KnE Social Sciences
4th INCLAR
4th International Conference on Law Reform
Volume 2024

Conference Paper

Legal Protection of Personal Data in Artificial Intelligence for Legal Protection Viewed From Legal Certainty Aspect

Muhammad Hilmy Rizqullah Ramadhan[1], Mohammad Isrok*[2], Isdian Anggraeny [2]Kyagus Ramadhani [1]Robbi Prasetyo[2]

[1]Master Of Law, Brawijaya University, Malang, Indonesia
[2]Faculty Of Law, University Muhammadiyah Of Malang, Malang, Indonesia

ORCID
Muhammad Hilmy Rizqullah Ramadhan: https://orcid.org/0000-0003-3422-3993

Abstract.
Protection of personal data is one of the rights possessed by humans, which is one of the privacy rights possessed by a person in maintaining and securing personal data owned by each individual. The development of Artificial Intelligence (AI)-based technology has developed rapidly in the digital world 4.0, where legal protection is needed in personal data protection legal instruments. This research aims to examine the use of AI as a tool in protecting personal data and to examine the urgency of a special regulation in Indonesia in protecting personal data. The research method used in writing this law is normative legal research. In this research, what is meant by juridical research is the 1945 Constitution of the Republic of Indonesia, the Law on Information, and Electronic Transactions Number 11 of 2008, the Regulation of the Minister of Communication and Information Number 20 of 2016, Government Regulation Number 82 of 2012, and UDHR by conducting a study of legal products in the form of laws and regulations. Furthermore, what is meant by normative research is related to the principle of legal certainty, which later can be linked to the urgency of personal data protection regulations for the protection, supervision, and utilization of personal data abuse.

Keywords: personal data, artificial intelligence, protection, urgency

Corresponding Author:
Mohammad Isrok; email:
mohammadisrok869@gmail.com

Published 5 January 2024

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the 4th INCLAR Conference Committee.

1. INTRODUCTION

Along with the times, especially in terms of technology and electronic information, it opens opportunities for access to information between one person and another, which includes opening access to exchange of information. It also does not rule out the possibility that the exchange of information opens opportunities to exchange information privately or privately, where in terms of the development of information technology and electronics, there is no longer any sense of boundaries regarding the space and scope of exchanging information. Indonesia has embraced the era of Industrial Revolution 4.0, where the internet and interconnected devices enable remote control of virtually

everything. This period brings significant implications as digital technology becomes an integral part of daily life, empowering people to enhance work efficiency, foster socio-economic connections, and streamline various tasks.[1] The swift advancement of computer-based information and communication technology has led to significant convenience for individuals. However, this has also resulted in a concerning issue where personal data can be accessed by others without the owner's consent or control. For instance, businesses or electronic system operators can collect personal data from customers both offline and online, and this digital data can be traded or misused without the data owner's knowledge or permission. Additionally, interconnected personal data is susceptible to being hijacked or stolen (hacked) by third parties.[2]

The misuse of personal data highlights the existence of system vulnerabilities and inadequate supervision, allowing unauthorized individuals to exploit such data, leading to losses for the data owner. The misuse, theft, or sale of personal data constitutes a violation of information technology laws and can be considered a breach of human rights since personal data is a fundamental right that requires protection. Several instances exemplify cases of personal data misuse, such as:

1. Copying customer ATM card data and information (skimming) where the skimming actor withdraws funds elsewhere.

2. Online loans, where the transaction mechanism fills in data online but in the case of late payments it is not uncommon to use collectors to intimidate customers, the customer's family, the leader where the customer works and can even access data from the customer's mobile phone. So in the case of online loan sites where after we download an application we are asked to agree to all terms and conditions and also the application asks to be allowed to access all data and contacts in our device.

