

## **Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage**



**Yudo Arhuma Binardy<sup>1</sup>, Joko Setiyono<sup>2</sup>**

<sup>1,2</sup>Master of Law Program, Faculty of Law, Universitas Diponegoro, Semarang

**ABSTRACT:** This study aimed to analyze the legal protection arrangements in Indonesia for privacy rights in cases of personal data leakage and to examine the urgency of the establishment of the Personal Data Protection Law as an effort to prevent personal data leakage. This study used a normative juridical research approach, the type of data was secondary data with data collection techniques in the form of library research and documentation studies. The results of this study are that the privacy right gets legal protection in Indonesia through Law Number 19 of 2016 concerning Information and Electronic Transactions, also regulated in its implementing regulations, namely Government Regulation Number 71 of 2019 and Regulation of the Minister of Communication and Information Technology Number 20 of 2016. The regulation has not been able to overcome the rampant cases of privacy rights violations and has not been able to protect the owner of personal data. The stipulation of a personal data protection law as an effort to combat the leakage of personal data is an urgent matter to meet the demands of information disclosure in government institutions and protect individual rights concerning collection, processing, maintenance, dissemination of personal data.

**KEYWORDS:** Protection, Personal Data, Leakage, and Privacy Rights

### **A. INTRODUCTION**

The rapid development of technology in addition to providing a positive impact is also an effective means to commit the crime of "cybercrime." Cybercrime began to bloom in 2003. Information, such as carding crimes (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware (viruses/worms/trojans/bots), cybersquatting, pornography, online gambling, transnational crime (drug trafficking, mafia, terrorism, money laundering, human trafficking, underground economy) started happened since then (Rumlus & Hartadi, 2020).

One form of cybercrime that is currently rife is the violation of privacy rights due to the leakage of personal data. In Indonesia, cases of leakage of personal data throughout 2020 that attracted a lot of public attention include: first in early May 2020, as many as 91 million user data and more than seven million Tokopedia merchant data were sold on dark websites that include gender, location, username, user's full name, e-mail address, mobile number, and password, a group of hackers by the name of ShinyHunters claims to have sold 1.2 million Bhinneka.com customer data. ShinyHunters reportedly sold 1.2 million Bhinneka.com users with a tag of 1,200 US dollars or around Rp. 17.8 million in May 2020, millions of population data belonging to Indonesian citizens including much sensitive information, such as full names, family card numbers, identification numbers Citizenship (NIK), place and date of birth, home address, and several other personal data were allegedly leaked and shared through the hacker community forum. The data is claimed to be the 2014 Election DPT data. Data belonging to a technology company from Indonesia engaged in the financial sector (fintech), Kreditplus, was allegedly leaked and sold freely on the internet in August 2020. The leak of KreditPlus user data about 890,000 Kreditplus customers is described in a report from the cybersecurity firm from the United States, Cybele (Stephanie, 2021).

In May 2021, another mass leak of personal data occurred, namely the leak of BPJS Kesehatan data containing card numbers, family data or dependent data, and payment status. This case was discovered after an account called Kotz who acted as a buyer and seller of personal data (reseller) offered it on an online forum Raid Forums. The seller claims to have 279 million copies of the identity data of Indonesian citizens by showing approximately 100,000 examples (Widayati, 2021).

Cases of privacy rights violations related to personal data leakage in Indonesia are difficult to resolve. The right to privacy is currently protected by law in Indonesia through several laws and regulations such as Article 26 of Law Number 19 of 2016 concerning Electronic Information and Transactions that any electronic information containing personal data may only be used with the person's permission. To provide legal protection, the Government has formed a Bill on Personal Data Protection (RUU PDP) as an effort to prevent the leakage of personal data. However, the government has not been able to provide protection to the owners of personal data and overcome the rampant cases of personal data leakage in Indonesia. Based on the above background, the formulation of the problem in this research are how is the regulation of legal protection in Indonesia for privacy

## Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage

rights in cases of personal data leakage? and what is the urgency of the establishment of the Law on Personal Data Protection as an effort to prevent the leakage of personal data?

### B. RESEARCH METHOD

The research approach used normative juridical research, namely research based on secondary data sourced from various legal regulations, court decisions, legal theories, and legal expert doctrines (Sunggono, 2015). This approach was chosen because it will study whether there is consistency between the Law and Government Regulations governing the protection of privacy data in electronic systems. The research specification used was descriptive-analytical which aimed to provide an overview and answer questions regarding the regulation of legal protection in Indonesia for privacy rights in cases of personal data leakage and the urgency of the formation of a law on the protection of privacy rights as an effort to overcome the criminal act of leaking personal data.

