RECHTENSTUDENT JOURNAL
Volume 4 Number (1) April 2023, pp. 15-25
DOI: https://doi.org/10.35719/rch.v4i1
Published by the UIN KHAS Jember, Indonesia
ISSN: 2723-0406 | E-ISSN: 2775-5304 Available online 28 April 2023

Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims

Mayada Afriga Arum Dari*
KH Achmad Siddiq Jember State Islamic University, Indonesia
Nadya Melinda Oktarina
University of Jember, Indonesia
Corresponding Author's Email: mayadaafriga08@gmail.com

Article

How to cite:
Mayada Afriga Arum Dari & Nadya Melinda Oktarina, **'Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims'** (2023) Vol. 4 No. 1 Rechtenstudent Journal Sharia Faculty of KH Achmad Siddiq Jember State Islamic University.

DOI:
10.35719/rch.v4i1.226

Article History:
Submitted: 13/12/2022
Reviewed: 10/02/2023
Revised: 07/03/2023
Accepted: 25/04/2023

ISSN:
2723-0406 (printed)
E-ISSN:
2775-5304 (online)

Abstract

Law Number 11 of 2008 has an important role in the realization of building a cyber regime. Cases of data misuse on social media are rife along with the development of technology. According to the detikinet page, at least 14 million social media accounts were affected by personal data leaks. In Islam, abuse of identity without the consent of the party is one of the actions that prohibited by Allah SWT, this is because it's an act that damages and causes harm to other people. The purpose of this study is to find out the form of handling cybercrime in Indonesia, to find out the perpetrators accountability of data misuse according to the ITE Law, and to find out the responsibility for misusing information data on social media according to Islamic Criminal Law. The research method used is a qualitative approach with library research, the data sources used are primary and secondary data sources. Technical data collection by collecting data from primary and secondary sources, namely with a conceptual approach. Research results 1) The form of handling Cybercrime can be carried out with the obligation of operators to provide education to users 2) ITE crimes are regulated in 9 Articles, from Article 27 to Article 35. In these 9 articles, 20 forms are formulated/ type of ITE crime. 3) Accountability for data misuse on social media included in the ta'zir category for violations. The appropriate sanction according Islamic law is imprisonment, also additional punishment in the form of a fine.
Keywords: *Islamic Criminal Law*, *Missues Information, Social Media.*

Abstrak

Undang-Undang Nomor 11 Tahun 2008 memiliki peranan penting dalam terwujudnya membangun rezim siber atau telematika. Kasus penyalahgunaan data di media sosial marak terjadi seiring dengan perkembangan teknologi informasi dan komunikasi. Menurut laman detikinet menyebutkan bahwa setidaknya 14 juta akun sosial media sosial terdampak atas kebocoran data pribadi. Dalam Islam sendiri penyalahgunaan identitas milik orang lain tanpa persetujuan pihak yang bersangkutan merupakan salah satu tindakan yang dilarang Allah swt., hal tersebut dikarenakan merupakan perbuatan yang merusak dan menimbulkan kemudharatan orang lain. Tujuan penelitian ini ialah untuk mengetahui bentuk penanganan tindak pidana *Cybercrime* di Indonesia, Mengetahui pertanggungjawaban pelaku tindak pidana penyalahgunaan data menurut UU ITE, serta mengetahui pertanggungjawaban atas penyalahgunaan data informasi di media sosial menurut Hukum Pidana Islam. Metode penelitian yang digunakan adalah pendekatan kualitatif, jenis penelitian yang digunakan menggunakan jenis penelitian riset kepustakaan (*library research*), sumber data yang digunakan merupakan sumber data primer dan sekunder. Teknis pengumpulan data dengan mengumpulkan data dari sumber-sumber primer dan sekunder yaitu dengan pendekatan konseptual. Hasil penelitian 1) Bentuk penanganan tindak pidana *Cybercrime* di Indonesia dapat

dilakukan dengan kewajiban penyelenggara sistem informasi untuk memberikan edukasi kepada pengguna sistem elektronik 2) Tindak pidana ITE diatur dalam 9 Pasal, dari Pasal 27 sampai dengan Pasal 35. Dalam 9 pasal tersebut dirumuskan 20 bentuk/jenis tindak pidana ITE. 3) Pertanggungjawaban atas penyalahgunaan data informasi di media sosial yaitu masuk dalam kategori jarimah ta'zir atas pelanggaran-pelanggaran. Sanksi yang tepat menurut hukum Islam adalah hukuman penjara, hukuman tambahan berupa denda.
Kata Kunci: *Hukum Pidana Islam, Penyalahangunaan Data, Media Sosial.*

