legal regulations, and
the establishment of a special agency that monitors the movement of internet lines or cyber troops.

The special agency intended to deal with cyber crimes or special crimes
cyberspace in Indonesia is still in the planning and discourse process. As is
a special agency in handling cyber crime cases is expected to be able to
reduce the crime in Indonesia which is getting higher and higher
the threat, the formation of a special agency for cybercrimes is also expected
involving the police as an agency that is indeed engaged in the
criminal law enforcement. In other words, in the days to come the body
This special program will be able to assist the police in uncovering and apprehending criminals
suspects who use technology as a crime tool.

Constraints experienced by law enforcement in handling criminal cases
relating to information technology in accordance with Law No. 19 of the year 2016 concerning Information and Electronic Transactions are as follows:

1) Limited personnel such as IT experts and cyber forensics
There are only Indonesian cybercrimedi investigators, while the number of members
Cyber policing in China has reached 18,000 (eighteen thousand) personnel.
So the number of personnel in charge of cyber crime in Indonesia is indeed
considered very less compared to the number of crimes that occurred in Indonesia.
Even though this type of crime has increased in recent years, it should be thickening
personnel to anticipate the negative effects of this crime carried out immediately
In addition, the Sub-directorate of cybercrime under its directorate noted,
the number of cybercrime reports in 2017 was only 781 reports. of the number

Of these, only 86 reports were successfully completed. In 2018 the number of reports
jumped to 1,347 reports with a completion of 115 reports only. As for the year
2019, there were 1,324 reports with 307 case settlements, while
During January to October 2020, there were 1,325 reports with a total number of cases
completed as many as 355;10

2) Limited number of expert personnel

Indonesia and China are very different in number
personnel. It is even more ironic that reports of cyber crime rates in Indonesia are increasing
increasing, with limited personnel and experts on the Indonesian police side
then the settlement of the case cannot be resolved quickly. As a result
directly felt by the victim or cybercrime. Quality of technological facilities
information in Indonesia is already quite good, but not comparable to
security guarantees by users. Limitations of experts on the police
indeed a very big factor, with a limited number of expert members

This disclosure and investigation of cyber crime cases cannot be resolved
in a fast time, so that it will make the perpetrators more flexible in
in action. Moreover, it is known that the number of members of the Indonesian cyber police is only
amounted to 18 people, the number is not proportional to the number of cases
included in the police report on cyber crime. Police member
still not very technology literate, even many of the cyber members
Indonesian police are still new to using computers. It can be said that the ability of the police
Indonesia in cyberspace is still in the standard or beginner stage
the need for experts must also be balanced with the availability of facilities and infrastructure as well as
sophisticated and advanced equipment facilities to support network security and
also to facilitate the tracking of criminals so that cyber crime cases
can be resolved quickly;

3) Limited operating budget

A crucial problem apart from legal instruments, namely human resources who have not

sufficient, budget and facilities and infrastructure to support disclosure
cases of cyber crime. The insufficient budget is the cause of the
very large in disclosing cybercrime cases, with limitations
budget will have a direct impact on the equipment used by the parties
the police to track down cybercriminals;
4) Weak government supervision
Weak supervision of internet use has the potential to create
opportunities for the occurrence of cyber crime (cyber world). Because of crime
by using technology occurs if there is adequate internet access.
Internet facilities in Indonesia can be said to be adequate both in terms of speed
access and ease of installation of internet access networks. With the interference
the government's hand in supervising the licensing of internet network access installations
it is hoped that the level of cyber crime can be minimized;
5) Procedural constraints of the Electronic Information and Transaction Law (UU ITE)