This of course invites the rise of privacy violations which can lead to someone's personal data, for example, when someone does not pay a debt borrowed through an online loan, that person's personal data can be contaminated just like that. Based on these events, it can be deduced that personal data in the form of metadata, provided for various purposes like banking or e-commerce, is willingly submitted and digitally stored by businesses or individuals. However, this data is vulnerable to being accessed by unauthorized parties, either due to negligence or third-party hacking, leading to its misuse for purposes not agreed upon. Misuse of personal data involves elements of criminal acts, akin to theft and fraud, encompassing both objective and subjective aspects. Existing administrative, civil, and criminal sanctions may not be sufficient to address this form of crime, as it represents a sophisticated offense. With the rise of Indonesian social media users, it cannot be denied that there are many cases of leakage

of users' personal data. According to data from the Indonesian National Police, there are an average of 1,409 cases of fraud every year due to leaks of personal data of social media users[3]. In addition, it is also supported by a graph which provides evidence that there has been an increase in cases of sharing personal data. One of these leaks is the identification of the Artificial Intelligent platform, which can access all of our personal information and data. In Law Number 27 of 2022 it has not yet been regulated regarding the use of Artificial Intelligence in accessing the personal data of Artificial Intelligence users. Article 36 only states that in essence the Personal Data Controller is obliged to maintain the confidentiality of Personal Data. However, it is not explained more concretely related to how the government's role in regulating and controlling Artificial Intelligence is in protecting the personal data of artificial intelligence users.

The description provided above stands in stark contrast to Article 28G of the 1945 Constitution, which guarantees everyone's right to self-protection, protection of their family, honor, dignity, and controlled property, along with the right to feel secure and protected from threats and fear. These constitutional protections are further reinforced by the Law on Information and Electronic Transactions, specifically in Articles 26, 30, 31, 32, 33, and 35 of Law Number 11 of 2008. Article 26 of the Law on Information and Electronic Transactions Number 11 of 2008 explicitly states that the use of personal data through electronic means must be based on the consent of the individuals involved. Moreover, in cases of losses caused by the misuse of personal data, there are two routes to address the issue: a non-litigation approach through deliberation, and a litigation route, which involves filing a lawsuit in court to seek compensation. These legal provisions are put in place to safeguard individuals and provide a legal recourse for cases of personal data misuse.[4]

Article 26 of Law Number 11 of 2008 on Information and Electronic Transactions provides clarity on the rights of individuals, including the protection of their personal data. Additionally, Government Regulation Number 82 of 2012 regarding System Operators and Electronic Transactions emphasizes the storage, care, and safeguarding of specific individual data, ensuring its confidentiality. The definition of personal data, as outlined in Article 1 numbers 1 and 2 of Minister of Communication and Information Regulation Number 20 of 2016, refers to identifiable information that serves as clear evidence of a person's identity, maintained, guarded for accuracy, and kept securely in secrecy. Furthermore, Article 2 number 1 of the same regulation outlines the processes related to personal data, encompassing acquisition, collection, processing, analysis, storage, presentation, disclosure, transmission, dissemination, and destruction, all of which aim to protect personal data as a matter of privacy. In Government Regulation No. 82 of

2012, personal data is defined in Article 1 number 27 as specific individual data that is stored, maintained, and protected with confidentiality.[5]

The importance of safeguarding personal data is evident in its recognition as a fundamental human right, enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR). This article establishes a legal foundation for member states, emphasizing their responsibility to protect and uphold the right to privacy for all their citizens. Furthermore, the International Covenant on Civil and Political Rights also emphasizes the urgency of protecting personal data, reiterating its status as an essential human right. Both these international agreements stress the significance of preserving personal data as an inherent right for individuals in every country.

2. METHODOLOGY/ MATERIALS

The legal approach method used in writing this law is normative legal research. What is meant by juridical research in this research is the 1945 Constitution of the Republic of Indonesia, the Law on Information and Electronic Transactions Number 11 of 2008, Regulation of the Minister of Communication and Information Number 20 of 2016, Government Regulation Number 82 of 2012, and the UDHR by conducting a study of legal products in the form of laws and regulations. Furthermore, regarding what is meant by normative research is related to the principle of legal certainty which later this principle can be linked to the urgency of personal data protection regulations for the protection, supervision, and use of misuse of personal data. Qualitative analysis methods can be realized using prescriptive analysis methods, namely methods that are realized by interpreting laws by connecting them with laws related to the urgency of personal data protection regulations for legal protection against misuse of personal data.

