# Criminal Law Protection Against Victims Dissemination of Personal Data in the Perspective of the Law on Personal Data Protection

Dona Raisa Monica,[1, a)] Firganefi,[2] Rendie Meita Sarie Putri,[3] Prastika Wulandari[4]

[1, 2, 3, 4] Department of Law, Faculty of Law, Universitas Lampung, Bandar Lampung, Indonesia

[a)] Corresponding author*: dona.raisa@fh.unila.ac.id*
[b)] *firganefi.1963@fh.unila.ac.id*
[c)] *rndmeitaa@gmail.com*
[d)] *prastikawulandari01@gmail.com*

**Abstract**. The development of the world's digital industry today, the use of personal data is increasing. a person easily submits personal data to online applications, such as Financial Technology and online transactions, as a condition to be able to use these services. However, the use of personal data can risk leakage and harm the community, such as the leakage of 1.3 billion SIM Card data belonging to Indonesia, 26 million Indihome data, more than 17 million PLN data, and many others. This study aims to discuss the criminal law protection for victims of personal data dissemination based on the personal data protection law which was recently passed by the DPR on 20 September 2022. This research method is normative research. The approach to the problem is the statutory approach and the conceptual approach. The results of the study show that legal protection for victims of personal data dissemination is divided into two, namely preventive legal protection provided by the government by creating cyber police. Meanwhile, repressive legal protection is in the form of criminal sanctions as regulated in Chapter XIII concerning Criminal Provisions based on the Personal Data Protection Law. The advice that the author gives is that the public is expected to be even wiser in using the internet, especially in the use of social media, and the public is also advised to be aware of the importance of personal data.

**keyword :** Digital, Victim, Protection

## INTRODUCTION

Commercial entities and governmental organizations collect, maintain, and use extensive personal information for myriad purposes, so it has become an all-but-priceless resource for exploding digital industries in the big data era. However, the burgeoning of digital industries has resulted in risk around personal information protection because of such issues as information leaks, illegal and excessive use of personal information, infringement on information privacy, and so on. The risk has created ethical and legal concerns around the world, giving rise to constant innovation in personal information protection regulations.

Unlawful acts in cyberspace are a very worrying phenomenon, considering that acts of carding, fraud, hacking of personal data, terrorism, and the dissemination of destructive information have become part of the activities of criminals in cyberspace. So it can be said that information and communication technology is like a double-edged sword, which in addition to making a positive contribution to the improvement of human welfare, progress, and

civilization, is also a potential means and an effective means to commit acts against the law. It is undeniable that such rapid technological developments have also changed people's attitudes and behaviors in communication and interaction. Almost all aspects of people's lives have always been in direct contact with technology and have proven to bring benefits to human development and civilization. Advances in technology have produced several situations that humans have never thought of before. Based on the background above, it raises the formulation of the problem of how to legally protect consumers whose personal data is hacked.

## METHOD

This research uses normative juridical and empirical juridical methods. The normative juridical approach is carried out with several approaches such as a statutory approach, an analytical approach, a comparative approach and a case approach. The empirical juridical approach is carried out by looking at, examining the actual legal conditions in society, especially related to the Criminal Law Protection Against Victims Dissemination of Personal Data in the Perspective of the Law on Personal Data Protection

## RESULTS AND DISCUSSION

Currently, information technology has developed rapidly and rapidly, so that it provides a signal of convenience that allows everyone to communicate in all corners of the world without being limited by space and time. The development is in the form of the internet, which appears and provides a new style for the community to be used as a means of communication. Therefore, the emergence of electronic media is a logical consequence of the industrial revolution 4.0 where the way of working has moved from conventional to modern.[1] When this happens, it cannot be denied that the emergence of the industrial revolution 4.0 which proposes many benefits, but has obstacles that must be faced by a country, namely in the field of law, which raises problems such as the internet has created the business world as if without limit, provides many benefits and conveniences. On the basis of this convenience, it certainly has a huge impact on the protection of personal data. Thus, the problems related to the misuse of such data and information have a relationship with the right to privacy.

The right to privacy itself is a data protection as well as a key element for individual freedom and dignity. Data protection is a driving force for the realization of political, spiritual, religious freedom and even sexual activities. The right to self-determination, freedom of expression and privacy are rights that are essential to making us human. The right to privacy is an inherent right of a person not to, or to determine, to provide his/her personal data. Therefore, when someone can access, collect or disseminate someone's personal data then this becomes a crime against privacy. Personal rights as a human right explained by danrivanto Budhijanto that protection of personal rights or privacy rights will increase human values, improve relations between individuals and their communities, increase independence or autonomy to exercise control and gain appropriateness, as well as increase tolerance and keep away from discriminatory treatment and limit government power.