Introduction

The ease of accessing the internet in addition to making it easier for humans also causes the emergence of evil acts aimed at the information technology system. Technological advances can make it easier for irresponsible individuals to misuse one's personal data to do things against legal actions. The act of misusing one's personal data causes a lot of harm to victims, from physical to non-physical losses.

As an example of the case is Ferry Piscesa, who was defendant after joining the hacker community on Facebook, from there Ferry bought 100 credit cards at a price of Rp. 3,000,000, - apart from that, the defendant committed the crime of *carding*. The data that has been obtained then accessed to buy several items such as watches, and others using laptops and smartphones. From this case, the perpetrator was charged under Article 48 Paragraph (1) Jo. Article 32 Paragraph (1) RI Law No. 11 of 2008 of Information and Electronic Transactions. (Malang District Court Decision Number: 597/Pid.Sus/2018/PN Mlg).

The guarantee regarding the protection of personal data itself has been explained in Article 28G paragraph (1) of the 1945 Indonesia Constitution which reads: "*Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asas".*[1]

Regulations explaining the protection of personal information data are also contained in the ITE Law Number 11 of 2008 which states: "*Setiap Penyelenggara Sistem Elektronik wajib menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan Orang yang bersangkutan berdasarkan penetapan pengadilan.*"[2] The purpose of the ITE Law cannot be separated from the creation of a society that always applies ethics in technology. The existence of Law Number 11 of 2008 about ITE is expected to be able to solve crimes in the field of information and technology.[3]

Article 30 paragraph (2) of Law Number 11 of 2008 about ITE (UU ITE) describes actions that are prohibited in the use of electronic media which reads: "*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.*" This article is the legal basis for the protection of information regarding personal data or personal data of a person through electronic media such as computers, and several of the articles above have been amended by Law Number 19 of 2016. This article has the intention to prohibiting anyone intentionally and without rights or against the law accessing other people's electronic systems without consent with the aim of obtaining other people's

[1] Article 28G paragraph (1) of the 1945 Indonesia.
[2] Article 26 of Statutory Regulation No. 11 of 2008 of Information and Electronic Transactions.
[3] Ria Safitri, "Undang-Undang Informasi dan Transaksi Elektronik Bagi Perguruan Tinggi, Jurnal Sosial & Budaya" Syar-I, Vol. 5 No. 3, (2018), 200.

information in a way that violates, exceeds, breaks, or breaks through technology security systems.[4]

Misuse of someone identity is one of the actions that is prohibited and hated by Allah SWT. These actions that cause harm to other people and damage in any form are actions that are contrary to the values of Islamic law.

In its implementation, UU ITE has actually attempted to respond and bridge various new legal requirements with the needs of society. In the context of the telematics legal regime, UU ITE has an important role in realizing the establishment of a cyber or telematics legal regime. In addition, it's also hoped that UU ITE can provide legal certainty in its utilization of the ITE field. Although, there are still many deficiencies and improvements that needed to become a national law related to cyber law issues in Indonesia.[5]

Because of the background above, the author is interested in studying and analyzing how legal remedies and sanctions are against perpetrators of misuse of one's data in a scientific work in the form of a Journal entitled "Islamic Criminal Law Principles in Regulation of Misuse Information on Social Media Victims."