3. RESULTS AND DISCUSSIONS

3.1. Forms of Legal Protection against Leakage of Personal Data against Electronic System Operators

In article 28G of the 1945 Constitution of the Republic of Indonesia it is stated that:

“Every person has the right to protection of self, family, honor, dignity and property under his control, and has the right to feel safe and protected from threats of fear to do or not do something that is a human right”

From the explanation above, an understanding can be drawn that everyone has the right to personal data protection which is a human right owned by a person, as seen from several cases that describe the form of legal protection against leakage of personal data that has not gone according to the wishes of article 28G of the 1945 Constitution of the Republic of Indonesia, this is of course because in that article it is still explained that it is limited to an understanding that does not lead and leads to regulations that will be regulated specifically but seen in article 28G of the 1945 Constitution of the Republic of Indonesia which in essence everyone has the right to personal self-protection which must be regulated immediately. in statutory arrangements to guarantee legal compliance itself.

Furthermore, personal self-protection apart from being contained and regulated in the 1945 Constitution of the Republic of Indonesia is also contained in the ITE Law which is divided into several articles, namely articles 26, 30, 31, 32, 33, 35 where in essence some of these articles regulate violations committed by someone in the electronic world but do not specifically regulate regulations regarding the protection of personal data, this certainly does not realize the purpose of law, namely the principle of legal certainty where the law must be clear and without being vague as described in the previous chapter, meaning that the writer saves here we need a good form of regulation to create legal certainty in the protection of personal data

Article 15 paragraph (1) of the ITE Law states that Electronic System Operators are required to operate electronic systems reliably and safely and are responsible for the proper operation of electronic systems. Article 15 paragraph (2) states that Electronic System Operators are responsible for operating their electronic systems. However, the provisions as stated in Article 15 paragraph (1) are limited by Article 15 paragraph (3) which explains the provisions of Article 15 paragraph (1) become invalid in the event that Electronic System Operations can prove the existence of a force majeure, and/or an error/negligence on the part of the electronic system user. A person who feels aggrieved as a result of the leakage of his personal data can use Article 15 paragraphs (1) and (2) as a legal basis in his lawsuit.

It should be noted that the use of Article 15 paragraphs (1) and (2) as a legal basis in the case of demands from Tokopedia cannot prove the existence of a force majeure and the fault/negligence is on the part of the user/consumer. However, the ITE Law does not specifically explain the sanctions or penalties that can be imposed on Electronic System Operators who violate the provisions of Article 15 paragraph (1) and/or (2). Further explanation is contained in Government Regulation Number 71 of 2019 concerning

Implementation of Electronic Systems and Transactions. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions is a revision of Government Regulation Number 82 of 2012. Article 3 paragraph (1) PP 71/2019 requires that PSE in the implementation of electronic systems must be carried out reliably, safely and responsibly.

In general, personal data can be defined as data that contains information about a person's identity, which can be in the form of personal codes, symbols, letters or numbers that are only attached to each individual. Within the scope of data protection regulations that already exist in Indonesia, currently, there is no specific legal instrument that regulates the use and protection of personal data. Meanwhile, the current regulations governing this matter are still contained and scattered in several laws that only reflect. Aspects of personal data protection in general and regulations that are specific in nature contain aspects of personal data protection have not been ratified. Regulations for personal data protection in general include Law Number 8 of 1997 concerning Company Documents, Law Number 36 of 1999 concerning Telecommunications, Law Number 24 of 2013 concerning Population Administration, Law Number 19 of 2016 concerning Information and Electronic Transactions, Law Number 36 of 2009 concerning Health, and Law Number 43 of 2009 concerning Archives.[6]