Legal protection is something that protects legal subjects through applicable laws and regulations and is forced to implement them using a sanction. Legal subjects are people and legal entities. Legal protection is divided into two, namely preventive legal protection and repressive legal protection. Preventive legal protection is provided by the government to prevent before violations occur. This is contained in laws and regulations to prevent a violation and provide signs in carrying out obligations. Repressive legal protection is the final protection in the form of sanctions such as fines, imprisonment, and additional penalties given if a dispute has occurred or a violation has been committed.[2]

The data leak case that was hot in Indonesia in 2021 was an alleged data breach that was sold on online forums which was suspected to be data from a government agency, namely BPJS. Quoted from Liputan6.com, the Head of the Cyber Communication and Information System Security Research Center explained that the leaked 240MB of data contained a Population Identity Number (NIK), Mobile Number, Address, E-mail address, NPWP, place of residence and contained the number of dependents and other personal data, there are even 20 million data containing

[1] Sinaga, Erlina Maria Christin. (2020). Formulasi Legislasi Perlindungan Data Pribadi. Jurnal RechtVinding 9(2): 237–56.
[2] Moh Kusnardi dan Harmaily Ibrahim, *Hukum Tata Negara Indonesia*, Jakarta: Sinar Bakti, 1998, hlm. 102.

photos and from the leaked data there is BPJS health card number data stated by the perpetrators even having detailed data of 272,788,202 million residents. It is possible that the alleged leak came from BPJS Health because the BPJS Health number in the stolen file is the same as the name in the BPJS Health file. From this case of data leakage and theft, actually there is no data that is too sensitive, but with the presence of personal data in the form of existing photos, social media criminals are sufficient to provide real threats and misuse that harm victims, both material and immaterial losses.

The urgency to protect personal data can also be witnessed through protection of personal data which is part of human rights which is regulated by article 12 of the Universal Declaration of Human Rights (UDHR) which is the legal basis for its member countries. In this case, it is said that it is the duty of the state to protect and respect the personal data of its citizens.[3] Legal protection for the misuse of personal data can be done using the self-regulation method or what is also said as a prevention effort, if the current regulations do not reach the regime of misuse of personal data.[4] Because of this, laws or legal arrangements regarding this matter must be immediately made and ratified, given the increasing prevalence of misuse of personal data and even many other countries that have regulated and have special regulations regarding the misuse of personal data. For comparison, the protection of personal data has been regulated in the UK in 2000 by the Data Protection Act 1998, while the manager is called The Data Protection Commissioner whose job is to protect all those who own personal data.[5] Referring to Article 14 of the Data The Protection Act 1998 states that if a court finds that personal data operated by a data controller is in fact invalid, the court has the authority to order the correction, blocking, deletion or destruction of that data. Victims who are directly affected by the invalid processing of personal data can ask the board of commissioners to evaluate the process to determine whether it meets the requirements of the Data Protection Act 1998.

The protection of personal data must be guaranteed by the Indonesian government. This is something that really needs to be considered and given special attention to regulate the criminal acts that should be imposed on the perpetrators of theft of personal data. Which perpetrators use this personal data to commit violations of gospel rights that lead to unlawful acts that result in material and immaterial losses for the victims. It is generally accepted that the Indonesian Constitution, namely the 1945 Constitution, provides an understanding to protect the ownership of personal data from a person. With this acknowledgment, the big question is whether data can be considered as a fundamental right shared by all Indonesians. If the answer to this question is yes, then the follow-up to this is the role of the future government of Indonesia to care more and protect this right.

The legal basis for this personal data is regulated separately in several rules according to sectoral interests, such as Law Number 24 of 2013 concerning Population Administration. This regulation provides data protection for citizen registrants in the implementation of population administration. UU no. 24 of 2013 requires protecting personal data such as information about physical or mental disabilities, Fingerprints, Signatures and other elements that are a person's disgrace. Thing this is also regulated in Article 95A of Law Number 24 of 2013 which states that anyone who spreads personal data without rights will be punished with a term of 2 years in prison and with a maximum fine of Rp. 25,000,000.00 (twenty five million rupiahs).

