DE LEGA LATA Jurnal Ilmu Hukum
Volume 8 Nomor 2 July , December. Tahun 2023
E-ISSN: 2477-7889 I ISSN: 2477-653X I Akreditasi: SINTA 3, SK No: 28/E/KPT/2019
http://jurnal.umsu.ac.id/index.php/delegalata

URL: http://jurnal.umsu.ac.id/index.php/delegalata

Actualization Of Criminal Liability For Personal Data Protection In The Use Of Financial Technology: A Comparative Study Of Law Number 11 Of 2008 Concerning Information And Electronic Transactions And Law Number 27 Of 2022 Concerning Protection Of Personal Data

Erwin Asmadi[1], Adi Mansar[2], Triono Eddy[3]
[1,2,3]Universitas Muhammadiyah Sumatera Utara
Kpt. Muchtar Basri No.3, Glugur Darat II, Kec. Medan Timur,
Kota Medan, Sumatera Utara 20238
E-mail: erwinasmadi@umsu.ac.id (Corresponding Author)

Accepted: 14-06-2023 Revised: 20-06-2023 Approved: 22-06-2023 Published: 03-07-2023
DOI: 10.30596/dll.v8i2.15252

How to cite:
Asmadi, E., et.al. (2023). "Actualization Of Criminal Liability For Personal Data Protection In The Use Of Financial Technology: A Comparative Study Of Law Number 11 Of 2008 Concerning Information And Electronic Transactions And Law Number 27 Of 2022 Concerning Protection Of Personal Data", De Lega Lata: Jurnal Ilmu Hukum 8 (2): p. 292-300.

ABSTRACT

Unlike Law Number 27 of 2022 Concerning Personal Data Protection, the ITE Law does not stipulate criminal penalties for people who distribute personal data without the consent of the owner of the personal data. Misuse of personal data is an act that fulfills the elements of a criminal act such as the elements of the crime of theft and elements of the crime of fraud and other crimes both in terms of objective elements and subjective elements. With the fulfillment of these elements, administrative sanctions, civil sanctions and criminal sanctions are not sufficient to accommodate the criminal act of misusing personal data which is actually a perfect form of crime. Article 67 of Law Number 27 of 2022 Concerning Personal Data Protection outlines criminal threats for violating what has been regulated in Article 65. Meanwhile, the ITE Law does not regulate criminal responsibility for people who disseminate personal data, unless it is followed by a violation of decency, gambling, insulting or defaming as well as extortion and threats.

Keywords: Liability, Criminal, Data, Personal.

INTRODUCTION

The Republic of Indonesia is a constitutional state based on Pancasila and the 1945 Constitution of the Republic of Indonesia which is democratic, guarantees all citizens equal status in law and government, upholds human rights5 and makes law the commander in chief in all dynamics of state life. Globalization has become another driver of the era of information technology development. Along with these developments, humans as subjects of this ssat law have left conventional ways and turned to modern ways, namely by utilizing information technology based on "intelligent" automation. Law is a protector of human interests, but because human interests are dynamic, the law must also be dynamic. If not followed by law, developments or information technology can in fact have a bad influence on the activities of human civilization (Chazawi & Ferdian, 2011).

Advances in internet-based technology in this era bring many influences to human life. Technology has a very large role in supporting various activities of human life, one of which is in the financial industry in Indonesia. The increasing competition in the financial sector has led to various strategies being carried out by financial managers, especially banks, to attract the public to become their customers. Banking parties compete to provide the best service that can foster public trust, but in practice many Indonesian people do not have access to banking so that various innovations in non-bank financial services have emerged that can help people's finances by utilizing technology and information systems that are developing very rapidly in Indonesia. Innovations that occur in the financial industry are marked by the presence of financial technology or fintech.

Advances in information technology, especially in the field of social networking have proven to have a positive impact on the progress of human life. Behind the advantages and conveniences offered by this technological advancement, it also has a negative impact that can destroy human life and culture itself. One of them is the leakage of technology user data, including social media users. Social media is a medium for socializing with each other through the internet network that allows humans to interact with each other easily and participate, communicate, share and create various content without being limited by space and time. Generally, social media is designed to make it easier for someone to socialize and communicate with other people (Pertiwi & Dkk, 2021).

