



Criminal Liability Of Misuse Personal Identity Number For Cellphone Cards Registration Illegally

Ubait Kurniawan Aziz¹, Nur Azizah Hidayat²

¹Faculty of Law, University of Muhammadiyah, Surabaya - Indonesia. Email: ubait.kurniawan.aziz-2018@fh.um-surabaya.ac.id

²Faculty of Law, University of Muhammadiyah, Surabaya - Indonesia. Email: nurazizah.hidayat@fh.um-surabaya.ac.id

ABSTRACT

The telecommunication network is a necessity needed today and ever after. This momentum is exploited by several cheaters who looking for big profits. One bad trick is to misuse someone else's ID card to register a cellphone SIM Card so it can be sold faster. And that's actually against not only Law no. 24 of 2013 concerning Population Administration but also Law No. 19 of 2016 concerning Amendments to Law no. 11 of 2008 concerning Information and Electronic Transactions. The regulations about criminal liability misuse of ID cards by another person for registration cellphone SIM cards do not get serious attention from the government. Therefore, the purposes of this research are: (1) to analyze the criminal liability of misusing Personal Identity numbers and Family Identity numbers for cellphone cards registration illegally is an act of crime in Indonesia; (2) to analyze and compare the laws and regulations concerning misuse other people's Identity Number and Family Identity Number for cellphone card registration based on the ITE Law and the Population Administration Law. This research uses normative legal research, while methods use Statute Approach and Conceptual Approach. The results of this research found criminal liability sanctions for misuse of someone else's Personal Identity Number and Family Identity Number for registering cellphone SIM Cards illegally based on the ITE Law, the Criminal Code Law, and the Population Administration Law.

Keywords: Cellphone Card; Criminal Liability; Personal ID

Citation: Aziz, Ubait Kurniawan, and Nur Azizah Hidayat. 2022. "Criminal Liability Of Misuse Personal Identity Number For Cellphone Cards Registration Illegally". *Mulawarman Law Review* 7 (1), 17-30. <https://doi.org/10.30872/mulrev.v7i1.790>.

INTRODUCTION

Today information technology systems are becoming more and more sophisticated, this has penetrated the realm of trade, entertainment industry, transportation, government systems, and also the financial industry. The scope of information technology systems starts from collecting, storing in warehouses, processing, and distributing goods, beginning from industrial locations being delivered to user's address efficiently and effectively¹. One of the advancements in the field of technology is the rise of various applications contained in our gadgets. The development of the

¹ Shinta Dewi. (2015). *Aspek Data Privacy Menurut Hukum Internasional, Regional dan Nasional*. Bandung: PT Refika Aditama, p.33

digital era causes all affairs to change from offline to online and it causes people to depend on the importance of the internet². If we want to operate many useful gadget applications in our daily activity, we need an internet quota that is provided by the phone card company. The development of technology and information made some positive and negative impacts. Among the negative impacts are data misuse, sales of personal data, theft of personal data, fraud, and others. The leak of personal data can cause a big effect on its users³.

However, there are many deficiencies to protect Personal Identity Numbers and Family Identity Numbers as contained in ITE Law. Once a time author was offered a former Telkomsel salesperson who had a Microsoft Excel file in which there was 20,000 Personal Identity Number/Family Identity Number. In 2019, even trading of Personal Identity Numbers/Family Identity Numbers has also been widespread on social media Facebook, Twitter, and other social media⁴. This problem does not stop and in 2021 there is the same problem done at Banda Aceh. Aceh's Police found 1 store with the initials SP in Banda Raya District, Banda Aceh City, from the results of the raid with evidence such as 20 boxes of Loop cards, 2 boxes of Axis Cards, 6 boxes of as starter packs, 4 boxes of Telkomsel Cards (active), 12 boxes of Telkomsel Cards (unregistered), 1 unit of Lenovo computer, 4 units of Laptops (active), 5 units of Modem Loop (active), and 2 Modem Loop units (damaged). Meanwhile, the results of the raid in the Aceh Tamiang area, with evidence such as 3 units of silver DELL brand laptops, 6 units of red and black SANDISK flash disks, 4 units of black FOXCOM brand modem pools, 3 units of black LEKA brand modem pools, 10 units of laptop chargers. Then 1 unit of black RAEAN brand monitor, 1 unit of black POWER UP brand keyboard, 25 boxes Telkomsel of 25 GB cards, 13 boxes Telkomsel of 6.5 GB cards, 3 boxes Telkomsel of 15 GB cards, 18 boxes AXIS cards each containing 1000 pieces.⁵ In 2022, this problem does not decrease with data stating that not only patient personal data but also included patient medical records collected from various hospitals were sold freely on the RaidForum website. The number of patients whose data was found leaked reached 6 million patients with a size of up to 720GB⁶.

