

# LEGAL PROTECTION AGAINST HACKED CONSUMER PERSONAL DATA

Joice Soraya

*Faculty of Law, Wisnuwardhana University Malang, Terusan Danau Sentani No.99 65139, IDN  
joicewijayas99@gmail.com*

**Abstract.** With the development of the times, the advancement of technology is a very useful thing for humans. However, in its development, technology has shortcomings, such as cyber crimes, one of which is hacking personal data. Cyber abuse creates several problems including legal issues. One of the legal issues that arise is the issue relating to the protection of personal data. Various laws and regulations in Indonesia, which regulate personal data protection, cannot provide sufficient protection for personal data. Based on the background above, the formulation of the problem in this article is how to legally protect consumers whose personal data is hacked. The research method in writing this article is to use normative legal research methods. The results of this study are first, the protection of personal data has been specifically regulated in the Regulation of the Minister of Communication and Informatics No. 20 of 2016, but the repressive legal protection in the regulation has not been able to provide sufficient protection because there does not have sufficient sanctions to stop or reduce perpetrators of personal data violators. Forms of the legal protection of consumers' data. Preventive legal protection is protection provided by the government to prevent the occurrence of violations. Repressive legal protection is legal protection carried out based on a decision established by a legal entity of a binding nature aimed at resolving a dispute.

**Keywords:** personal data, legal protection, electronic systems

## INTRODUCTION

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

The type of research in writing this article is to use the method of writing normative laws. The method of writing Normative Law is a legal research method that describes the condition of norms that conflict with norms (*geschijld van normen*), vague or unclear norms (*vague van normen*) or empty norms (*leetmen van normen*). Normative research is literature law

research or legal research based on data, namely secondary data.<sup>1</sup> This research approach method uses the provision of laws, as well as the provision of the Conceptual.

## RESULTS AND DISCUSSION

Indonesia is a country of law and is included in Article 1 paragraph (3) of the 1945 Constitution. The principle of protection in the State of law appears inter alia in the declaration of independence, the declaration contains the principle that the person living in this world, has been created free by God, by being endowed with some rights that cannot be deprived or destroyed, the right is expressly protected in the State of law.

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.<sup>2</sup>

Data protection can relate to specific privacy, as stated by Allan Westin who for the first time defined privacy as the right of individuals, groups, or institutions to determine whether or not information about them will be communicated to others so the definition put forward by Westin is called information privacy because it concerns personal information.<sup>3</sup> The reasons why privacy should be protected are:

1. In cultivating relationships with others, a person must close part of his personal life so that he can maintain his position at a certain level.
2. A person in his life needs time to be able to be alone (solitude) so privacy is indispensable for a person.
3. Privacy is a right that stands alone and does not depend on anything else but this right is lost if the person publishes matters of a private nature to the public.
4. Privacy also includes a person's right to have domestic relationships including how a person fosters marriage and fosters his family and others should not know about those personal relationships so then Warren refers to it as the right against the word.
5. Another reason why privacy deserves legal protection is that the losses suffered are difficult to assess where the losses are felt to be much greater than physical losses

---

<sup>1</sup> Soerjono Soekanto, *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, CV. Rajawali, Jakarta, 1985, pp. 15.

<sup>2</sup> Moh Kusnardi dan Harmaily Ibrahim, *Hukum Tata Negara Indonesia*, Jakarta: Sinar Bakti, 1998, pp. 102.

<sup>3</sup> Kornelius Benus, Siti Mahmudah, dan Ery Agus Priyono, *Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia*, Jurnal ilmu Hukum, Vol.3 No.2, April, 2019, pp. 155.

because they have interfered with their personal lives so if there are losses suffered, the victims must be compensated.<sup>4</sup>

Protection of Personal Data is divided into two forms, namely the form of data protection in the form of securing the physical data, both visible data and invisible data. The second form of data protection is the existence of a regulatory side that regulates the use of data by unauthorized others, misuse of data for certain interests, and destruction of the data itself.<sup>5</sup>

Personal Data protection arrangements are intended to protect the interests of consumers and provide economic benefits to Indonesia. The consumers referred to in this study are the end consumers. This arrangement will protect consumers' data against misuse when the data has a high value for business purposes, the collection, and processing of which becomes easier with the development of information and communication technology. The development of regulations on the protection of personal data, in general, will put Indonesia on an equal footing with countries with developed economic levels, which have implemented laws regarding the protection of personal data. For the benefit of consumers, the need for the protection of consumers' personal radically in an era where Personal Data is becoming more invaluable to business interests, raises concerns that consumers' data is used without consumer consent. For this reason, there is a need for a law regarding the protection of Personal Data of a special nature to ensure that consumers' data is protected.