Research Methods

This type of research uses normative legal research, namely legal research conducted by examining primary legal materials, secondary legal materials using statutory approaches. This type of research uses library research, because in this study it utilizes library resources to obtain research data. Literature research is a form of data collection that requires reviewing relevant books, literature, records and reports.[6] Normative legal research is a study or research on principles, norms, laws, court decisions and doctrines in order to form a system of norms.[7] Normative legal research is oriented towards practical aspects, namely by resolving legal issues both in the form of disputes and matters to be sought regarding how and where a legal issue is regulated by law and is carried out through research on the facts of relevant legal regulations and cases.[8] The research approach used in this study is a conceptual approach that's implemented on provisions related to Law Number 11 of 2008 and Islamic Criminal Law.[9]

Result and Discussion

Endeavor to Handle Cybercrime in Indonesia

Misuse of data has many form, for example filing fake administrative requirements, creating fake accounts from someone, acting as someone, buying and selling data illegally, bullying and sexual harassment, it doesn't rule out the possibility of misusing data on social

[4] Tanzizal Afuw, "Perilaku Hukum Pengguna Instagram Terhadap Peretasan Data Pribadi (Studi Kasus Mahasiswa Fakultas Universitas Negeri Malang)",*Undergraduate Thesis* of Law Faculty, Muhammadiyah Malang University (2020), 11

[5] Go Lianawati, "Aspek Perlindungan Data Privasi Dalam Undang Nomor 11 Tahun 2008", Jurnal Yustika, Vol. 15 No 1, (2012), 59

[6] Dyah Ochtorina & A'an Efendi, *Penelitian Hukum,* (Jakarta : Sinar Grafika, 2014), 48.

[7] Mukti Fajar & Yulianto Achmad, *Dualisme Penelitian Hukum Normatif dan Empiris,* Cetakan IV (Yogyakarta: Pustaka Pelajar, 2017), 33.

[8] Depri Liber Sonata, "Metode Penelitian Hukum Normatif dan Empiris: Karakteristikk Khas Dari Metode Meneliti Hukum", Jurnal Ilmu Hukum, Vol. 8 No. 1, (2014), 26.

[9] Dewi Magfirotul Akbar "Physical Neglect and Violence Towards Children by Parents: An Analysis of Criminal Law", Rechtenstudent Journal, Vol. 3 No. 3, (2022), 270.

media. The following are examples of cases of data misuse on social media that have occurred in Indonesia as follows, especially on social media, namely the theft of personal data by Adam Deni who is a social media activist. Adam was named a suspect by the Karo Penmas Public Relations Division of the Indonesian National Police, Brigadier General Ahmad Ramadhan, for having committed an unlawful act by copying and uploading other people's personal data. Adam Deni was reported by someone with the initials SYS. Because of these actions, Adam was charged with Article 48 paragraphs (1), (2), and (3) in conjunction with Article 32 paragraphs (1), (2), and (3) of Law (UU) Number 11 of 2008 About Information and Electronics (ITE).

Sajipto Raharjo defines legal protection as an activity to protect the human rights of people who have been harmed so they can enjoy all the rights granted by law. In providing and implementing legal protection, the media is needed in its implementation, which is called a means of legal protection.[10]

Article 30 becomes the legal basis for the protection of information relating to a person's personal data in electronic media. This article contains a prohibition against anyone who intentionally and without rights or unlawfully accesses another person's electronic system with the aim of obtaining electronic information in any way that violates, exceeds, penetrates, or breaks through the electronic system security system.

Article 12 of PP PSTE states that in order to prevent misuse of data, electronic system operators are required to implement risk management for losses that will arise. This risk management must be carried out by electronic system operators by analyzing risks and overcoming threats or losses that will occur.

The handling of cyber crime victims by law enforcement in providing legal protection is still a problem among the public. Judging from several cases that have occurred on social media such as spreading hoax news, etc. law enforcement in handling this case are still in a dilemma in providing protection for victims, because on the one hand the Criminal Code (KUHP) and UU ITE used as a benchmark and basis in carrying out investigations and contains a criminal system that is a "determinate sentence", so that it's not possible for officials to pass decisions on other types of crimes as determined by the Criminal Code and UU ITE.[11]

Laws and regulations become the legal basis regarding the protection of the data of a person who has been registered with an electronic system operator. The data protection rights are regulated in Article 26 paragraph (1) of ITE Law. In this article, it is explained that the submission of personal data must go through the consent of the person concerned. Every social media platform must provide an option to agree or not to submit the relevant user data. Regarding the protection of personal data from unauthorized use, Article 26 of the ITE Law states that the use of any personal data in an electronic media must obtain the consent of the owner of the data concerned. Everyone who violates this provision can be sued for the losses incurred.