The author also works as a salesperson for the TRI card operator (3) in the Tenggilis District area, Surabaya City. Because of personal data leaks, sometimes customers felt that they only used their Identity Number and Family Identity Number identities on one SIM Card, but when they buy a SIM Card from another cellular operator and used their Identity Number and Family Identity Number, they did not register successfully

² Priyantono & Mardi. (2017). *Digital Mastery, Membangun Kepemimpinan Digital Untuk Memenangkan Era Disrupsi*. Jakarta: PT. Gramedia Pustaka Utama, p.41

³ Paul Marett. (2002). *Information Law in Practice*, Edisi ke-2. London: MPG Books, p.95

⁴ Kompas. (2019). *Harian Kompas*. <https://nasional.kompas.com/read/2019/07/30/14193401/ada-jual-beli-data-kk-dan-nik-di-medsos-kemendagri-lapor-ke-bareskrim-polri> [Accessed April 4, 2022].

⁵ Pelopor. (2021). 'Harian Pelopor'. <https://pelopor.id/2021/10/19/polisi-ciduk-penjual-sim-card-yang-gunakan-data-orang-lain> [Accessed May 25, 2022].

⁶ Bisnis.com, (2022). 'Harian Bisnis', <https://kabar24.bisnis.com/read/20220109/15/1486824/data-pribadi-bocor-lagi-ruu-perlindungan-data-pribadi-makin-mendesak> [Accessed June 2, 2022].

because the notification from the operator stated that their Identity Number and Family Identity Number has been used a maximum of 3 times. It was not the customer who used his Identity Number and Family Identity Number for registration to activate the purchased cellphone SIM Card. Outlet sellers sometimes do anything against the law including misuse of other Personal Identities for cellphone card registration. Of course, their motives are getting a low price, avoiding losses, and seeking maximum profit. The purposes are that the phone SIM card sells well and is not expired. And that way it opens/ broke the cellphone SIM card seal and then activates it, and that register it using someone else's ID illegally.

Personal Identity Number is personal data owned by a person and their confidentiality must be protected because they contain personal elements that cannot be shown to the public. ID cards and Family Card can be used in various public facilities, for example, to get some jobs, education, medical health records, ownership of assets, accounts payable, and so on. So that if they fall into criminal or cheaters, their Identity Number can be misused without the owner's permission. An important element of the information systems business that is currently booming is maintaining data security owned by customers. Many cases of leaks regarding data manipulation have become one of the serious problems in law enforcement in Indonesia especially concerning ITE Law enforcement. These cases including adding or subtractive data, creating customer profiles, integrating global consumer data, and other business mechanisms were done illegally and violated the law.⁷

In another case, the use of a cellphone card that is registered using someone else's identity can have an impact on the weak verification system of the Go-Jek application in the process of registering a Go-Jek Application user account, so that everyone can have a Go-Jek Application account without a clear identity or use someone else's identity⁸. In addition, now many people are starting to use online loans because in this era no need to meet creditors but only using the internet, everything can be fast and easier. Even people no longer need to go to the bank and apply directly to get a loan. With this convenience, many people choose online loans instead of having to borrow at a bank. From this convenience arises a loophole in the criminal act of fictitious online loans that log in using a phone card from someone else's identity⁹. This concerns the protection of personal data until now there is no law that clearly and specifically regulates this. So, if this is allowed, it will certainly harm Indonesia. The development of information technology and the continued increase in internet service

⁷ Shinta Dewi. (2016). "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia". *Jurnal Yustisia*, Vol.5(1), pp. 22-30

⁸ Aditya Hermawan, Syukri Hidayatullah, Erna Susanti. (2018). "Legal Protection of Go-Jek Driver That Experiences Damages Due To The Fictive Order In Go-Food Menu In Go-Jek Application", *Mulawarman Law Review*, Vol. 3(2), pp. 124–132

⁹ Anggraini Dila Pitaloka. (2020). "Pertanggungjawaban Pidana Pelaku Pinjaman Online Yang Berimplikasi Tindak Pidana", *Jurnal Jurist Diction*, Vol. 3(5). pp. 1597–1616

users in Indonesia increasingly show the need for special arrangements to protect personal data privacy for Indonesians¹⁰.

