



CRIMINAL ACTS AGAINST MISUSE OF PERSONAL DATA IN CYBERWORLD

Samuel Purba¹ T. Riza Zarzani² Rahul Ardian³

¹²³Universitas Pembangunan Panca Budi

E-mail: samuelpurba333@gmail.com rizazarzani@dosen.pancabudi.ac.id
rahulardian@dosen.pancabudi.ac.id

Article Info	Abstract
Article History Received: 2025-07-05 Revised: 2025-08-06 Published: 2025-09-05 Keywords: <i>Crime, Abuse, Personal Data</i>	<p>This study aims to determine How Criminal Acts of Misuse of Personal Data Are Based on Statutory Regulations in Cyberspace. The research methodology used in this study is normative juridical research using a statutory approach, a conceptual approach, and a case approach.</p> <p>The results of the discussion stated that the regulations regarding Personal Data in Indonesia are regulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) which was ratified on Tuesday, September 20, 2022. If there is a failure in Personal Data Protection, Administrative Sanctions will be imposed under Article 57 and Criminal Provisions under Article 67 and Article 69. In the case of criminal acts, Article 70 will be imposed.</p>

I. INTRODUCTION

In the Industrial Revolution 4.0 era, computer technology and telecommunications have transformed the design of information systems and changed work patterns from ancient times to the present. Previously, it took days to transfer data or data that had to be processed before being sent to another part of the world (cyberspace), now all of this can happen in seconds. Therefore, it is inevitable that almost every activity in daily life in the digital age requires personal data. Personal data is closely related to the concept of personal privacy, which states that a person has the right to close or open spaces in their life. This makes it increasingly important to maintain the confidentiality of Personal Data.

According to Article 1 number 22 of Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, it states that "Personal Data is certain individual data that is stored, maintained, and kept accurate and its confidentiality is protected." Then, the delegated regulations of the Electronic Information and Transactions Law, namely Article 15 paragraph (1) of Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Organizers contain the obligations of Electronic System organizers, stating that:

Electronic System Organizers are required to:

- maintain the confidentiality, integrity and availability of the Personal Data it manages;
- guarantee that the acquisition, use and utilization of Personal Data is based on the consent of the owner of the Personal Data, unless otherwise stipulated by statutory regulations; and
- guarantee that the use or disclosure of data is carried out based on the consent of the owner of the Personal Data and in accordance with the purposes conveyed to the owner of the Personal Data at the time of data acquisition."

The Agency for the Assessment and Application of Technology (BPPT) stated that developments in information and communication technology (ICT) play a crucial role in increasing the speed and efficiency of various services. However, they also carry the risk of misuse of information technology from cyber threats that can cause damage or endanger information and communication technology.

In carrying out security, the Organizer must also prepare a measure that can guarantee a person that the confidentiality of his data is stored

safely without any losses arising if there is a failure in carrying out security that can cause data to be exposed to the virtual world (internet network). If this digital security system is ignored and there is no solution to the occurrence of a failure in carrying out security, it will result in an error for which the organizer of the electronic system must be responsible.

Hendri stated that the development of this technology is a result of behavioral patterns and needs in society, because of the behavior and desires of society, technology is increasingly advanced and they are also the ones who have developed ways to commit crimes, as the adage goes "where there is society there is crime".

Error is also generally defined as an act that is objectively inappropriate, because the act is at least reprehensible. Therefore, to be considered an error, it must have the following elements:

- a. the ability to be responsible;
- b. the spiritual relationship between the perpetrator and his actions, whether intentional (*dolus*) or negligent (*culpa*);
- c. there is no excuse for the mistake or no excuse for forgiveness;

In criminal law, a person who has committed a mistake can be held responsible for his mistake in the form of criminal responsibility if the mistake contains elements of criminal responsibility.

Based on this description, the researcher formulated the problem of how criminal acts of misuse of personal data are based on statutory regulations in cyberspace.