Endeavor to prevent this can also be done with the information system administrator's obligation to provide education to users of electronic systems. One of the educations that needs to be done is not to share their very important personal data and to be careful in sorting

[10] Zennia Almaida, Moch. Najib Imanullah, "Perlindungan hukum preventif dan bagi pengguna uang elektronik dalam melakukan transaksi tol non tunai", Privat Law Vol. 9 No 1, (2021), 222.

[11] Hartono, "Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban dari Perilaku Cyber Crime Ditinjau Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik", Law Faculty of Sigapbangsa University,.1 No.1, (2016), 34

out the data they will share. Education can also be about various modes of crime in the cyber world when they share their personal data. This obligation is stated in Government Law (PP) No. 71 in year 2019 about Implementation of Electronic Systems and Transactions (PP PSTE) Article 28. The education referred to includes the rights, obligations and responsibilities of all related parties and the procedure for filing complaints. The obligations of the system operator mentioned in Article 30 Paragraph (1) PP PSTE are the obligation to provide features according to the characteristics of the electronic system in order to protect the rights or interests of electronic system users. It is further said that these features at least apply the facilities in Paragraph (2), one of which is to make corrections. Not only prevention, but there are also rules regarding prevention. In Article 14 it is stated that electronic system operators have an obligation to implement the principles of personal data protection, namely that processing personal data must be done by protecting data security from misuse of personal data.

The Regulation of the Minister of Communication and Information of the Republic of Indonesia in Article 5 paragraph (2) also discusses the protection of personal data in electronic systems which reads "*Setiap penyelenggara sistem elektronik harus menyusun aturan internal perlindungan data pribadi sebagai bentuk tindakan pencegahan untuk menghindari terjadi kegagalan dalam perlindungan data pribadi yang dikelola.*" From this explanation it can be understood that each party administering the electronic system, especially social media such as Twitter, Facebook, Instagram, etc. Develop rules in the form of terms and conditions, such as partner code of ethics and terms of service. With these terms and conditions, social media parties are required to maintain the confidentiality of users' personal data in accordance with Article 28 letter b of the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 about Protection of Personal Data in Electronic Systems which reads "Maintain truth, confidentiality, accuracy, and relevance and suitability for the purpose of obtaining, collecting, processing, analyzing, storing, displaying, posting, transmitting, distributing and destroying personal data.[12]

The law used in Indonesia as protection against misuse of personal data, are: [13]

1. Statutory Regulation No. 36 Year of 2009 about Health which regulates the confidentiality of the patient's personal condition;
2. Statutory Regulation No. 10 Year of 1998 about Bank which regulates the customer's personal data storage and savings;
3. Statutory Regulation No. 19 Year of 2016 regarding Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions;
4. Statutory Regulation No. 24 Year of 2013 concerning Amendments to Law Number 23 of 2006 concerning Citizen Administration;
5. Government Regulations No. 37 of 2007 Implementation of Law Number 23 of 2006 Concerning Citizen Administration

Legal protection regarding the misuse of data on social media is inseparable from the obstacles that will occur, such as difficulties in tracking down the main perpetrators and proving them, as well as difficulties in handling them. Therefore, the role of the government

[12] Adetya Firnanda, Revita Pirena Putri, dkk. "Kebocoran Data Pribadi Melalui Fitur Sticker Didalam Platform Instagram" National Seminar of Technology and Disciplines, Vol.1 No.1, (2021), 156.