Regulation on Personal Data is very necessary because it regulates the collection, use, disclosure, transfer, and security of personal data of individuals with the needs of governments and business people to obtain and process personal data for reasonable and lawful purposes.<sup>6</sup>

Meanwhile, the forms of the legal protection of consumers' data are divided into two of them:

1. Preventive Legal Protection

The protection is provided by the government to prevent the occurrence of violations. This is contained in laws and regulations with the intention of preventing a violation and providing signs or restrictions in carrying out an obligation. Ministerial Regulation Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. For the prevention of cyber hacking, internal regulations or self-regulation by each electronic system operator are needed. In practice, self-regulation cannot run alone without the intervention of the state that provides regulation and information for consumers to business actors (electronic system operators) who are safe for transactions. Therefore, the state regulates Article 5 (1) of Ministerial Regulation Number 20 of 2016 concerning the protection of personal data in the electronic system of electronic system operators, which requires electronic system operators to have internal rules regarding the protection of personal data of their consumers. With the

---

<sup>4</sup> Andrew pelealu, *Tesis: "Perlindungan Hukum Atas Data Pribadi Konsumen Dalam Transaksi E-Commerce"*, Yogyakarta : Universitas AtmaJaya Yogyakarta, 201), pp. 18-19.

<sup>5</sup> Lia Sautunnida, "*Urgensi Undang - Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia*", *Kanun Jurnal Ilmu Hukum* , Vol.20, No.2, Agustus, 2018, pp. 374.

<sup>6</sup> Shinta Dewi Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*, Refika Aditama, Bandung, 2015, pp. 15.

rules on self-regulatory standards provided by the government, it is hoped that the security of consumers' data can be properly maintained by electronic system operators, and can prevent hacking or hacking actions that target consumers' data.

## 2. Repressive Legal Protection

Repressive legal protection is legal protection carried out based on decisions set by legal entities of a binding nature aimed at resolving a dispute.<sup>7</sup> The provisions regarding personal data as previously stated are a provision that places an electronic system provider company as a party that is obliged to always maintain all personal data of its consumers. Violations of the provisions of personal data have been regulated by Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning electronic information and transactions (ITE Law). Article 30 of the ITE Law emphasizes the perpetrators of hacking (Hackers). As an effort to protect the repressive law intended for consumers so that there is legal certainty when the personal data they have is used unlawfully for certain interests. As for the provisions of Article 36 (1) of Ministerial Regulation Number 20 of 2016 concerning personal data in electronic systems, it provides administrative sanctions to everyone who misuses someone's data.

The emergence of rights and obligations between the electronic system provider company and the consumer is when the consumer agrees to the term of Service (terms of service) provided by the electronic system provider company. That way there has been an agreement that has occurred between the parties. The Term of Service is an electronic contract provided by an electronic system delivery company to consumers to meet or follow the regulations that have been made by the electronic system provider company. In this case, consumers entrust the personal data they have to process to the company that organizes the electronic system.

The Civil Code clearly distinguishes between an agreement arising from an agreement and an agreement arising from an Act. The legal consequences of an agreement born of an agreement are indeed desired by the parties because indeed the agreement is based on an agreement, namely the conformity of will between the parties who agree. As for the legal consequences of an agreement born of law, it may not be desired by the parties but the legal relationship and its legal consequences are determined by law. If there is a violation of the agreed agreement, a tort lawsuit can be filed, because there is a contractual relationship between the party that caused the loss and the party who suffered the loss. If there is no contractual relationship between the party who caused the loss and the party who received the loss, a lawsuit against the law can be filed.