Based on the Decree of Indonesian Telecommunications Regulatory Body Number 03 of 2018 Article 1 letter (d) it is stated that everyone who has one Personal Identity Number and Family Identity Number can only use 3 cellphone SIM cards from various cellular operators. For example, a man named "X" with Personal Identity Number "Y" and Family Identity Number "Z" for example can only use their identity for 1 MSISDN Telkomsel, 1 MSISDN XL, and 1 MSISDN Indosat. If you want to change to a new AXIS card, the resident named "X" must confirm UNREG at one of the Telkomsel/ XL/ Indosat outlets so that they can use the Personal Identity Number "Y" and Family Identity Number "Z" for registration on the new AXIS card. However, there is also one Personal Identity Number and Family Identity Number that is used by more than 3 cellphone SIM cards, and even 50 cellphone SIM cards or even more are used through certain registration systems.

Furthermore, in the same context, Indonesia already has some regulations concerning the restriction and limitation of SIM Card registration, as stipulated in Law Number 19 of 2016 concerning Information and Electronic Transactions¹¹ and Law Number 24 of 2013 concerning Population Administration¹². The two laws above, it is related to the Personal Identity Number and Family Identity Number because if the Personal Identity Number and Family Identity Number are written in certain electronic media such as cell phones and are used for trading transaction activities, then they are included in information and/or electronic documents. As explained in the Population Administration Law article 1 paragraph 4 where the meaning of an Electronic Document is data in the form of electronic information that is created and stored until it transfers through a digital form or the like that can be seen, heard, or visualized via computer media or other gadgets. The intended electronic information is not only limited to images, sounds, or writing but also access passwords or other passwords that can be understood by someone else. This is a concern of the Ministry of Communication and Information (Kominfo) and also the Ministry of Domestic Affairs as a protective agency for a person's Identity Number/Family Identity Number so that unscrupulous persons are not used.

This research has been compared with another research. One of them is research from Anggraini Dila Pitaloka, a student from Airlangga University. Her journal-title is "Criminal Accountability of Online Loans with Criminal Implications" which is published in *Jurist Diction* Volume 3 No. 5, September 2020. In her journal, she discusses a new business model in Indonesia, named peer-to-peer (P2P) lending or information technology-based (online) loan services. So online loans do not escape cheating actors

¹⁰ Sasongko, et. all. (2020). 'Konsep Perlindungan Hukum Data Pribadi Dan Sanksi Hukum Atas Penyalahgunaan Data Pribadi Oleh Pihak Ketiga', *Proceeding of Conference on Law and Social Studies*, Vol. 1(1). pp. 16–27

¹¹ Indonesia. *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*.

¹² Indonesia. *Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan*.

who commit fraud, including using someone's ID card to be manipulated to get loan funds. It has the same theme of misusing personal data, but different activities misuse personal data between online loans and cellphone card registration.

Secondary, this research is compared with research from the Concept of Legal Protection of Personal Data and Legal Sanctions for Misuse Personal Data by Third Parties. That journal is written by Sasongko as the main author from PGRI Madiun University which is published in the Journal of the Proceeding of Conference on Law and Social Studies Faculty of Law – Universitas PGRI Madiun in December 2020. In his research, they discussed victims whose personal data was misused so that they took legal action to make compensation because they had been harmed.

The author's research is something brand new research that compared with two previous research. The first research discusses the object of personal data research that is being misused for online loans that are currently rife in society. Meanwhile, the author's research specifically discusses the misuse of Personal Identity Numbers and Family Identity Numbers in the form of electronic transactions for illegal cellphone SIM card registration activities.

In comparison with the second research, it shows a different topic discussion. It's discussing more legal remedies and compensation for victims whose personal ID has been misused, including for any criminal activity. It can be for online loans, bank loans, and other forms of fraud. While author's research more specifically discusses how the criminal liability that electronic data of Personal Identity Number and Family Identity Number for cellphone SIM card registration illegally. So from the comparative research above, author research is something brand new research that can analyze more clearly and deeply.

The issue of a large number of Personal Identity Number and Family Identity Numbers leaked very easily accessible on the internet is a serious problem because there are many administrative that Personal Identity Number and Family Identity Number requirements if misused by criminals, will have a fatal consequence for the victims who have legitimate Personal Identity Number and Family Identity Number.