[13] Muhammad Hasan Rumlus, Hanif Hartadi, "Kebijakan Penanggulangan Dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media)", Jurnal HAM, Vol.11 No. 2, (2020), 291-292.

and law is very important in dealing with and protecting crimes of personal data misuse that occur in the field of technology. The role of law enforcement is very influential in overcoming cybercrime with the existence of laws and regulations. The ITE Law is one of the laws and regulations relating to crimes in the field of information technology, especially those relating to the Internet.

Cybercrime law enforcement, as was carried out by the National Police Headquarters in 2007 above, was carried out by interpreting cybercrime into the Criminal Code legislation and specifically laws related to the development of information technology such as:[14]

1. Statutory Regulation No. 36 Year of 1999 about Telecommunication.
2. Statutory Regulation No.19 Year of 2002 about Copyright.
3. Statutory Regulation No 25 Year of 2003 regarding Amendments to Law No. 15 of 2002 about the Crime of Money Laundering.
4. Statutory Regulation No 15 Year of 2003 on the Eradication of Criminal Acts of Terrorism.

Criminal Liability of Perpetrators of Personal Data Misuse Crime on Social Media according to the ITE Law

Van Hamel defines criminal liability as something psychic normalcy and proficiency which carry three kinds abilities, namely being able to understand the meaning and consequences earnestly from one's own actions, able to realize that these actions are contrary to public order and able to determine the will to do.[15]

In the Criminal Code there is no provision regarding the meaning of the ability to be responsible. The KUHP doesn't regulate regarding ability to be responsible, but stipulates just the opposite, namely inability to be responsible as specified in article 44 of the KUHP. The article related to this is Article 44 which reads: "Whoever commits an act for which he cannot be held accountable, because his soul is disabled in his body or his soul is disturbed due to illness. If he cannot be accounted for, it is because of other things, for example his soul is not normal because he is still very young or something else, this article cannot be used.

With the existence of rules relating to the ability to take responsibility as formulated in Article 44 of the Criminal Code, which only regarding the inability to take responsibility because the soul is disabled in the body or disturbed due to illness, then the consequences if you cannot be responsible because the soul is still young or not old enough, then the article does not apply, so it must use a broader basis, namely using the unwritten principle. Usually in practice this is referred to as no intention, because what is done is not desired.

In Article 26 of the ITE Law it is stated that users of personal data through electronic media must be based on the consent of the person concerned, while losses arising from misuse of data can take legal or non-legal channels. Article 26 is one of the articles that protects personal data and personal rights, while the text of the article is as follows:

1. Unless otherwise stipulated by laws and regulations, the use of any information through electronic media about a person's personal data must be carried out with the consent of the person concerned.

[14] Ahmad S. Daud, "Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi" Lex Crimen, Vol II No. 1, (2013), 100.

[15] Moeljatno, *Asas-Asas Hukum Pidana*, (Jakarta: Rineka Cipta, 2008), 180-182.

2. Everyone who the rights get violated as referred to in paragraph (1) can file a lawsuit for losses incurred under this Law.

There are 20 (twenty) types of crimes regulated by the ITE Law, regarding sanctions for criminal acts of Data misuse on social media including those that deliberately violate the law without the right to access another person's computer or electronic system. They can be held liable if they fulfill the four conditions as stated in article 1365 of the Civil Code, including:

1. There is an act;
2. There is an element of unlawful;
3. There is a loss;
4. There is a causal relationship between errors and losses

The use of data that occurs between social media as the organizer of the electronic system and users is contained in the Statement of Rights and Responsibilities. In this case, it means that the user has agreed to the policies set by each social media that he wants to use. However, things may happen that are not in accordance with the agreement between the user and social media services.