Regulations regarding the security of a person's personal data in Indonesia regarding the use of various services in cyberspace have been regulated in several laws, including Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE), Government Regulation Number 82 of 2012 concerning Implementation of Systems and Electronic Transactions, Peratu Regulation of the Minister of Communication and Informatics Number 20 of 2016. Some of these regulations have legally defined the definition of personal data, including Article 26 paragraph (1) of the ITE Law which reads "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, but this law has not specified a specific definition of personal data itself. But in the elucidation of Article 26 of the ITE Law it explains that "in the use of Information Technology, protection of personal data is one part of personal rights (privacy rights)". Referring to personal rights regulated in the article contains several things namely

"Personal rights are the right to enjoy private life and be free from all kinds of disturbances; Personal rights are rights to be able to communicate with other people without spying; and Personal rights are rights to monitor access to information about a person's personal life and data."

The important points that are the focus of the protection of personal data are that each individual has the right to determine for himself which data, to whom, and how completely the data can be disclosed and the protected object in this case is information about a person's personal data contained in the form of the individual's data. Therefore, protection of personal data is important because it relates to a person's right to privacy. A person's right to privacy is a manifestation of human rights inherent in each individual where the protection of this right to privacy was previously guaranteed in Article 28 G paragraph (1) of the 1945 Constitution which reads "everyone has the right to protection of himself/herself, family, honor, dignity and property under his control, and is entitled to a sense of security and protection from threats of fear to do or not do something which is a human right". Guided by this article, it can indirectly be said that the state has a legal obligation to protect the privacy of every citizen. The existence of provisions governing the protection of personal data in several regulations in Indonesia indicates that the protection of privacy rights to personal data has not yet become the focus of attention of legislators.[7]

Anticipating this, the government has actually prepared a Personal Data Protection Bill (Personal Data Protection Bill) to provide more legal certainty to the public, but it is not yet known when this bill will be passed. This Personal Data Protection Bill contains articles that regulate the protection of personal data namely

Article 23 regulates "Personal data management is obliged to carry out proper supervision of people involved in the process of organizing personal data under the orders and supervision of personal data organizers";

Article 24 regulates "Personal data providers are obliged to ensure that the personal data obtained will be managed accurately and completely in terms of: a). The personal data used will affect the legal standing of the personal data subject; b). Personal data disclosed to other parties based on the consent of the owner of the personal data"

Article 25 states "Personal data providers are responsible for ensuring the protection of personal data from unauthorized requests, collection, use, processing and disclosure".

Based on the various incidents that have occurred related to personal data breaches, such as the leakage of personal data experienced by the cases described above, it can be concluded that the protection of personal data is still at an alarming stage because the data has the potential and vulnerability to be misused by irresponsible parties who do not provide legal protection by the occurrence of personal data leaks.

3.2. Legal Implications of Legal Regulations on Personal Data as Privacy Rights in Electronic Systems from the Aspect of Legal Certainty

Today, there are many sites and applications that are easily accessible via the internet. So far, we have been provided with convenience and comfort in accessing all of these sites and applications. This is in accordance with the development of computer-based information communication technology which has developed very rapidly, so that the community is facilitated by the development of this technology. However, to access some of these electronic systems, you must first create a personal account or personal data. For example, in accessing social media such as Instagram, Whatsapp, Facebook, Line, and so on. Furthermore, to access and use e-commerce (Shopee, Grab, Gojek, and so on), we need to create an account with our personal data. Then than that, as we know and we do regarding the obligation to use the Peduli Protect application to be able to enter a place. This obligation is to find out whether a person has carried out the vaccine or not. In accessing careprotect, users are required to create an account by entering personal data such as NIK KTP, name, date of birth, and others.