II. RESEARCH METHODS

Legal research is conducted to generate new arguments, theories, or concepts as prescriptions to address the problems faced. This research is based on normative juridical research using a statute approach, a conceptual approach, and a case approach. The analysis of this problem then goes through several stages: inventory, systematization, and finally interpretation.

III. RESULTS AND DISCUSSION

A. General Overview of Criminal Acts

The term "criminal act" comes from the Dutch criminal law term "*Strafbaar feit*," which consists of three words: *straf*, *baar*, and *feit*. "*Straf*" means

"criminal" and "law." "*Baar*" means "can" or "permissible." "*Feit*" means "act," "event," "violation," or "deed."

According to Moeljatno, a criminal act is an act that is prohibited by a legal regulation, this prohibition is accompanied by a threat (sanction) in the form of a certain penalty for anyone who violates the prohibition or punishment.

According to Vos, a crime is a human act that is threatened with punishment by regulations or laws, which means that a crime is a behavior that is generally prohibited with the threat of punishment.

A crime is a basic concept in criminal law (normative juridical). A crime or evil act in the normative juridical sense is an act as manifested in abstracto in criminal regulations.

The term criminal act is often used in legislation, although the word "act" is shorter than "deed", but "act" does not refer to abstract things such as actions, but only states concrete things, as is the case with events with the difference that an act is a person's behavior, conduct, gestures or physical attitude, which is better known as actions, actions and acting and recently "action" is also often used.

Barda Nawawi Arief stated that "a crime in general can be interpreted as an act that is against the law, both formally and materially."

People who can be declared as perpetrators of criminal acts include:

- a. The person who does (*dader plagen*)

A person who acts alone to carry out his/her goals in a criminal act.

- b. The person who orders the action (*doen plagen*)

To commit a crime, at least two people are needed, namely the person who commits it and the person who orders it to be done, so it is not the first party who commits the crime, but with the help of another party who is a tool to commit the crime.

- c. The person who does (*made plagen*)

People who commit a crime together. In this case, at least two people are required to commit a crime, namely the father and the victim.

- d. A person who exploits or abuses his position, gives wages, makes agreements, forces someone or intentionally persuades another person or party to commit a crime.

Acts that can be punished are acts that are prohibited by law and people who violate these prohibitions.

It can be concluded that a crime is an act that is against the law which results in the perpetrator being punished.

For an act to be considered a crime, it must fulfill several elements. The elements of a crime are divided into two, namely:

- a. Subjective elements, namely things that are inherent in the perpetrator or closely related to the perpetrator, most importantly those related to his inner self. These include:
 - (1) intent (dolus) or negligence (culpa)
 - (2) intention or purpose in all its forms
 - (3) whether or not there is planning
- b. Objective elements are things related to external circumstances, namely circumstances in which the crime was committed outside the perpetrator's mind.
 - (1) Fulfill the formulation of the law
 - (2) Unlawful nature
 - (3) The quality of the perpetrator
 - (4) Causality is the relationship between the cause of an action and its consequences.

Basically, criminal acts cannot be separated from two factors, namely factors within the perpetrator and factors outside the perpetrator or environmental factors.

Personal data is specific individual data that is stored, maintained, and kept accurate, as well as confidential. The term data protection was first used in Germany and Sweden in the 1970s. The rationale for this protection was the increasing use of computers to store population data, particularly for population census purposes. It turns out that in everyday life, many violations occur, both by the government and the private sector. Therefore, to prevent misuse of personal data, regulations are necessary.

Article 3 of the Draft Personal Data Protection Law explains the types of personal data, namely:

- (1) Personal Data consists of:
 - a. General Personal Data; and b. Specific Personal Data.
- (2) General Personal Data as referred to in paragraph (1) letter a includes: a. full name; b. gender; c. nationality; d. religion; and/or e. Personal data combined to identify a person.
- (3) Specific Personal Data as referred to in paragraph (1) letter b includes: a. health data and information; b.

biometric data; c. genetic data; d. sexual life/orientation; e. political views; f. criminal records; g. child data; h. personal financial data; and/or i. other data in accordance with statutory provisions.