Based on Article 27 of the 2008 ITE Law which reads: "*Every person intentionally and without rights distributes and/or transmits and/or makes accessible electronic information and/or electronic documents that have content that violates decency. Criminal threats Article 45 paragraph (1) of the Criminal Code. Maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 1,000,000,000.00 (one billion rupiah*)". Article 28 of the 2008 ITE Law: *Everyone intentionally and without right spreads false and misleading news that results in consumer losses in electronic transactions.* Article 29 of the ITE Law of 2008: "*Every person intentionally and without right sends electronic information and/or electronic documents that contain threats, violence or intimidation that are directed personally (Cyber Stalking).* Criminal threats Article 45 paragraph (3), *everyone who fulfills the elements referred to in Article 29 shall be punished with imprisonment for a maximum of 12 (twelve) years and/or a fine of up to Rp. 2,000,000,000.00 (two billion rupiahs)".* Article 30 paragraph (3) of the ITE Law of 2008: "*Every person intentionally and without rights or unlawfully accesses computers and/or electronic systems in any way by violating, breaking through, exceeding, or breaking through the security system (cracking, hacking, illegal access).* Criminal threats Article 46 paragraph (3), *everyone who fulfills the elements referred to in Article 30 paragraph (3) shall be punished with imprisonment for a maximum of 8 (eight) years and/or a fine of up to Rp. 800,000,000.00 (eight hundred million rupiah)".*[16]

ITE crimes are regulated in 9 articles, from Article 27 to Article 35. In these 9 articles, 20 forms/types of ITE crimes are formulated. Article 36 does not formulate the basis for criminal aggravation which is placed on the consequences of harming other people in the criminal acts regulated in Articles 27 to Article 34. Article 37 also regulates the basis for aggravation of punishment (with reasons other than Article 36) in criminal acts Article 27 up to Article 36. While the punishment is determined in Article 45 to Article 52.[17]

[16] Abdul Rahim Wahab, dkk. "Analisi Yuridis Tentang Pertanggungjawaban Pidana Terhadap Pelaku Cyber Crime" Islamic University of Kalimantan, (2022)

[17] Adami Chawazi dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, (Malang: Sang Free, 2011), 3.

Responsibility for Dissemination of Information Data According to Islamic Criminal Law

Surah Al-An'am verse 164 explains the principle of accountability, which means: "*Say, will I seek a god other than Allah, even though He is the Lord of all things. And it is not someone who makes a sin but his harm returns to himself, and someone who sins will not bear the sins of others. Then to your Lord you will return, and I will give you what you disputed."*

Factors that result in criminal liability are immoral acts, acts against the law. Even though an unlawful act is a cause for criminal liability, there are still two conditions, namely knowing and choosing. If one of the conditions is not met, then there is no criminal responsibility.

The crime of misusing information data on social media in qualifying information technology crimes is included in the ta'zir finger category. This reason is because when viewed at the time of the Prophet, he was not familiar with computers or even the internet like today. In addition, cyber crimes are not regulated in the texts of the Koran or hadith so that data misuse or cyber crime can be categorized in ta'zir crime.

The implementation of takzir punishment is the right of the state ruler or the task appointed by him because every punishment carried out aims to protect the community. As seen in Surah An-Nisa ayah 59 that state *"O you who have believed, obey Allāh and obey the Messenger and those in authority among you. And if you disagree over anything, refer it to Allāh and the Messenger, if you should believe in Allāh and the Last Day. That is the best [way] and best in result."* Therefore it becomes his right and is carried out by the guardian of the community. The difference between takzir jarimah and other jarimah is that hadd punishment cannot be aborted or forgiven, while takzir jarimah can be forgiven by the state authorities at any time.

Criminal responsibility in Islamic criminal law is imposed on a person as a result of an act committed of his own free will, where he understands the intent and purpose of the act. Misuse of information data on social media can be categorized as a criminal act of theft. This is because someone deliberately took and or accessed other people's social media in secret to retrieve the important data listed therein.

In the implementation of ta'zir, namely the actions that have been carried out by the prophet described in the hadith narrated by At-Tirmidhi that Rasulullah SAW. once detained someone who was under accusation and then released him. The condition for ta'zir punishment to be imposed on the perpetrators of crimes is that the person is intelligent. Therefore it is clear that the perpetrators of misusing information data through social media are intelligent people.

Perpetrators of misuse of information data can be punished because they have fulfilled the elements of jarimah, that is, the perpetrator is a person who is reasonable and good-natured, the perpetrator knows that the action he is taking is a prohibited action, the perpetrator knowingly commits the action. Punishments for misuse of information data fall into the category of ta'zir for violations. This is because the act of misusing information data is troubling the owners or users of social media because they have stolen other people's information data and used it for things that are not good and disrupt the public good.