METHOD

This research uses normative legal research, while the method uses a *statute approach* and *conceptual approach*. The conceptual approach will answer the first problem in this research, its shows that using someone else's Personal Identity Number and Family Identity Number without the permission of the legitimate owner is included a criminal act. Meanwhile, the statute approach is used to solve the second problem of this research, which is more specific in discussing criminal liability contained in ITE Law as well as Population Administration Law.

The primary legal source used to analyze the second problem regarding criminal liability are Article 362 of the Criminal Code Law concerning the theft act, Law Number 19/2016 concerning Electronic Transaction Information, and also Law No. 24/ 2013 concerning Population Administration. The secondary legal source used to discuss the first problem is the information needed to obtain study data regarding criminal liability

against registered cellphone SIM card sellers, such as legal journals, news, scientific papers, books, websites, etc.

DISCUSSION

Using Personal Identity Number And Family Identity Number Other Person Without Permission From Legitimate Owner Include As Crime Act

This research found that using someone else's Personal Identity Number and Family Identity Number without the owner's permission is a criminal act. In addition, criminal acts have implications for the penalties contained in the Act related to misuse of Personal Identity Number and Family Identity Number for any activity. Furthermore, we will discuss more deeply the meaning of Personal Identity Number/Family Identity Number and also the form of criminal liability if it is misused for electronic transactions.

The principle of legal certainty prioritizes the juridical-formal characteristic because the existing legal norms have been formulated in written regulations, so that the application and enforcement of the law have become clear, permanent, and also consistently maintain its objectivity¹³. Criminal liability is based on the fault of the maker and not only based on all elements of the crime. So that the wrongdoing of the criminals is used as the main factor of criminal liability and not necessarily just a factor of mental awareness of criminals' acts¹⁴.

According to Simons, the basis of criminal liability is the fault of the mind of the criminals concerning an act that can be punished and the mentality of the criminals can be reproached for their actions. Therefore, the guilt of the criminals must be proven, and several things related to the criminals must first be determined, including¹⁵:

- Ability to take the ability for his actions;
- The relationship between the psychological condition between the criminals and the consequences of their actions (including actions that are not against the law during daily activities);
- Dolus and culpa, namely mistakes including subjective elements of criminal acts. Consequence part of the argument to link strafbaarfeit with the error act.

Criminal acts are categorized into two important elements, namely Dolus and Culpa. The most important part of the Dolus crime is that it is a criminal act based on intentional factors and has a criminal motive, meaning that the criminal act is done intentionally, the criminal act is carried out by the criminals consciously with legal consequences related to the consequences of criminal sanctions. Different factors with Culpa, namely the criminal act is not deliberate by the criminals and does not understand the consequences of legal sanctions. The criminal act can be caused by the

¹³ Mario Julyano & Aditya Yuli Sulistyawan. (2019). "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum". *Jurnal Crepido*, Vol. 1(1), pp. 13-22

¹⁴ Chairul Huda. (2006). *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*. Jakarta: Kencana Prenada Media, p. 4

¹⁵ Oemar Seno Adji. (1991). *Etika Profesional dan Hukum Pertanggungjawaban Pidana Dokter*. Jakarta: Erlangga. p.34

negligence of the criminals, so the consequences that occur are not desired by the criminals. His criminal actions from Culpa are not included in criminal acts, but Culpa is categorized as just a person's mistake. So the criminal implications of Culpa are usually reasonable mistakes by the people. In contrast to Dolus, whose actions cannot be accepted by people, because the elements and character of his actions are classified as Criminal act¹⁶.

Data security and confidentiality are important aspects concerning information systems. This is because the data will be sent and received by the person concerned. Information becomes useless if in the process it will be tapped and hijacked by unauthorized parties. Therefore, the security of information systems in electronic transactions is an important issue. Without this data protection, the benefits will not be felt by society¹⁷.

The relationship between identity and the protection of personal data related to a registered telephone card is very close. It is contained in regulations related to the integral protection of personal data as stated in Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE) and article 28G of the 1945 Constitution. However, identity is a human right owned by citizens¹⁸.

As described in Law Number 24 of 2013 concerning Population Administration article 1 paragraph (12) the mean of Personal Identity Number is the resident identity number, which can be referred to as original Indonesian citizens or foreigners registered as Indonesian citizens who are registered as Indonesian citizens. It has a unique and different character and is owned by citizens of one person with another. Whereas paragraph (13) explains that the Family Identity Number is a number that contains data regarding the name, structure, and relationship in the family. In one Family Identity Card, there can be several Personal Identity Numbers that are related to each other or are not blood-related but are in the same domicile in a certain area.