Dispute resolution two channels can be used by consumers to resolve personal data disputes, namely litigation (through the court) by making a civil lawsuit against the electronic system operated by the procedures set by the law. The next step is the settlement of disputes outside the court (non-litigation) can be taken through BPSK (Consumer Dispute Resolution Agency) whose duties and authorities include the implementation of handling and resolving consumer disputes, using mediation or arbitration, or conciliation, which in

---

<sup>7</sup> Phillipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia*, PT. Bina Ilmu, Surabaya: 1987. Pp. 29.

addition to being a medium for dispute resolution can also impose administrative sanctions on business actors (electronic system operators) who violate the prohibitions certain that are imposed on business actors. This is as stipulated in Article 52 of Law Number 8 of 1999 concerning Consumer Protection.

In the Ministerial Regulation Number 20 of 2016 concerning Personal Data Protection, it also regulates the procedures for resolving disputes that occur, this is regulated in Articles 29 to 33. In its provisions, consumers can complain that there has been a failure to protect Personal Data to the ministry of communication and informatics. Consumers are no later than making complaints to the Ministry of Communication and Informatics, which is for 30 days after consumers learn of a failure to protect their personal data. In his report the consumer must bring supporting evidence. If the complaint has been received by the Ministry of Communication and Informatics, the Personal Data dispute resolution agency must respond to the complaint no later than 14 working days from the time the complaint is received. The resolution of this Personal Data dispute is carried out by deliberation or through other alternative settlements. If the consultancy does not find an agreement, the consumer can file a civil lawsuit in accordance with the provisions of the law.

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, the advancement of technology is a very useful thing for humans. However, in its development, technology has shortcomings, such as cyber crimes, one of which is hacking personal data. Various laws and regulations in Indonesia, which regulate the protection of personal data are not able to provide sufficient protection of personal data. The protection of personal data has been specifically regulated in the Regulation of the Minister of Communication and Informatics No. 20 of 2016, but the repressive legal protection in the regulation has not been able to provide sufficient protection because there are not enough sanctions to stop or reduce perpetrators of personal data violators. Forms of the legal protection of consumers' data. Preventive legal protection is protection provided by the government to prevent the re-occurrence of violations. Repressive legal protection is legal protection carried out based on a decision set by a legal entity of a binding nature aimed at resolving a dispute. The responsibility of the company that organizes electronic systems in case of hacking of personal data against its consumers. The emergence of rights and obligations between the electronic system provider company and the consumer is when the consumer agrees to the term of Service (terms of service) provided by the electronic system provider company. That way there has been an agreement that has occurred between the parties.

## **REFERENCES**

- [1] DR. Siswanto Sunarso, SH, MH, M.Kn, Hukum Informasi dan Transaksi Elektronik, Jakarta, 2009, pp. 39.
- [2] Maskun, Kejahatan Siber Cyber Crime, (Jakarta: Kencana Prenada Media Grup, 2013), pp. 29.
- [3] Edmon Makarin, Tanggung Jawab Hukum penyelenggaraan Sistem Elektronik, Jakarta, 2010 pp. 2.
- [4] Soerjono Soekanto, Penelitian Hukum Normatif Suatu Tinjauan Singkat, CV. Rajawali, Jakarta, 1985, pp. 15.

[5] Moh Kusnardi dan Harmaily Ibrahim, Hukum Tata Negara Indonesia, Jakarta: Sinar Bakti, 1998, pp. 102.

[6] Kornelius Benus, Siti Mahmudah, dan Ery Agus Priyono, Perlindungan hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia, Jurnal ilmu Hukum, Vol.3 No.2, April, 2019, pp. 155.

[7] Andrew pelealu, Tesis: “Perlindungan Hukum Atas Data Pribadi Konsumen Dalam Transaksi E-Commerce”, Yogyakarta : Universitas AtmaJaya Yogyakarta, 201), pp. 18-19.

[8] Lia Sautunnida, “Urgensi Undang - Undang Perlindungan Data Pribadi di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia”, Kanun Jurnal Ilmu Hukum , Vol.20, No.2, Agustus, 2018, pp. 374.

[9] Shinta Dewi Rosadi, Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, Refika Aditama, Bandung, 2015, pp. 15.

[10] Phillipus M. Hadjon, Perlindungan Hukum Bagi Rakyat Indonesia, PT. Bina Ilmu, Surabaya: 1987. pp. 29.

[11] Abdul Halim Barkatullah, Abdul Halim Barkatullah, Hukum Transaksi Elektronik, Nusa Media, Bandung, 2017, pp. 138.