The ta'zir crime sanction for criminal acts of misuse of proper data according to Islamic law is imprisonment, while additional punishments can be in the form of fines, or can be punishments in the form of dismissal, reprimands. The punishment given aims solely to give a deterrent effect to the perpetrators who have committed crimes. These punishments are given

by the authorities or judges taking into account the severity of the actions committed by the perpetrators of these crimes.

To ensnare perpetrators of crimes of misuse of personal data on social media based on Law Number 19 of 2016 concerning ITE, they must fulfill the theory of proof contained in the Criminal Law. Evidence itself can be in the form of evidence that aims to strengthen and provide clues that the perpetrator has actually committed a crime of abuse on social media. Regarding the evidence in cases of data misuse, it has been explained in Article 184 paragraph (1) of the Criminal Code (KUHP), which reads: "Witness statements, letter statements, instructions, and statements of the accused. And if the ITE Law itself can be in the form of additional evidence related to electronics.

Conclusion

Regarding the protection of personal data from unauthorized use, Article 26 of the ITE Law states that the use of any personal data in an electronic media must obtain the consent of the owner of the data concerned. Everyone who violates this provision can be sued for the losses incurred. Efforts to prevent this can also be done with the information system administrator's obligation to provide education to users of electronic systems. One of the educations that needs to be done is not to share their very important personal data and to be careful in sorting out the data they will share. Education can also be about various modes of crime in the cyber world when they share their personal data in an insecure manner. This obligation is stated in PP PSTE Article 28. The education referred to includes the rights, obligations and responsibilities of all related parties and the procedure for filing complaints. The obligations of the system operator mentioned in Article 30 Paragraph (1) PP PSTE are the obligation to provide features according to the characteristics of the electronic system in order to protect the rights or interests of electronic system users.

Appropriate sanctions or punishments for perpetrators of criminal acts of abuse on social media according to Article 48 in conjunction with Article 32 paragraph (1) of Law Number 19 of 2016 are imprisonment for a maximum of 8 (eight) years and a fine of Rp. 2,000,000,000.00 (two billion rupiah).

Punishments for misuse of information data fall into the category of ta'zir for violations. This is because the act of misusing information data is troubling the owners or users of social media because they have stolen other people's information data and used it for things that are not good and disrupt the public good. The ta'zir finger sanction for criminal acts of misuse of proper data according to Islamic law is imprisonment, while additional punishments can be in the form of fines, or can be punishments in the form of dismissal, reprimands. The punishment given aims solely to give a deterrent effect to the perpetrators who have committed crimes. These punishments are given by the authorities or judges taking into account the severity of the actions committed by the perpetrators of these crimes.

Bibliography

Book

Chawazi, Adami & Ardi Ferdian. *Tindak Pidana Informasi dan Transaksi Elektronik Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik.* Malang: Sang Free.

Fajar, Mukti & Yulianto Achmad. 2017. *Dualisme Penelitian Hukum Normatif dan Empiris, Cetakan IV.* Yogyakarta: Pustaka Pelajar.

Mardani. 2019. *Hukum Pidana Islam*. Jakarta: Pernada Media Books.
Muchlis, Ahmad Wardi. 2005. *Hukum Pidana Islam*. Jakarta: Sinar Grafika.
Moeljatno. 2008. *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta.
Ochtorina, Dyan & A'an Efendi. 2014. *Penelitian Hukum.* Jakarta: Sinar Grafika.