However, the positive implications given in terms of ease of access to online transactions certainly have a drawback in the form of an impact that can be given to debtors. In online loans, there are features that are used for access in the form of applications that can be downloaded via a smartphone. When compared to the past, of course it is very different in terms of lending and borrowing regulations. The basic features of the application can be accessed by everyone through several usage mechanisms, namely, downloading the application, registering by including your identity and account number, then waiting for approval from the service to be reviewed and approved, after which the loan funds are disbursed. In several cases that are currently circulating, there are many recognitions that the online loan application feature has a very fatal impact. Several social media outlets stated that there were allegations that online loan business actors leaked the debtor's personal data.

As well as circulating cases of violations against fintech cited by Tirto.id and Kompas.com, with cases of terror against debtors through personal data. It is true that the fact is that after fulfilling the requirements as a debtor and filling in the registration correctly, the loan funds will be disbursed. However, the influence exerted is so fatal and cannot be ruled out, regarding the interest given, the payment is uncertain when it is past due, while the security of personal data cannot be ensured. In addition, if the debtor cannot pay off the payment, the interest given is so large and the method of collection is carried out by the online debt collector by threatening the debtor. The threat given was in the form of terror and also the threat of leaking the debtor's personal identity data.

Based on Article 1 point 1 of Law Number 27 of 2022 Concerning Personal Data Protection that . Personal Data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems. Then based on Article 65 of Law Number 27 of 2022 Concerning Personal Data Protection that:

1. Everyone is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to them with the intention of benefiting themselves or others which can result in loss of Personal Data Subjects.
2. Everyone is prohibited from unlawfully disclosing Personal Data that does not belong to him.

3. Everyone is prohibited from unlawfully using personal data that does not belong to him.

Criminal threats for people who disclose other people's personal data in an unlawful way are stated in Article 67 paragraph (2) that "Any person who intentionally and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be punished with criminal maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000.00 (four billion rupiahs)." Law Number 11 of 2008 concerning Information and Electronic Transactions also regulates the prohibition of using someone's personal data without that person's consent. Article 26 of Law Number 11 of 2008 Concerning Information and Electronic Transactions states that "Unless otherwise stipulated by Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned.".

RESEARCH METHOD

This research is a basic research (basic research). The sample in this study is the Medan District Court. The source of the data in this research is the laws and regulations and procedural law books in Indonesia. The data collection method used in this study was through library research, to obtain theoretical and doctrinal conceptions, opinions or conceptual thinkers and previous research related to the object, as well as conducting interviews with informants as additional or complementary data in this study. Through the study of documentation will be known and identified problems that are often faced by students in choosing a career. Documentation study. A research cannot be said to be research if it does not have research methods because of the purpose of the research adalah untuk mengungkapkan suatu kebenaran secara sistematis, metodologis dan konsisten (Koto, 2021).

DISCUSSION AND ANALYSIS

The Correlation of Criminal Law in Protecting Personal Data Regulated Through the ITE Law and the Personal Data Protection Law

Today's human life is almost inseparable from technology. Technology in the form of various equipment related to the human body such as telephones, glasses, medical equipment, cars, televisions, computers and even all forms of technology that can form genes. The rapid pace of electronic technology has a direct proportional impact with the increasing human need for this technology. Humans as social beings, need devices and tools as a result of technological development, namely in the context of communicating and exchanging information (Asmadi, 2021).

In the era of globalization with technology that is growing very rapidly like now it makes life easier. Advances in technology certainly greatly help human life to be more practical. But if there is a positive impact, of course there will also be a negative impact from technological progress. Because technology is very sophisticated, personal data can be shared easily through social media and other devices born from advances in information technology, of course this can disturb someone whose personal data is not widely spread on social media without their consent, therefore it is necessary to protect personal data.

Based on Article 1 number 2 of Law Number 27 of 2022 Concerning Personal Data Protection that Personal Data Protection is the entire effort to protect Personal Data in the Personal Data processing chain in order to guarantee the constitutional rights of Personal Data subjects. Article 65 of Law Number 27 of 2022 Concerning Personal Data Protection that; 1)

Everyone is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to them with the intention of benefiting themselves or others which can result in loss of Personal Data Subjects, 2) Everyone is prohibited from unlawfully disclosing Personal Data that does not belong to him, 3) Everyone is prohibited from unlawfully using personal data that does not belong to him.