Every Indonesian citizen must have a Personal Identity Number and Family Identity Number as fixed in the Population Administration Law article 101 letter (a) in which the government is obliged to regulate the identity of the Personal Identity Number of its citizens. From here, even newborns have been registered and subsequently, have a Personal Identity Number/Family Identity Number as evidence as an Indonesian citizen, and the government guarantees that every citizen has a Personal Identity Number.

Personal Identity Number and Family Identity Number are important to protect their privacy because they are contained in Law Number 24 of 2013 concerning Population Administration article 64 as explained in paragraph (1) that in one Personal Identity

¹⁶ Ramlan Surbakti. (2011). *Penanganan Pelanggaran Pemilu* (Buku 15). Jakarta: Kemitraan Bagi Pembaruan Tata Pemerintahan. p. 34

¹⁷ Radian Adi Nugraha. (2012). *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik*. Jakarta: Universitas Indonesia, p.26

¹⁸ Cynthia Hadita. (2018). "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia". *Jurnal HAM*, Vol. 9(2), pp. 191–204

Number identity there is data on population data elements regarding name, place, and date of birth, gender. Besides that, it also contains data about the address, marital status, religion, occupation, passport photo, blood type, citizenship, and owner's signature. Whereas in paragraph (2) it is explained that the Personal Identity Number is the identification number of citizens to carry out public service affairs. So that public service facilitators serve customers by tracking a person's Identity Number. And it is explained in paragraph (3) that the Government as an agency that regulates public services is based on the Personal Identity Number of its citizens.

Personal Identity Number is integrated with several public services so that Personal Identity Number/Family Identity Number data must be protected by privacy and guaranteed confidentiality. If it is accessed by other people, it can be fatal for the legitimate owner of the Personal Identity Number, even though it is not the owner of the Personal Identity Number who carries out any transaction activities involving the legitimate owner of that Personal Identity Number. This rule is also contained in Article 79 paragraph (1) of the Population Administration Law which states that information regarding citizens is an important archive whose privacy must be protected by the Government/State.

Taking something belonging to someone else is included in the category of theft as stated in Article 362 of the Criminal Code Law concerning theft. Judging from the elements of the theft criminal article, it is proven that taking part or all of the property of another person is an act of theft. This is reinforced to take other people's belongings to be used for personal gain. In the case of registration of a cellphone SIM Card, if you use someone else's Personal Identity Number and Family Identity Number, the act can also be categorized as a criminal act of theft because it takes and uses another person's identity to activate a cellphone SIM Card, either partially or completely. From the data found in the field, many sellers, outlet owners, or sales from the provider, intentionally activate the cellphone SIM Card first so that the cellphone SIM Card is easy to sell because buyers don't want to bother registering the cellphone SIM Card that they bought. Because it is also possible that the buyer does not remember his Identity Number/Family Identity Number or the buyer's Identity Number/Family Identity Number has been used a maximum of 3 (three) times for registration of a cellphone SIM card, so it uses someone else's Personal Identity Number/Family Identity Number for registration of the purchased cellphone SIM Card.

Many cases are found at the outlet, the legitimate owner of the Personal Identity Number/Family Identity Number is also confused when they want to register the cellphone SIM Card that was purchased using their Identity Number and Family Identity Number because when registering the cellphone SIM Card suddenly a notification appears that the Personal Identity Number/Family Identity Number owned has been used 3 (three) times used, even though it is not the buyer himself who uses his Identity Number/Family Identity Number. That can happen because his Personal Identity Number/Family Identity Number is exposed on the public internet so that it is accessed by others and used to register other cellphone SIM cards. The author who works as a salesperson from provider 3 (Three) found other people's Identity Numbers and Family Identity Numbers which can be easily accessed on the internet. By using the

keyword “election voter”, there is a website link that shows Personal Identity Number/Family Identity Number data belonging to other people in the thousands or even hundreds of thousands of Personal Identity Number/Family Identity Number.

Furthermore, manipulating another Personal Identity Number/Family Identity Number is also categorized as a criminal act as stipulated in Article 32 of the Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. If we look at the elements in paragraph (1), it can be explained that changing and transferring other people's electronic documents is a prohibited act. It is further clarified that the elements of prohibited acts are accessing and storing electronic documents such as the Personal Identity Number/Family Identity Number belonging to another person, which is further explained in paragraph (2) transferring and using the Personal Identity Number/Family Identity Number belonging to another person who is not entitled to also be included in the category of a criminal act. And in the explanation of paragraph (3) that anyone who gives access to a secret Personal Identity Number/ Family Identity Number is also categorized as a crime. So the elements in the article are manipulating electronic documents into authentic data and then transferring them without the permission of the legitimate owner so that they can be accessed by other people and disturbing the legitimate owner to access his data. So it is clear from here that a security and protection system for Personal Identity Number and Family Identity Number data is needed so that they are not misused by others.