Journal

Akbar, Dewi Magfirotul. "Physical Neglect and Violence Towards Children by Parents: An Analysis of Criminal Law", *Rechtenstudent Journal,* Vol. 3 No. 3 (2022).
Almaida, Zennia dan Moch. Najib Imanullah. "Perlindungan hukum preventif dan bagi pengguna uang elektronik dalam melakukan transaksi tol non tunai" *Privat Law.* Vol. 9 No. 1 (2021).
Anjani, Sari dan Irwansyah. "Peranan Influencer Dalam Mengkomunikasikan Pesan Di Media Sosial Instagram (The Role Of Social Media Influencer In Communicating Messages Using Instagram)." *Jurnal Ilmiah,* Vol. *16* No. *2,* (2020).
Daud, Ahmad S. "Kebijakan Penegakan Hukum Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi" *Jurnal Lex Crimen*, Vol. II No. 1, (2013).
Firnanda, Adetya dan Revita Pirena Putri, dkk. "Kebocoran Data Pribadi Melalui Fitur Sticker Didalam Platform Instagram" *Seminar Nasional Teknologi dan Disiplin Imu,* Vol. 1 No. 1, (2021)
Hartono. "Perlindungan Hukum Pengguna Teknologi Informatika Sebagai Korban dari Perilaku Cyber Crime Ditinjau Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik." *Fakultas Hukum Universitas Sigapbangsa,* Vol. 1 No. 1 (2016).
Lisanawati, Go. "Aspek Perlindungan Data Privasi Dalam Undang Nomor 11 Tahun 2008" *Jurnal Yustika,* Vol. 15 No. 1, (2012).
Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan Di Negara Lain)" *Jurnal Yuridis,* Vol. 7 No.1, (2020).
Nurdiani, Iftah Putri. "Pencurian Identitas Digital Sebagai Bentuk *Cyber Related Crime*." *Jurnal Kriminologi Indonesia*, Vo. 16 No. 2, (2020).
Priscyllia, Fanny. "Perlidungan Privasi Data Pribadi Perspektif Perbandingan Hukum" *Jatiswara,* Vol. 34 No. 3, (2019).
Rahmawati, Ineu. "Analisis Manajemen Risiko Ancaman Kejahatan Siber (*Cyber Crime*) Dalam Peningkatan *Cyber Defense the Analitysus Of Cyber Crime Threat Risk Management To Increase Cyber Defense*" *Jurnal Pertahanan & Bela Negara*, Vo. 7 No. 2, (2017)
Rumlus, Muhammad Hasan dan Hanif Hartadi. "Kebijakan Penanggulangan Dalam Media Elektronik (Policy the Discontinuation of Personal Data Storage in Electronic Media)" *Jurnal HAM,* Vol. 11 No. 2, (2020).
Safitri, Ria. "Undang-Undang Informasi dan Transaksi Elektronik Bagi Perguruan Tinggi" *Jurnal Sosial dan Budaya Syar'I,* Vol. 5 No. 3 (2018).
Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia" *Kanun Jurnal Ilmu Hukum*, Vol. 20 No. 2 (2020).
Sonata, Depri Liber. "Metode penelitian Hukum Normatif dan Empiris: Karakteristik Khas dari Metode Meneliti Hukum" *Fiat Justisia Jurnal Ilmu Hukum*, Vol. 8 No.1, (2014).

Tacino, M. Jefri Maruli. "Perlindungan Hukum Terhadap Hak Pribadi Seseorang di Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik". *Dinamika, Jurnal Ilmiah Ilmu Hukum*, Vol. 26 No. 2, (2020).

Wahab, Abdul Rahim, dkk. "Analisis Yuridis Tentang Pertanggungjawaban Pidana Terhadap Pelaku *Cyber Crime*" *Universiras Islam Kalimantan,* (2022).

Thesis

Afuw, Tanzizal. "Perilaku Hukum Pengguna Instagram Terhadap Peretasan Data Pribadi (Studi Kasus Mahasiswa Fakultas Universitas Negeri Malang)" *Skripsi.* Fakultas Hukum Universitas Muhammadiyah Malang, 2020.

Statutory Regulations

1945 Indonesia Constitution.

Government Law (PP) No. 71 in year 2019 about Implementation of Electronic Systems and Transactions.

Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 about Protection of Personal Data in Electronic Systems.

Statutory Regulation No. 11 of 2008 of Information and Electronic Transactions.

Statutory Regulation No. 1 of 1946 about Criminal Code.