Of course there will be criminal threats for everyone who carries out the prohibitions as described above. Article 67 of Law Number 27 of 2022 Concerning Personal Data Protection describes criminal threats for violations of what has been regulated in Article 65 above; 1) Every person who deliberately and unlawfully obtains or collects personal data that is not owned by him with the intention of benefiting himself or another person which can result in loss of personal data subjects as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah), 2) Everyone who deliberately and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be subject to imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp. 4,000,000,000.00 (four billion rupiah), 3) Everyone who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000.00 .00 (five billion rupiah).

Law Number 11 of 2008 concerning Information and Electronic Transactions also regulates the prohibition of using someone's personal data without that person's consent. Article 26 paragraph (1) of Law Number 11 of 2008 Concerning Information and Electronic Transactions states that "Unless otherwise stipulated by Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned". Then in Article 26 paragraph (2) that "Every person whose rights are violated as referred to in paragraph (1) can file a lawsuit for losses incurred under this Law."

Unlike Law Number 27 of 2022 Concerning Personal Data Protection, the ITE Law does not stipulate criminal penalties for people who distribute personal data without the consent of the owner of the personal data. Misuse of personal data is an act that fulfills the elements of a criminal act such as the elements of the crime of theft and elements of the crime of fraud and other crimes both in terms of objective elements and subjective elements. With the fulfillment of these elements, administrative sanctions, civil sanctions and criminal sanctions are not sufficient to accommodate the criminal act of misusing personal data which is actually a perfect form of crime. (Situmeang, 2021).

Actualization of Criminal Liability for Violators of the ITE Law and the Personal Data Protection Law in Protecting Personal Data

Negative use of technology creates a new type of crime called cybercrime. Cybercrime has many types, one of which is doxing. In short, doxing is a crime committed on the internet by collecting the victim's personal data and then spreading it on the Internet and social media with the aim of intimidating and threatening the victim. media that causes the perpetrator to dislike the victim (Armando & Soeskandi, 2023).

As explained in the previous discussion, Article 67 of Law Number 27 of 2022 concerning Protection of Personal Data outlines criminal threats for violations of what has been regulated in Article 65 above:

1. Everyone who deliberately and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which can

result in loss of the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah).

2. Everyone who deliberately and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be subject to imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp. 4,000,000,000.00 (four billion rupiah).
3. Everyone who intentionally and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000.00 .00 (five billion rupiah).

Whereas the ITE Law does not regulate criminal liability for people who disseminate personal data, unless followed by violations of decency, gambling, insults or defamation as well as extortion and threats. This is regulated in Article 27 of the ITE Law as follows; 1) Everyone intentionally and without rights distributes and/or transmits and/or makes Electronic Information and/or Electronic Documents accessible that have content that violates decency, 2) Everyone intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that have gambling content, 3) Everyone intentionally and without rights distributes and/or transmits and/or makes accessible Electronic Information and/or Electronic Documents that contain insults and/or defamation, 4) Everyone intentionally and without rights distributes and/or transmits and/or makes Electronic Information and/or Electronic Documents accessible that contain extortion and/or threats.
The criminal threat is stated in Article 45 of the ITE Law as follows:

1. Everyone who fulfills the elements referred to in Article 27 paragraph (1), paragraph (2), paragraph (3), or paragraph (4) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp. 000,000,000.00 (one billion rupiah).
2. Everyone who fulfills the elements referred to in Article 28 paragraph (1) or paragraph (2) shall be punished with imprisonment for a maximum of 6 (six) years and/or a fine of up to Rp. 1,000,000,000.00 (one billion rupiah) .
3. Everyone who fulfills the elements referred to in Article 29 shall be subject to imprisonment for a maximum of 12 (twelve) years and/or a maximum fine of Rp. 2,000,000,000.00 (two billion rupiahs).