This also refers to the Minister of Communication and Informatics Number 5 of 2020 concerning Implementation of Private Electronic Systems which requires all electronic system operators to register with the government. With the existence of a policy related to having an account by entering personal data which is a person's privacy rights, it is necessary to have super tight security in applications that contain someone's personal data. But in fact there were 1.4 million accounts that experienced user data leaks in Indonesia during the second quarter of 2022, according to data from cybersecurity company Surfshark. That number has jumped 143% from the first quarter of 2022 (quarter to quarter/qtq), which totaled 430.1 thousand accounts.

With data related to the spike in existing data leaks, it can be said that a person's personal data is easily accessed by other people without any control from the owner of the personal data. In this case, for example, business actors or electronic system operators can collect personal data from customers or prospective customers offline or online, where digital data can be traded without the knowledge and permission of the data owner or misused, connected personal data can also be hijacked, stolen (hack) by third parties. As is the case in the case of buying and selling personal data via the friendmarketing.com site where it is stated that those who need data can buy on that site.[4]

With the misuse of personal data, it can be seen that there are system weaknesses, lack of supervision (as explained in the previous sub-chapter), so that personal data can be misused and result in losses for the owner of the data. Misuse, theft, sale of personal data is a violation of law in the field of information technology and can also be categorized as a violation of human rights, because personal data is part of human rights that must be protected.

Regarding personal data which is a certain individual data that is stored, cared for, and guarded for truth and its confidentiality is protected. Likewise, regarding what is included in personal data, it has been stated in Article 84 paragraph (1) of Law Number 24 of 2013 including:

a. Information about Physical and/or Mental Disabilities;

b. Fingerprint;

c. iris;

d. Signature; And

e. Other Data Elements That Are Someone's Disgrace.

Likewise in Law Number 23 of 2006 Population Administration. The law explains that the personal data of residents that must be protected in article 84 includes:

a. Family Card Number,

b. NIK (Resident Identification Number).

c. Date/month/year of birth

d. Information about physical and or mental disabilities

e. biological mother's NIK

f. father's NIK, and

g. Some of the contents of the note important events

A person from the data owner to the service provider has also allowed the service provider to provide or disseminate the data to third parties, and if this really happens, then the service provider's actions can be considered to have violated the law. Therefore, if the consumer can prove that there has been a sale and purchase of data or the service owner leaked the data causing harm to the data owner as a consumer, then the consumer has the right to sue legally and ask for compensation for the losses it has caused.

In fact, the 1945 Constitution has regulated the existence of a person's right to privacy which is regulated in article 28 G of the 1945 Constitution which stipulates that every person has the right to protection of himself/herself, family, honor, dignity and property under his authority and has the right to feel safe and protected from threats of fear. In

the ITE Law it has been regulated in Articles 26, 30, 31, 32, 33, 35 of the ITE Law. In Article 26 of the ITE Law it is stated that the use of personal data through electronic media must be based on the consent of the person concerned, and losses arising from misuse of personal data can take non-litigation channels through deliberations, take litigation routes either through lawsuits in court as an effort to file for compensation. From the provisions of Article 26 paragraph 2 of the Law on Information and Electronic Transactions as mentioned above, criminal provisions have not appeared or have not been regulated, therefore reformulation of the norms is needed by adding criminal sanctions, this is so that it creates a deterrent effect even though the criminal sanction is a last resort (ultimum remedium). The absence of a clear form of legal certainty against the misuse of personal data will result in financial security that impacts the welfare of society.[8]

It cannot be underestimated also related to the data leak. Constraints against data leakage are also one of the important instruments in implementing a secure electronic system. Then, rather than that, the obstacles to legal protection for the use of personal data are inseparable from the obstacles that will be faced, for example, difficulties in tracking down the main perpetrators and proving them, difficulties in handling them, etc. Boelewoekli is of the view that the direct involvement of the government and the law in the matter of personal data is something that is needed, especially in resolving disputes that arise in the field of telematics.