The definition of personal data can be found in laws and regulations, including:

- a. Article 1 Number 1 and 2 of the Regulation of the Minister of Communication and Informatics No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems states that personal data is intended as a person's clear and obvious identity which is a determination of personal evidence against him which is maintained, kept true and placed safely and confidentially. Meanwhile, Article 2 number 1 regulates the acquisition, collection, processing, analysis, storage, display, announcement, delivery, dissemination and destruction of personal data which is the protection of personal data in electronic systems that respect personal data as privacy.
- b. Article 1 Number 27 of Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions, defines personal data as certain individual data that is stored and kept accurate and its confidentiality is protected.

Currently, personal data protection is contained in several laws and regulations, including:

- a. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions;
- b. Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Organizers

B. Criminal Acts of Misuse of Personal Data Based on Statutory Regulations in Cyberspace

The Personal Data Protection Bill was passed on Tuesday, September 20, 2022. The ratification of Law Number 27 of 2022 concerning Personal

Data Protection brings good news, as previously, provisions regarding Personal Data Protection were regulated in separate regulations.

Regulations regarding Personal Data in Indonesia are stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Article 4, concerning Types of Personal Data, states:

- (1) Personal data consists of:
 - a. Personal data of a specific nature; and
 - b. General personal data.
- (2) Specific personal data as referred to in paragraph (1) letter a includes:
 - a. health data and information;
 - b. biometric data;
 - c. genetic data;
 - d. criminal record;
 - e. child data;
 - f. personal financial data; and/or
 - g. other data in accordance with statutory provisions.
- (3) General personal data as referred to in paragraph (1) letter b includes:
 - a. full name;
 - b. gender;
 - c. citizenship;
 - d. religion;
 - e. marital status; and/or
 - f. personal data combined to identify an individual.

Personal data is used as identification so that others can identify us as legal subjects. Law Number 27 of 2022 concerning Personal Data Protection, Article 16, regulates the processing of Personal Data, which serves as a principle for Personal Data protection.

- (1) Personal Data Processing includes:
 - a. acquisition and collection;
 - b. processing and analysis;
 - c. storage;
 - d. fixes and updates;
 - e. appearance, announcement, transfer, dissemination, or disclosure; and/or
 - f. deletion or destruction.
- (2) The processing of Personal Data as referred to in paragraph (1) is carried out in accordance with the principles of Personal Data Protection, including:
 - a. Personal Data is carried out in a limited and specific manner, legally valid and transparent;

- b. processing of Personal Data is carried out in accordance with its purpose;
- c. processing of Personal Data is carried out by guaranteeing the rights of Personal Data Subjects;
- d. processing of Personal Data is carried out accurately, completely, not misleadingly, up to date and can be accounted for;
- e. processing of Personal Data is carried out by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, and deletion of Personal Data;
- f. processing of Personal Data is carried out by notifying the purpose and processing activities, as well as the failure of Personal Data Protection;
- g. Personal Data is destroyed and/or deleted after the retention period ends or based on the request of the Personal Data Subject, unless otherwise determined by statutory regulations; and
- h. processing of Personal Data is carried out responsibly and can be clearly explained.

- (3) Further provisions regarding the implementation of Personal Data processing as referred to in paragraph (1) are regulated in Government Regulations.

Personal Data processing must be carried out in accordance with the intended purpose and must be done by protecting the security of the Personal Data from any unauthorized access. The following are the individuals who may process Personal Data as stated in Article 18 of Law Number 27 of 2022:

- (1) Personal Data processing can be carried out by 2 (two) or more Personal Data Controllers.
- (2) In the case of Personal Data Processing carried out by 2 (two) or more Personal Data Controllers, the minimum requirements must be met:
 - a. there is an agreement between the Personal Data Controllers which contains the roles, responsibilities and

relationships between the Personal Data Controllers;

- b. there are interrelated purposes and jointly determined methods of processing Personal Data; and
- c. there is a jointly designated contact person.