This study used secondary data as the main data. Secondary data was sourced from literature studies by reviewing or studying various legal books and legislation related to research problems. The secondary data in this study came from legal materials, both primary, secondary and tertiary legal materials. Primary legal materials come from (1) Law Number 19 of 2016 concerning Electronic Information and Transactions; (2) Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions; and (3) Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Privacy Data in Electronic Systems.

Mechanical collection of legal materials to be used as a resource in this research was the study of literature and documentation study. The research data already collected by the researchers then qualitatively analyzed through the logical study to think deductively (Amiruddin & Asikin, 2015). Deductive logic may mean that researchers in making conclusions from this research problem succinctly ranging from the general to the particular case to as the normative research which makes the deductive method as the main grip. In analyzing the data juridical normative are the stages: first, formulate the secondary data and the data of positive law into their principles of law, the second is to formulate the notion of law related to the research problem, the third form applicable legal standards related to the research problem and fourth, legal obstacles encountered are formulated in detail and clearly (Amiruddin & Asikin, 2015).

### C. RESULT AND DISCUSSION

#### 1. Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage

In general, personal data is defined as very personal information that is kept for oneself or at least only known by a limited number of people. Personal data itself is part of a person's right to monitor access to information about his personal life and data. It is essential and crucial for personal data to be kept confidential. Problems with personal data will arise when the confidentiality of personal data cannot be protected so that it is vulnerable to being misused against the law. Another crucial reason why personal data must be guarded and protected is that personal data is part of a person's privacy aspect (Rosadi, 2016). In the current digitalization era, personal data has become a commodity that has economic value so that it can be traded (Kornelius Benuf, 2021).

Regarding personal data, it is regulated in Article 1 of the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 that says:

"Personal Data is certain individual data that is stored, maintained and kept true and is protected by confidentiality".

Then Article 3 states that the protection of personal data in the electronic system is carried out in the process; acquisitions and collecting, processing and analyzing, storing, appearing, announcing, delivering, dissemination and or access opening, and destructing. Regarding the right to privacy, it has been included in several regulations in Indonesia. Especially in the 1945 Constitution, in Article 28 G paragraph (1) which, although it does not explicitly explain data privacy, this article still concerns the freedom of individuals to store information and protect data and information attached to them. Meanwhile, Russell Brown defines the right to privacy as the right to private property of a particular resource (Brown, 2006).

In general, the protection of the right to privacy can be categorized in 4 ways, namely: first, information privacy, which involves the establishment of regulations governing the collection and handling of personal data such as financial information and medical records. The second is body privacy, which involves protecting people's physical self against invasive procedures such as drug testing and cavity searching. Third, communication privacy, which includes the security and privacy of mail, telephone, e-mail, and other forms of communication; and Fourth, territorial privacy, which concerns setting boundaries for intrusion into the domestic and other environments (Anggara, 2015).

Personal data protection is a form of privacy right which is an individual right so it must be guaranteed by the state (Tebbit, 2017). The concept of personal data protection implies that individuals have the right to determine whether or not to share their

## Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage

personal data (David Marrani, 2009). Privacy rights through personal data protection are very important and even a key element for individual freedom and dignity (Lokugamage & Pathberiya, 2017). The protection of personal data is a strong driver for the realization of political, spiritual, religious, and even sexual freedom. The right to self-determination, freedom of expression, and privacy are rights that are essential to making us human (Benuf et al., 2019). Everyone who feels that their privacy has been violated has the right to file a lawsuit known as a *privacy tort*. The reference to Indonesian legal products, the Law concerning Protection of Personal Data in Electronic Systems of 2016 Article 2 paragraph 3 that privacy is the freedom of the owner of personal data to declare secret or not to disclose the secret of his personal data unless otherwise stipulated in accordance with the provisions of the legislation.

The right to privacy is currently protected by law in Indonesia through several laws and regulations such as Article 26 of Law Number 19 of 2016 concerning Electronic Information and Transactions that any electronic information containing personal data may only be used with the person's permission. Then the Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and also the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Privacy Data in Electronic Systems (Raila et al., 2021). However, these regulations are not able to overcome the rampant cases of violation of privacy rights so that they have not been able to protect the owner of the personal data.