Ministerial Regulation Number 20 of 2016 states that in this regulation personal data is defined as written on the basis of article 1 paragraphs 1 and 2, personal data can be interpreted as personal data that is truly attached and identifies individuals and related legal entities to keep their confidentiality and truth. This regulation only regulates separately that the protection of personal data is in the information system which includes protection against the transmission, management, storage, display and dissemination and destruction of personal data. In addition, this protection must incorporate the principles of personal data protection that provide pending rights such as for example personal data to privacy.

Government Regulation No. 82 of 2012 also defines personal data that applies to electronic systems and transactions. Article 1 number 27 explains that personal data is certain personal data that is stored, its truth is guarded to protect its confidentiality. At first glance this rule includes any information from a person but in this regulation it is not clear what is actually considered as personal data and whether anonymous data publicly available data is included in this definition. The ITE Law also regulates legal protection efforts for users of online administration services that require users to upload their personal data. Article 26 paragraphs 1 and 2 of this canon state which in paragraph 1 in connection with the use of a person's personal data, its use must be based on the

---

[3] Latumahina, R. E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. Jurnal Gema Aktualita, 3 (2). 14-25., hlm. 17.

[4] Sari, W., & Febilita. (2015). Perlindungan Hukum Atas Data Pribadi Nasabah dalam Penyelenggaraan Layanan Internet Banking Dihubungkan dengan Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas UndangUndang Nomor 7 Tahun 1992 Tentang Perbankan. Jurnal Majalah Ilmiah Unikom, 7(2), 1-11., hlm. 5.

[5] Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. Kanun Jurnal Ilmu Hukum, 20(2), 369-384., hlm. 377.

consent of the data subject in paragraph 2 confirms that if there is a violation as referred to in paragraph 1, the aggrieved party can file claim for damages received for the act. The State of Indonesia does not yet have a special legal arrangement that regulates the protection of personal data. If you look at how many definitions of legal rules or legal frameworks relating to the protection of personal data exist in Indonesia, the government should immediately pass a special law to regulate criminal acts that should be imposed on perpetrators of personal data theft. However, this plan is still under discussion and discussion.

The conclusion is that we are still lacking in regulations that regulate and provide a deterrent effect to criminal acts of theft of personal data or misuse of personal data for irresponsible persons. So this has become a joint task for the government and the community to uphold justice together. Government Regulation No. 82 of 2012 also defines personal data that applies to electronic systems and transactions. Article 1 number 27 explains that personal data is certain personal data that is stored, its truth is guarded to protect its confidentiality. At first glance this rule includes any information from a person but in this regulation it is not clear what is actually considered as personal data and whether anonymous data publicly available data is included in this definition.

The ITE Law also regulates legal protection efforts for users of online administration services that require users to upload their personal data. Article 26 paragraphs 1 and 2 of this canon state which in paragraph 1 in connection with the use of a person's personal data, its use must be based on the consent of the data subject in paragraph 2 confirms that if there is a violation as referred to in paragraph 1, the aggrieved party can file claim for damages received for the act.

The State of Indonesia does not yet have a special legal arrangement that regulates the protection of personal data. If you look at how many definitions of legal rules or legal frameworks relating to the protection of personal data exist in Indonesia, the government should immediately pass a special law to regulate criminal acts that should be imposed on perpetrators of personal data theft. However, this plan is still under discussion and discussion. The conclusion is that we are still minimal in the existence of rules that regulate and provide a deterrent effect to perpetrators of criminal acts of theft of personal data or misuse of personal data for irresponsible persons. So this has become a joint task for the government and the community to uphold justice together.

Article 28 of Ministerial Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems states that: Every Electronic System Operator must:

a. Certifying the Electronic System it manages in accordance with the provisions of laws and regulations;
b. Maintain the truth, validity, confidentiality, accuracy and relevance and conformity with the purposes of obtaining, collecting, processing, analyzing, storing, displaying, announcing, transmitting, disseminating and destroying Personal Data;
c. Notify in writing to the Owner of the Personal Data in the event of a failure to protect the confidentiality of the Personal Data in the Electronic System he manages, provided that the notification is as follows:
    1. Must be accompanied by the reason or cause of the failure to protect the confidentiality of personal data;
    2. It can be done electronically if the Owner of the Personal Data has given Consent to it stated at the time of the acquisition and collection of his/her Personal Data;
    3. It must be ensured that it has been received by the Owner of the Personal Data if the failure contains potential losses to the person concerned; and
    4. Written notice is sent to the Owner of the Personal Data no later than 14 (fourteen) days from the time the failure is known;
d. Have internal rules related to the protection of Personal Data in accordance with the provisions of laws and regulations;
e. Providing an audit track record of all activities implementing the Electronic System it manages;
f. Provide options to the Owner of the Personal Data regarding the Personal Data that he manages may/or cannot be used and/or displayed by/on third parties with the Consent to the extent that it is still related to the purposes for which the Personal Data was obtained and collected;
g. Provide access or opportunity to the Owner of personal data to change or update his/her Personal Data without disturbing the personal data management system, unless otherwise provided by the provisions of laws and regulations;
h. Destroying Personal Data in accordance with the provisions in this Ministerial Regulation or the provisions of other laws and regulations that specifically regulate in each Sector Supervisory and Regulatory Agency for it; and

i. Providing a contact person who is easily contacted by the owner of the personal data regarding the management of his personal data

## CONCLUSION

With the development of the times, technological progress is something that is very useful for humans. But in its development, technology has shortcomings, such as cyber crime, one of which is the hacking of personal data. Various laws and regulations in Indonesia that regulate the protection of personal data are not able to provide adequate protection for personal data. Personal data protection has been specifically regulated in the Regulation of the Minister of Communication and Information Technology Number 20 of 2016, but the repressive legal protection in the regulation has not been able to provide adequate protection due to the absence of sufficient sanctions to stop or reduce the perpetrators of personal data violators. The Bill on Personal Data Protection really needs to be ratified immediately considering that there are many things that pushed the bill, including increasing cases of personal data breaches, protecting and guaranteeing citizens' basic rights, as well as providing legal certainty to citizens. So with the existence of the Personal Data Protection Bill, it can accommodate several national legal principles, ranging from justice, certainty and legal benefits. Furthermore, regarding the concept of the Personal Data Protection Bill, it is the government's effort to build a special and comprehensive basis or rules in order to protect personal data, especially regarding the privacy rights of the Indonesian people, moreover, demands in the era of technological advances make crime more complex and unlimited. This Personal Data Protection Bill, in addition to specific and comprehensive rules, can also harmonize the presence of laws from each work sector as contained in the ITE law and its derivatives. With the concept of personal data protection, of course, it can protect individual personal data against misuse of collection, especially for consumers who urgently need legal protection, especially in an era where personal data is becoming more valuable for business interests, raising concerns that consumer personal data is sold or used without it. their approval. Therefore, to prioritize the Personal Data Protection Bill, it is immediately passed.

## REFERENCES


1. Abdul Halim Barkatullah, Abdul Halim Barkatullah,2017,Hukum Transaksi Elektronik, Nusa Media, Bandung.
2. Edmon Makarin, 2010, Tanggung Jawab Hukum penyelenggaraan Sistem Elektronik, Jakarta.
3. Sinaga, Erlina Maria Christin. 2020. Formulasi Legislasi Perlindungan Data Pribadi. Jurnal RechtVinding.
4. Moh Kusnardi dan Harmaily Ibrahim, 1998, *Hukum Tata Negara Indonesia*, Jakarta: Sinar Bakti.
5. Latumahina, R. E. 2014. Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. Jurnal Gema Aktualita.
6. Sari, W., & Febilita. 2015. Perlindungan Hukum Atas Data Pribadi Nasabah dalam Penyelenggaraan Layanan Internet Banking Dihubungkan dengan Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas UndangUndang Nomor 7 Tahun 1992 Tentang Perbankan. Jurnal Majalah Ilmiah Unikom.
7. Sautunnida, L. 2018. Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. Kanun Jurnal Ilmu Hukum.
8. Soerjono Soekanto, 1985, Penelitian Hukum Normatif Suatu Tinjauan Singkat, CV. Rajawali, Jakarta.
9. Kornelius Benus, Siti Mahmudah, dan Ery Agus Priyono, 2019, Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia, Jurnal ilmu Hukum, Vol.3 No.2.
10. Lia Sautunnida, 2018, “Urgensi Undang - Undang Perlindunngan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia”, Kanun Jurnal Ilmu Hukum , Vol.20, No.2
11. Shinta Dewi Rosadi, 2015, Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, Refika Aditama, Bandung.
12. Phillipus M. Hadjon, 1987, Perlindungan Hukum Bagi Rakyat Indonesia, Bina Ilmu, Surabaya.