According to Law Number 27 of 2022 concerning Personal Data Protection, if there is a failure to protect Personal Data, an Administrative Sanction may be imposed as stated in Article 57, namely:

- (1) Violation of the provisions of Article 20 paragraph (1), Article 21, Article 24, Article 25 paragraph (2), Article 26 paragraph (3), Article 27, Article 28, Article 29, Article 30, Article 31, Article 32 paragraph (1), Article 33, Article 34 paragraph (1), Article 35, Article 36, Article 37, Article 38, Article 39 paragraph (1), Article 40 paragraph (1), Article 41 paragraph (1) and paragraph (3), Article 42 paragraph (1), Article 43 paragraph (1), Article 44 paragraph (1), Article 45, Article 46 paragraph (1) and paragraph (3), Article 47, Article 48 paragraph (1), Article 49, Article 51 paragraph (1) and paragraph (5), Article 52, Article 53 paragraph (1), Article 55 paragraph (2), and Article 56 paragraph (2) to paragraph (4) are subject to administrative sanctions.
- (2) Administrative sanctions as referred to in paragraph (1) include: a. written warning; b. temporary suspension of Personal Data processing activities; c. deletion or destruction of Personal Data; and/or d. administrative fines.
- (3) Administrative sanctions in the form of administrative fines as referred to in paragraph (2) letter d are a maximum of 2 (two) percent of annual income or annual receipts for violation variables.
- (4) The imposition of administrative sanctions as referred to in paragraph (2) is given by the agency. (5) Further provisions regarding the procedures for imposing administrative sanctions as referred to in paragraph (3) are regulated in Government Regulations.

To prevent misuse of personal data, criminal sanctions should be imposed, as any wrongdoing must be accountable. Law Number 27 of 2022

concerning Personal Data Protection stipulates criminal provisions in Article 67, which states:

- (1) Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him/her with the intention of benefiting himself/herself or another person which may result in loss to 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 IDR 5,000,000,000.00 (five billion rupiah).
- (2) 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 imprisonment for a maximum of 4 (four) years and/or a maximum fine of IDR 4,000,000,000.00 (four billion rupiah).
- (3) Any person who intentionally and unlawfully uses Personal Data that does not belong to him/her as referred to in Article 65 paragraph (3) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah).

Article 69 of Law Number 27 of 2022 concerning Data Protection states:

In addition to being subject to the criminal penalties referred to in Article 67 and Article 68, additional penalties may also be imposed in the form of confiscation of profits and/or assets obtained or resulting from the criminal act and payment of compensation.

Article 70 of Law Number 27 of 2022 concerning Data Protection states:

- (1) In the event that the criminal acts as referred to in Article 67 and Article 68 are committed by a Corporation, criminal penalties may be imposed on the administrators, control holders, order givers, beneficial owners, and/or the Corporation.
- (2) The only criminal penalty that can be imposed on a corporation is a fine.
- (3) The maximum fine imposed on a corporation is 10 (ten) times the maximum fine threatened.
- (4) In addition to being subject to a fine as referred to in paragraph (2), Corporations may be subject to additional penalties in the form of:

- a. confiscation of profits and/or assets obtained or proceeds from criminal acts;
- b. freezing of all or part of the Corporation's business;
- c. permanent prohibition from performing certain acts;
- d. closure of all or part of the Corporation's business premises and/or activities;
- e. carry out obligations that have been neglected;
- f. payment of compensation;
- g. revocation of permit; and/or
- h. dissolution of the Corporation.

IV. CONCLUSIONS AND RECOMMENDATIONS

In Law Number 27 of 2022 concerning Personal Data Protection, if there is a failure in Personal Data Protection, Administrative Sanctions will be imposed under Article 57 and Criminal Provisions under Article 67 and Article 69. In the case of criminal acts, Article 70 will be imposed. However, the unclear regulations regarding criminal liability in the event of a failure in Personal Data Protection in Cyber Crimes create legal uncertainty for Legal Subjects.