### 2. Urgensi Pembentukan Rancangan Undang-Undang Tentang Perlindungan Data Pribadi Sebagai Upaya Penanggulangan Pembocoran Data Pribadi

Weak protection of citizen privacy is also recognized by the government because the protection of personal data has not been regulated in law, but the regulation has begun to be included in Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions. The government itself wants to also establish the protection of personal data into law. In fact, mobile service users in Southeast Asia and Oceania in 2014 were 950 million and by the end of 2020, it is estimated to reach 1,240 million. Data usage traffic increased nine times. This condition is prone to misuse of users' personal data (Anggara, 2015).

Based on the weak protection of privacy, the government took the initiative to draft a Bill on the Protection of Personal Data and Information (RUU PDP). The PDP Bill was drafted because of the need to protect individual rights in society concerning the collection, process, administration, and dissemination of personal data. Adequate protection of privacy regarding personal data will be able to give the public the confidence to provide personal data and information for the wider community's interests without being misused or violating their personal rights.

The presence of the PDP Bill to be enacted into the PDP Law is urgently needed because of the demands for openness in government institutions. Indonesia is also one of the initiators of the Open Government Partnership (OGP) Movement which was formed in September 2011 together with 7 other countries: the United States, Brazil, Mexico, England, Norway, South Africa, and the Philippines. As the initiator of the OGP, Indonesia launched the Open Government Indonesia movement in January 2012. This OGI movement is an implementation of Law No. 14 of 2008 concerning the Openness of Public Information. Through this movement, Information Management and Documentation Officers have been formed in all ministries and agencies and around 30% of Local Governments. Indonesia has also succeeded in increasing its Open Budget Index (OBI) from 51 in 2010 to 59 in 2015.

This bill contains provisions on the definition and classification of the types of personal data that must be protected. In addition, this bill also outlines the procedures that must be followed when collecting, processing, and managing personal data. This bill consists of 16 chapters with 46 articles that are expected to create a balance between the rights of individuals and communities whose interests are represented by the state. Regulations regarding the privacy of personal data and information will make a major contribution to the creation of order and progress in the information society. Until now, the PDP Bill is still in the process of being discussed by the government (Anggara, 2015).

The objectives to be achieved by the PDP Bill are: (1) protect and guarantee the basic rights of citizens related to the privacy of personal data; (2) guarantee the public to get services from the government, business people, and other community organizations; (3) encourage the growth of the technology, information and communication industry; and (4) supporting the improvement of the competitiveness of domestic industries (Anggara, 2015).

The PIDP Bill divides the notion of personal data into two types, namely ordinary personal data and sensitive personal data. Sensitive personal data is defined as personal data which includes: religion/belief, health condition, physical and mental condition, sexual life, personal financial data, and others. While general personal data is data related to a person's life that can be identified either automatically or based on a combination with other information such as name, passport number, photos, videos, electronic mail, fingerprints, and others.

Sensitive personal data can be provided through written consent in terms of protecting the safety of the data subject; achieving the goal of fulfilling every right & obligation based on employment law; implementation of things related to medical

## Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage

purposes; law enforcement processes; implementation of the functions of various parties having the authority based on the laws and regulations; and sensitive personal data is already in the public domain.

The problem is that the PDP Bill does not have special provisions related to sensitive personal data or special procedures related to sensitive personal data. Currently, available regulations do not classify personal data, especially those that can be categorized as sensitive personal data. For example, related to medical records, based on Law No. 36 of 2009 concerning Health, hospitals are prohibited from publishing such data. Likewise, regarding a person's financial data which is categorized as privacy based on Law No. 6 of 1983 on Taxation (amended based on Law No. 16 of 2009) and Law No. 7 of 1992 concerning Banking (amended based on Law No. 10 of 1998). Meanwhile, data related to mental and physical health, fingerprints, and retinas are categorized as personal data based on Law No. 23 of 2006 concerning Population Administration (amended based on Law No. 24 of 2013).

The PDP Bill (RUU PDP) is an effort to prevent the leakage of personal data. It is hoped that the existence of the PDP Bill will be able to regulate clearly and unequivocally regarding the accountability of the parties to the leakage of personal data in the future starting from the Director-General in the field of informatics applications, the Minister of Communication and Informatics, business people, electronic system users, electronic system operators, and personal data owners.