Cases of leakage of personal data on the internet are increasingly appearing. In fact, various data leak cases have befallen giant global companies. Data leaks also occurred in Indonesia, a number of accounts and personal data of internet users were leaked via social media to e-commerce. Unfortunately, law enforcement in cases of leakage of personal data in Indonesia is very weak compared to other countries. This condition poses a risk that cases of personal data leakage will continue to recur without law enforcement. Data leak refers to a situation where sensitive data is accidentally exposed or accessed by unauthorized parties. Threats can occur via websites, emails, hard drives, or laptops. We need to know that data breaches have a different meaning from data leaks.

Misuse of personal data can also be carried out by crimes that are involved in it, namely personal data breaches. The act of data breach can be categorized as an act that violates Article 30 Paragraph (3) of the ITE Law, which reads: "everyone intentionally and without rights or unlawfully accesses computers and/or electronic systems in any way by violating, breaking through, exceeding, or break through the security system." For his actions, the perpetrator can be charged with imprisonment for a maximum of 8 years and/or a maximum fine of Rp. 800,000,000.- Data leaks that occurred successively hit the government, private companies, and

privately owned accounts. Such as the personal data leak of a public figure that was stolen and then uploaded on social media. Another case involved a group of hackers who claimed to have obtained 1.2 million user data from one of Indonesia's well-known e-commerce companies, as well as many other similar cases that continue to grow.

This problem arises with the current development of information technology which has given rise to new legal issues, namely regarding the security of personal data that takes place through electronic media. The large number of parties using electronic media as a means of communication and transactions results in the theft of personal data. However, so far Indonesia does not have a specific law dealing with misuse of personal data. In Indonesia, the regulations regarding this matter are contained in Article 26 of Law No. 19 of 2016 amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions and Government Regulation No. 71 of 2019 concerning the implementation of electronic systems and transactions. Changes to the ITE Law have been legalized to become Law Number 19 of 2016 concerning Amendments to the ITE Law.

The text of the law is recorded in the 2016 State Gazette of the Republic of Indonesia Number 251 and the Supplement to the State Gazette Number 5952. The law contains seven important points that revise the ITE Law, the government has the authority to cut off access and/or order electronic system operators to cut off access to electronic information that contains violating content. law. It is hoped that this will provide legal certainty to the public, so that they can be smarter and more ethical in using the internet. So that content with elements of SARA, Radicalism, pornography can be minimized (Pertiwi & Dkk, 2021).

The role of law enforcers is important in protecting personal data. In Article 14 of the Personal Data Protection Bill, it is stated regarding the principles and rights of owners of personal data in terms of: (a). National security, (b). The interests of the law enforcement process; (c) the interests of the press as long as personal data is obtained from information that has been published and agreed upon by the owner; (d) scientific and statistical research interests as long as personal data is obtained from information that has been published (reconfirmation for research purposes). In the Personal Data Protection Bill, it has not yet been regulated regarding the formation of an institution that has the function of overseeing and controlling or a personal data protection agency.

Meanwhile in Law no. 24 of 2013 concerning Population Administration has not yet been regulated regarding the processing, management and protection of personal population data, including third parties who carry out the processing, this is considering that e-KTP which is one of these personal data is a mandatory and important requirement to get good public services. from government and private sector. So the researchers are of the opinion that a separate institution should be formed that can handle specifically and become input in the Personal Data Protection Bill. Meanwhile, the National Cyber and Crypto Agency (BSSN) was officially formed since Presidential Decree No. 53 of 2017 concerning the National Cyber and Crypto Agency, dated May 19 2017.

In this regulation, the BSSN was formed by considering that the cyber security sector is one of the areas of government that needs to be encouraged and strengthened as an effort to increase national economic growth and achieve national security. The formation of the BSSN is an effort to organize the National Crypto Agency to become the National Cyber and Crypto Agency to ensure the implementation of government policies and programs in the field of cyber

security. BSSN is a non-ministerial government institution (LPNK) which is under and responsible to the President through the minister who organizes coordination, synchronization and control of governance in the fields of politics, law and security. BSSN has the task of carrying out cyber security effectively and efficiently by utilizing, developing and consolidating all elements related to cyber security.