The rise of cyber crime cases in Indonesia is considered by many groups to exist
There are legal loopholes in Indonesia that can be exploited by perpetrators
cyber crime, Information and Electronic Transaction Law Number 19
of 2016 concerning Amendments to Law Number 11 of 2008 concerning
Information and Electronic Transactions are still not implemented effectively. Due to
law enforcers are still not too familiar with cyber crime,
so that the implementation of the ITE Law has not been maximized. There are still many enforcers
who do not understand the meaning of the ITE Law, especially regarding acts that
prohibited in articles 27 to 37. This constraint has an impact that the implementation is not optimal
the ITE Law in Indonesia. Procedural constraints are also considered as
delays in legal action for perpetrators who are strongly suspected of being perpetrators
cyber crime, Article 43 paragraph 3 of the Information and Transaction Law
Electronic Number 19 of 2016 is a stumbling block for law enforcement

itself because in this article it requires law enforcers to have a letter
prior detention permit from the local court, making it easier for the perpetrators
to destroy evidence

III. CLOSING

III.1 Conclusion

Implementation of legal policies in the law enforcement process against
perpetrators of theft of other people's photos and misused to commit fraud in an effort to
providing legal certainty for victims is currently considered not going well, because
there are still many victims who do not want to report the case, the community is the victim
feel that law enforcers have not mastered the resolution of cases related to
cyber crime, so the implementation of the ITE Law has not been maximized. Still
many enforcers do not understand the meaning of the ITE Law. In UU ITE
requires law enforcers to first obtain a detention permit from
local courts, making it easier for perpetrators to eliminate evidence.

In this regard, in addition to the need for preventive action or caution,
of each person to protect their respective data, governments and providers
services are required to make verification mechanisms clearly regulated in the form of
Constitution.

III.2 Suggestions

Given the limitations or weaknesses of the criminal law's ability to
tackling criminal acts, especially the settlement of criminal cases using photos
and hijacking other people's social media accounts, so it can be concluded that the policy
The prevention of criminal acts in Indonesia cannot only use the means of punishment
but also must use non-penal means. Thus, it is quite reasonable to
continuously explore, utilize and develop non-penal efforts to
compensate for the shortcomings and limitations of these penal facilities. Law enforcer
are expected to play an active role in preventing criminal acts of using personal data

as well as the theft of photos and hijacking other people's accounts that are used to
commit a crime by an irresponsible party. Besides that
harmonize the laws and regulations so that there is no overlap
overlap between one rule and another. So that law enforcement is expected
can cover the gaps in the ITE legislation that is often an obstacle
procedures for law enforcement. With regard to the things that have been described
above, the researcher proposes that there must be the formation of norms that regulate sanctions
criminal law in its enforcement as a deterrent effect by making a special procedural law
in the settlement of criminal cases related to Information and Electronic Transactions
so as to provide a deterrent effect to the perpetrators and the victims
justice

REFERENCES

Book

Detik News, (2014). Penanganan Kasus Cyber Crime Terganjal Regulasi dan Anggaran., Detik News, Kiswondari, (2021).Panduan Kapolri Belum Sentuh Akar Permasalahan UU ITE.SINDO News, Ramli, Ahmad M. (2004) Cyber Law dan HAKI dalam Sistem Hukum Indonesia. Setiawan Radita, A. M. (n.d.). Efektivitas Undang-Undang Informasi dan Transaksi Elektronik., 139-145 Situmeang, Sahat Maruli Tua, (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber., S A S I, 27.1 (2021), 38-52 Soesilo, R. (1995). Kitab Undang-Undang Hukum Pidana**Journal**

Susrama, I Nengah; Sukma, Putu Angga Pratama, 'Pelaksanaan Courtroom Television Dalam Peradilan Pidana Dengan Agenda Saksi', *Jurnal Hukum Sasana*, 5.1 (2019), 61–74 <https://doi.org/https://doi.org/10.31599/sasana.v5i1.92>

News

Reza Efendi, 'Densus 88 Sita Pisau Hingga Busur Panah Saat Penangkapan Terduga Teroris Di Sumut', *Liputan 6*, 2020 <https://www.liputan6.com/regional/read/4510915/densus-88-sita-pisau-hingga-busur-panah-saat-penangkapan-terduga-teroris-di-sumut>