Now we discuss that categorizes using Personal Identity Number/Family Identity Number as a crime in Article 35 of the Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. The explanation of article 35 above, according to the author, is closest to categorizing using someone else's Personal Identity Number/Family Identity Number for registration of a SIM Card as a crime. Because manipulating Personal Identity Numbers and Family Identity Number identities of someone who does not belong to him becomes as if the original/authentic data belongs to him. So that is used to register a cellphone SIM card. If we look at a person's Family Identity Card or on the voter list, there are not only Personal Identity Number and Family Identity Number but also there are details in the form of the name, place of birth date, and other detailed information. Manipulating the data using Personal Identity Number and Family Identity Number so that it seems as authentic/original data to be used for SIM card registration, in this case, is a criminal act. This is prohibited because data manipulation is carried out without the permission/intention of the legitimate data owner.

When we are concerned about article 77 of the Population Administration Law, which says that manipulating population data is a prohibited activity, whether it is carried out by citizens in general or carried out by unscrupulous population administration employees. There could be a person from the population administration staff who leaked population data. That also violated the ethics code of their work by disseminating or trading population data that was not their authority. Of course, the purpose is to increase their gain. It doesn't have to be all the details of population data that can be traded. However, in the case of illegal SIM card registration, it only

requires a person's Identity Number and Family Identity Number as a manipulated residence document. The explanation above is also contained in Article 86 paragraph (1) and paragraph (1a) of the Population Administration Law where there is a prohibition for population administration officers to disseminate data on citizens who violate their professional authority. The explanation of the two articles above states that anyone is not allowed to facilitate or manipulate population data, both the wider community as stated in article 77 as well as the internal population administration officers as written in article 86. So from the explanation of several articles above it is clear that using a Personal Identity Number/ Family Identity Number belonging to another person and without permission of the legitimate owner is a form of criminal act category.

Criminal Liability Of Misuse Personal Identity Number/ Family Identity Number For Cellphone SIM Card Registration Illegally

Discussion in criminal law, computer networks such as the internet can make the problem of criminality more complex because of its wide scope. Criminality in cybercrime is a criminal act that occurs in cyberspace, and that reduces the function of community facilities and also a person's property¹⁹.

In comparison, the fundamental difference in criminal liability between ITE law and Population Administration law is in the use of personal identity numbers and family identity numbers. If the Personal Identity Number has not been used for electronic transactions, it will be prohibited to the article of the Population Administration law. However, if the Personal Identity Number is intended for electronic transactions, it will be prohibited by ITE laws.

So the articles above in proving that misuse of Personal Identity Number and Family Identity Number for illegal registration of SIM Card is a form of crime, this discussion will discuss that criminal liability. Some of the implications of the articles above can be categorized as:

Criminal liability for theft

In article 362 of the Criminal Code Law²⁰, it is explained that for anyone who commits theft then the punishment given by the criminals is five years in prison or a maximum fine of nine hundred rupiahs, of course after being converted with the current currency value.

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

The form of accountability misuse of someone else's Personal Identity Number/Family Identity Number for registration of cellphone SIM card according to Article 48 of the ITE Law which has implications from article 32 of ITE Law with the principle of criminal elements starting from manipulating electronic documents as in paragraph (1) then

¹⁹ Nudirman Munir. (2020). *Pengantar Hukum Siber Indonesia*. Depok: PT. Raja Grafindo Persada, p. 64.

²⁰ Indonesia. *Kitab Undang-Undang Hukum Pidana*.

transferring those listed in paragraph (2) to be easily accessible as described in paragraph (3). And the criminal liability is included as:

- In paragraph (1) for anyone who deliberately manipulates and stores electronic documents, the criminal sanction is imprisonment for a maximum of eight years and a maximum fine of two billion rupiahs will be imposed.
- Further explained in paragraph (2) for anyone who intentionally transfers electronic documents to a certain electronic system belonging to another person who is not entitled, for example, uploaded to a certain anonymous website link so that it can be accessed by others, the criminal sanction is a maximum imprisonment of nine years and imposed a fine of three billion rupiahs.