The existence of the National Crypto Agency, which is one of the agencies used as the BSSN, was finally regulated in Presidential Decree No. 103 of 2001 concerning Position, Duties, Functions, Authorities, Organizational Structure, and Working Procedures of Non-Departmental Government Institutions (LPND). This means that the National Crypto Agency is an LPND, whose job is to carry out governmental tasks in the field of coding in accordance with the provisions of the applicable laws and regulations. BSSN needs to have complete and clear authorities related to cyber and encryption issues, especially in anticipating the increasing frequency of attacks and cyber space crimes. Cyberspace crimes or what is known as cybercrime include identity and data theft (information resources), account hijacking (email, IM, social networks), spreading malware and malicious code, fraud, industrial espionage, taking critical information resources hostage. and cyberwarfare or war in cyberspace (Budiman, 2017).

Based on the description above, law enforcement against misuse of personal data depends not only on law enforcement in carrying out its law enforcement but also on the substance of the law that regulates it and legal awareness in preventing and overcoming data abuse that occurs in society. This is in accordance with the opinion of Lawrence M. Friedman, who said that a legal system has three parts or components, namely: (1) structural component; (2) substance components; (3) legal culture components (Ravena, 2017). the oversight mechanism is the same as the PDIP Bill, namely through the Central Information Commission. KIP has a function to ensure personal data providers comply with and comply with the provisions in the law and encourage all parties to respect the privacy of personal data. For this reason, in order for law enforcement to be effective in misusing personal data, it is important to strengthen / improve the substance aspect, strengthen the structural aspect, improve the cultural aspect.

Given the limitations or weaknesses of the ability of criminal law in overcoming criminal acts, the existence of criminal law is still needed. It's just that the policy of overcoming criminal acts in Indonesia cannot only use penal means 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 deficiencies and limitations of these penal facilities. When viewed from the perspective of criminal politics at a macro level, crime prevention policies using means other than criminal law or non-penal policies are the most strategic crime prevention policies.

CLOSURE

Conclussion

Unlike Law Number 27 of 2022 Concerning Personal Data Protection, the ITE Law does not stipulate criminal penalties for people who distribute personal data without the consent of the owner of the personal data. Misuse of personal data is an act that fulfills the elements of a criminal act such as the elements of the crime of theft and elements of the crime of fraud and other crimes both in terms of objective elements and subjective elements. With the fulfillment

of these elements, administrative sanctions, civil sanctions and criminal sanctions are not sufficient to accommodate the criminal act of misusing personal data which is actually a perfect form of crime. Article 67 of Law Number 27 of 2022 Concerning Personal Data Protection outlines criminal threats for violating what has been regulated in Article 65. Meanwhile, the ITE Law does not regulate criminal responsibility for people who disseminate personal data, unless it is followed by a violation of decency. , gambling, insulting or defaming as well as extortion and threats.

Suggestions

Synchronization must be carried out between the ITE Law and the PDP Law so that in the future it can accommodate crimes or crimes related to personal data. Criminal liability for personal data violations is in accordance with the ITE Law and the PDP Law, namely in the form of threats of imprisonment and fines. It is suggested to law enforcers to continue to carry out what has been mandated by law.

REFERENCES

Armando, M. A. C., & Soeskandi, H. (2023). Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut UU ITE dan UU PDP. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*(1), 559–568.

Asmadi, E. (2021). Rumusan Delik Dan Pemidanaan Bagi Tindak Pidana Pencemaran Nama Baik Di Media Sosial. *De Lega Lata: Jurnal Ilmu Hukum*, *6*(1), 16–32.

Budiman. (2017). *Optimalisasi Peran Badan Siber dan Sandi Nasional*. Majalah Info Singkat Pemerintahan Dalam Negeri.

Chazawi, A., & Ferdian, A. (2011). *Tindak PIdana Informasi & Transaksi Elektronik*. Media Nusa Creative.

Koto, I. (2021). Perlindungan Hukum Terhadap Korban Tindak Pidana Terorisme. *Prosiding Seminar Nasional Kewirausahaan*, *2*(1), 1052.

Pertiwi, E., & Dkk. (2021). Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial. *JURNAL RECHTEN: RISET HUKUM DAN HAK ASASI MANUSIA*, *3*(3), 10–16.

Ravena. (2017). *Kebijakan Kriminal: (Criminal Policy)*. Prenadamedia Group.

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Jurnal SASI*, *27*(1), 38–52.