Based on the description above, the protection of personal data is a shared responsibility, both the community, both individuals and legal entities and the government.[9] Because it is impossible to rely only on the prudential attitude of the people, but there must be a role for the government in making legal policies with the aim of providing protection to the community. These efforts can be through preventive efforts and repressive efforts. Preventive efforts, for example, are careful in providing personal data and monitoring efforts. There are two parties that are able and have the opportunity to carry out mass surveillance, namely the private sector and the government. Private parties can come from online service and content providers, internet service providers or internet infrastructure owners. This is because currently regulations related to personal data in general are still partial and sectoral.[10]

Protection of privacy data as part of respecting the right to privacy must begin by providing legal certainty. Therefore, guarantees for the protection of privacy data must be placed in a legal instrument that has the highest power, namely the constitution, because the Constitution or the Constitution is the highest legal instrument in a country.[11] Legal certainty (legality principle) is necessary and cannot be ruled out in the context of

law enforcement by every country. The state's step in providing legal certainty is to stipulate and guarantee these rights in the constitution, then through this instrument the character of a state can be seen regarding what matters are put forward, what legal system is used and how the government is regulated. With various explanations below. Above, it is still not comprehensively related to regulation of personal data protection, and it can be said that it is "urgent" for personal data protection laws and regulations as soon as the PDP Bill is passed.[6]

4. CONCLUSION AND RECOMMENDATION

Based on the results of research and discussion regarding the Urgency of Personal Data Protection Regulations for the Protection, Monitoring, and Utilization of Misuse of Personal Data, the authors conclude that Electronic System Operators must operate electronic systems reliably and safely and be responsible for the operation of electronic systems. Leakage of personal data is not a new thing, there are various problems such as data leakage on Tokopedia or on other platforms. So, if the validation is not carried out immediately, it does not rule out the possibility for more over-exploitation in the case of leakage of personal data due to its general explanation in Indonesia which it isn't being able to guarantee protection, supervision, and use of the law in the event of a leak of personal data. Also, the application of various regulations in various laws related to the protection of personal data is still not running perfectly. It can be seen by many cases of data leaks and abuse from year to year. There is also a legal vacuum related to the protection of personal data which explains in terms of the definition, types and legal protection of personal data in cyberspace. So, the problems that exist and have occurred make a reason related to the urgency of personal data protection regulations.

References

[1] Syaifudin, "Perlindungan Hukum Terhadap Para Pihak Di Dalam Layanan Financial-Technology Berbasis Peer to Peer (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta)". Dinamika. 2020;26(4):408–21.

[2] Aswandi R. P. R, and M. S, "Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS),". Legislatif. 2020;3(2):167–90.

[3] Tirto.id. "Pentingnya Menjaga Data Pribadi Di Era Digital." https://tirto.id/pentingnya-menjaga-data-pribadi-di-eradigital-gjb7

[4] Syailendra, “Pelaku Jual Beli Data Pribadi Punya Jutaan Salinan NIK.” https://nasional.tempo.co/read/1236549/pelaku-jual-beli-data-pribadi-punya-jutaan-salinan-nik

[5] Rahardjo S. Ilmu Hukum. Bandung: Citra Aditya Bakti; 2012.

[6] Latumahina RE. Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya. J. Gema Aktual. 2014;3(2):17.

[7] Azkiya V. “Kasus Kebocoran Data di Indonesia Melonjak 143% pada Kuartal II 2022.” https://databoks.katadata.co.id/datapublish/2022/08/09/kasus-kebocoran-data-di-indonesia-melonjak-143-pada-kuartal-ii-2022

[8] R. E. Latumahina, Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. 2014.

[9] R. Natamiharja and S. Mindoria, Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN. 2019.

[10] M. L. Aprilia and Prasetyawati, “Perlindungan Hukum terhadap Data Pribadi Konsumen Pengguna Gojek,” Mimb. Keadilan. 2017;90(105):93.

[11] Na’im Al Jum’ah, “Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi. Cyber Security dan Forensik Digital,” Cyber Secur. dan Forensik Digit., vol. 1, no. 2, p. 44, 2019.