The author suggests that the personal data protection law should clarify what types of misuse are subject to criminal penalties and what penalties will be imposed for misuse of personal data, particularly online. Data dissemination online can be very easy given the sophistication of technology.

REFERENCE LISTAN

- Adami Chazawi. (2007). Criminal Law Lessons I, Jakarta: PT. Raja Grafindo.
- B Fitrianto, TR Zarzani, A Simanjuntak, [Legal analysis of normative studies of truth and justice](#), Soumatera Law Review 4 (1), 93-103
- Barda Nawawi Arif. (1984). Abstract of Criminal Law II Lecture, Faculty of Law, Diponegoro University, Bandung.
- Hendri Diansah, Usman, Yulia Monita. (2022). "Criminal Law Policy on Carding Crimes", PAMPAS: Journal of Criminal, Vol 3 No. 1.
- I Risdawati, TR Zarzani, [Juridical Review Of Health Service Facilities Based On Law No 17 Of 2023](#), International Conference on Health Science, Green Economics, Educational

- International Journal of Law, Crime and Justice 1 (2), 108-113
- Ismu Gunadi & Joenadi Efendi. (2014). Criminal Law, Jakarta: Kencana.
- Moeljatno. (2008). Principles of Criminal Law, 8th Edition, Revised Edition, Jakarta: Renika Cipta.
- Article 15 paragraph (1) of Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Organizers
- Article 16 of Law Number 27 of 2022 concerning Personal Data Protection
- Article 18 of Law Number 27 of 2022 concerning Personal Data Protection
- Article 4 of Law Number 27 of 2022 concerning Personal Data Protection
- Article 67 of Law Number 27 of 2022 concerning Personal Data Protection
- Article 69 of Law Number 27 of 2022 concerning Personal Data Protection
- Article 70 of Law Number 27 of 2022 concerning Personal Data Protection
- R Rianto, TR Zarzani, YM Saragih, [Legal Responsibility of Online Media Corporations and Social Media Users for Broadcasting News Shared to the Public Containing ITE Crimes](#), JIIP-Scientific Journal of Educational Sciences 7 (1), 393-398
- RA Fikri, ARM Siregar, F Rafianti, S Mawarni, [Implementation Of A Restorative Approach In Child Criminal Rescue In Justice](#), Proceedings of the International Conference of Science Technology and Social
- RA Fikri, MA Siregar, MJ Rambe, N Syaharani, [Handling of Juvenile Brawl Crimes through Criminal Law Policy in Medan City](#), Sehasen Law Journal 10 (2), 481-488
- RA Fikri, MA Siregar, MJ Rambe, N Syaharani, [Strategy for Handling Criminal Acts of Fighting Due to Juvenile Delinquency in Medan City through Criminal Law Policy](#), International Conference Epicentrum of Economic Global Framework, 340-346
- Rosalinda Elsin Latumahina. (2014). Legal Aspects of Personal Data Protection in Cyberspace, Jurnal Gema Aktualita – Fhuph Surabaya, Vol. 3.
- Sahat Maruli Tua Situmeang. (2021). Misuse of Personal Data as a Form of Perfect Crime

- from a Cyber Law Perspective, Nationally Accredited Journal – FHUNIKOM, vol.27.
- Sudikno Mertokusumo. (1999). Understanding the Law, Yogyakarta: Liberty.
- TR Zarzani, I Ismaidar, W Fahriza, [Dimensions of Corporate Crime](#)
- Tri Andrisman. (2009). Criminal Law, Principles and Basic General Rules of Indonesian Criminal Law, University of Lampung.
- YM Saragih, TR Zarzani, [The law enforcement of corruption crimes in terms of authority abuse](#), International Journal of Law Reconstruction 7 (1), 54-62