The 2 points above explain a case in 2019 in the introduction who sell personal identity with objects in the form of Microsoft Excel files containing personal identity numbers and family identity numbers stored in a tool in the form of flash drives or memory storage in mobile phones. The element in the first criminal act point is anyone who has changed an electronic document so that it becomes incomplete again then with no right to store the electronic document. Then continued the second point with the element of criminal acts with the interest of electronic transactions of data in the form of personal identity numbers and family identity numbers to register mobile phone cards, and then the electronic documents are transferred and sell it to other people who are not entitled to have it.

- And the end of Article 48 of the ITE Law paragraph (3) is the implication of paragraph (1), whereafter the electronic document is intentionally manipulated then it can be accessed by others, the form of criminal sanction is a maximum imprisonment of ten years and a fine at most five billion rupiahs.

Based on the last paragraph in article 32, explain when an outlet seller registers a cellphone card so that the card was sold faster because the customer did not want to be difficult to register or to activate the card so as not to expire by using the other people identity. We can get easily pages of "Scribd" and "Google Scholar" to get someone's data in the form of a personal identification number and family identity number by typing the keyword "election voter data". A person who uploads the data is following the criminal act element of paragraph three in article 32 where anyone who deliberately uploads personal data is confidential so that it can be accessed by the public for the benefit of electronic transactions.

Then, as a form of the implication of Article 35 of the ITE Law, another form of criminal liability is mentioned in Article 51 of the ITE Law, whereas the criminals will be subject to a maximum imprisonment of twelve years and a maximum fine of twelve billion rupiahs. Article 35 of the ITE Law explains that the criminal element is someone who intentionally uses someone else's Personal Identity Number/Family Identity Number which is not their right to be used as authentic data to register a cellphone card. This criminal liability is also related to a case in 2021, that used another identity that was manipulated to register a cellphone card so there is much evidence that cellphone card registration was activated.

Criminal liability according to Law Number 24 of 2013 concerning Population Administration Law.

Implications of criminal liability from article 77 of the Population Administration Law which applies to the general public for anyone who manipulates and also disseminates the Personal Identity Number/Family Identity Number belonging to others, including registration activities cellphone SIM card is contained in Article 94 of the Law on Population Administration with a maximum imprisonment of six years and a maximum fine of seventy-five million rupiahs.

The criminal element in article 77 and article 94 are everyone is prohibited from manipulating population documents. The meaning of manipulation is that it can add, subtract, or change every detail of document data. It also includes personally identifiable data that allows it to be added, reduced, or altered for a specific purpose. Whether it comes from one's desires or someone's told. Including people who facilitate manipulation of population documents. So this criminal liability is not only for civilians but also for Population Administration employees who order someone or facilitate someone to manipulate population documents.

While the implications of criminal liability from article 86 paragraph (1a) of the Population Administration Law that has been described in Article 95A of the Population Administration Law will be sentenced to imprisonment for a maximum of two years and a maximum fine of twenty-five million rupiahs.

The element of criminal acts in article 95A is that both civilians and population administration officers are prohibited from disseminating personal data in population documents. The meaning of disseminating is that it can be known by the public detail of the document data. It also includes personally identifiable data leaked for specific purposes. This data also be sold for profit purposes. As explained in the article, of course it can also minimize the number of population administration officers who have the potential to spread and sell Personal Identity Numbers/ Family Identity Numbers for personal gain purpose.

CONCLUSION

This study highlighted and concluded that using a Personal Identity Number/ Family Identity Number without permission of the person who has it for electronic transactions is included as a criminal act. But unfortunately, there is no specific law that regulates Personal Identity Number/ Family Identity Number. So if we want to learn, it must require a connection with the other law. Using Personal Identity Number/ Family Identity Number for illegal registration of cellphone SIM Card then refer to article 362 of the Criminal Code Law on theft. If Personal Identity Number/ Family Identity Number is still in the raw form of electronic data then use for trade, refers to article 77 and article 86 paragraph (1a) of Law Number 24 of 2013 concerning Population Administration. While the criminal liability there is in article 94 and article 95A of Law No. 24 of 2013 concerning Population Administration. Furthermore, if Personal Identity Number/ Family Identity is in modified form and used in the electronic transactions such as registering a cellphone SIM card then refer to article 32

and article 35 of the Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information And Electronic Transactions. As for the criminal liability contained in article 48 and article 51 Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to the Law Number 11 of 2008 concerning Information and Electronic Transactions.

ACKNOWLEDGEMENTS

Firstly, the author expresses much gratitude to my parents who always support me to complete this research. The author does not forget to say millions of thanks to Mrs. Nur Azizah Hidayat, SH., MH., and Mr. Supriyono for their dedication and patience to correct as well as for being the best partner sharing in this research. Also thanks to CV. Esia Indoraya, a THREE (3) provider distributor in Surabaya introduced the author to work in telecommunication and information networking. In addition, the author works in that office to become a salesperson as well as getting wages to finance daily needs and also finance the author's college needs to graduate quickly. Furthermore, I also thank the editorial team and publication team of Mulawarman Law Review who are willing to review and publish this research. I hope all my friends and compatriots' kindness is always blessed with beautiful grace in this world as well as in the afterlife. Amiin. Best regard.

REFERENCES

Books

- Adji, Oemar Seno. (1991). *Etika Profesional dan Hukum Pertanggungjawaban Pidana Dokter*. Jakarta: Erlangga.
- Dewi, Shinta. (2015). *Aspek Data Privacy Menurut Hukum Internasional, Regional dan Nasional*. Bandung: PT Refika Aditama.
- Huda, Chairul. (2006). *Dari Tiada Pidana Tanpa Kesalahan Menuju Kepada Tiada Pertanggungjawaban Pidana Tanpa Kesalahan*. Jakarta: Kencana Prenada Media.
- Mardi & Priyantono. (2017). *Digital Mastery, Membangun Kepemimpinan Digital Untuk Memenangkan Era Disrupsi*. Jakarta: PT. Gramedia Pustaka Utama.
- Marett, Paul. (2002). *Information Law in Practice* (2nd Edition). London: MPG Books.
- Munir, Nudirman. (2020). *Pengantar Hukum Siber Indonesia*. Depok: PT. Raja Grafindo Persada.
- Nugraha, Radian Adi. (2012). *Analisis Yuridis Mengenai Perlindungan Data Pribadi Dalam Cloud Computing System Ditinjau Dari Undang-Undang Informasi dan Transaksi Elektronik*. Jakarta: Universitas Indonesia.
- Surbakti, Ramlan. (2010). *Penanganan Pelanggaran Pemilu* (Buku 15). Jakarta: Kemitraan Bagi Pembaruan Tata Pemerintahan.

Journal Articles

- Aditya Hermawan, Erna Susanti, Syukri Hidayatullah. (2018). "Legal Protection of Go-Jek Driver That Experiences Damages Due To The Fictive Order In Go-Food Menu In Go-Jek Application". *Mulawarman Law Review*, Vol. 3(2), pp. 124–132.
- Dewi, Shinta. (2016). "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia". *Jurnal Hukum Yustisia*, Vol. 5(1), pp. 22–30.
- Hadita, Cynthia. (2018). "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia". *Jurnal HAM*, Vol. 9(2), pp. 191–204.
- Julyano, Mario, & Sulistyawan, Aditya Yuli. (2019). "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum". *Jurnal Crepido*, Vol. 1(1), pp. 13-22.
- Pitaloka, Anggraini Dila. (2020). "Pertanggungjawaban Pidana Pelaku Pinjaman Online yang Berimplikasi Tindak Pidana". *Jurnal Jurist Diction*, Vol. 3(5), pp. 1597–1616.
- Sasongko, Et. all. (2020). "Konsep Perlindungan Hukum Data Pribadi dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga". *Proceeding of Conference on Law and Social Studies*, Vol. 1(1), pp. 16–27.

Laws

- Indonesia. *Kitab Undang-Undang Hukum Pidana*.
- Indonesia. *Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*.
- Indonesia. *Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan*.

World Wide Web

- Bisnis.com. (2022). *Harian Bisnis*. <https://kabar24.bisnis.com/read/20220109/15/1486824/data-pribadi-bocor-lagi-ruu-perlindungan-data-pribadi-makin-mendesak> [Accessed June 2, 2022].
- Kompas. (2019). *Harian Kompas*. <https://nasional.kompas.com/read/2019/07/30/14193401/ada-jual-beli-data-kk-dan-nik-di-medsos-kemendagri-lapor-ke-bareskrim-polri/> [Accessed April 4, 2022].
- Pelopor. (2021). *Harian Pelopor*. <https://pelopor.id/2021/10/19/polisi-ciduk-penjual-sim-card-yang-gunakan-data-orang-lain/> [Accessed May 24, 2022].