According to Hans Kelsen, responsibility is closely related to obligations, but not identical. This obligation arises because of the rule of law that regulates and gives obligations to legal subjects as orders from the rule of law. If the obligation is not carried out, it will result in sanctions. This sanction is a forced act of the rule of law so that obligations can be carried out properly by legal subjects. According to Hans Kelsen, legal subjects who are subject to sanctions are said to be "responsible" or legally responsible for violations (Kelsen, 2014).

Legal liability has several principles, including the principle of *liability based on fault*, which states that a person can be held legally responsible if an element of error has been committed. The "*presumption of liability principle*" is that the defendant is always considered responsible until he can prove that he is innocent. In this case, the reverse burden of proof applies to the defendant. The principle of presumption of not always being responsible. The principle of absolute responsibility, the principle that does not question the existence of an element of error, whether intentional or negligence as an element. The defendant can be directly held accountable without having to prove the element of guilt (Rezky & Tadjuddin, 2018).

### D. CONCLUSION

Based on the study results, it can be concluded that: (1) The right to privacy has legal protection in Indonesia through several laws and regulations such as Article 26 of Law Number 19 of 2016 concerning Electronic Information and Transactions that any electronic information containing personal data may only be used with the permission of that person. Then the Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions and the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Privacy Data in Electronic Systems. However, these regulations are not able to overcome the rampant cases of violation of privacy rights so that they have not been able to protect the personal data owner. (2) The formation of a bill on the protection of personal data as an effort to prevent the leakage of personal data is an urgent matter for the demands for information disclosure in Government institutions and to protect individual rights in the community concerning the collection, process, administration, and dissemination of personal data.

### BIBLIOGRAPHY

- 1) Amiruddin, & Asikin, H. Z. (2015). *Pengantar Metode Penelitian Hukum*. PT. Raja Grafindo Persada.
- 2) Anggara. (2015). Menyeimbangkan Hak : Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia. In *Institute For Criminal Justice Reform (ICJR)*.
- 3) Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum terhadap Keamanan Data Konsumen Financial Technology di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, 3(2), 145–160. <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>
- 4) Brown, R. (2006). *Rethinking Privacy: Exclusivity, Private Relation and Tort Law*. 43, 589–592.
- 5) David Marrani. (2009). Human Rights and Environmental Protection: The Pressure of the Charter for the Environment on the French Administrative Courts. *Sustainable Development Law & Policy*, 88(4), 52–57.
- 6) Kelsen, H. (2014). *Pure Theory of Law, terjemahan oleh Raisul Muttaqien, Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif*. Nusa Media.
- 7) Kornelius Benuf. (2021). Hambatan Formal Penegakan Hukum Pidana Terhadap Kejahatan Pencurian Data Pribadi. *Majalah Hukum Nasional*, 51(2), 261–279.
- 8) Lokugamage, A. U., & Pathberiya, S. D. C. (2017). Human rights in childbirth, narratives and restorative justice: a review. *Reproductive Health*. <https://doi.org/10.1186/s12978-016-0264-3>

## Legal Protection Arrangements in Indonesia for Privacy Rights in Cases of Personal Data Leakage

- 9) Raila, T. A., Rosadi, S. D., & ... (2021). Perlindungan Data Privasi Di Indonesia Dan Singapura Terkait Penerapan Digital Contact Tracing Sebagai Upaya Pencegahan Covid .... *Jurnal Kepastian ...*, 2, 1–16.
- 10) Rezky, W. A. S., & Tadjuddin, N. (2018). *Hukum Perlindungan Konsumen*. Mitra Wacana Media.
- 11) Rosadi, S. D. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, 9(3), 403–420. <https://doi.org/10.20961/yustisia.v0i94.2780>
- 12) Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, 11(2), 285. <https://doi.org/10.30641/ham.2020.11.285-299>
- 13) Stephanie, C. (2021). 7 Kasus Kebocoran Data yang Terjadi Sepanjang 2020 Halaman all - Kompas.com. In *Kompas.com*.
- 14) Sunggono, B. (2015). *Metodologi Penelitian Hukum*. PT. Raja Grafindo Persada.
- 15) Tebbit, M. (2017). *Philosophy of Law: An Introduction*. Routledge.
- 16) Widayati, L. S. (2021). Kebocoran Data Pribadi dan Urgensi Pembentukan UU Perlindungan Data Pribadi. *Isu Sepekan, Bidang Hukum. Pusat Penelitian Badan Keahlian Sekretariat Jendral DPR RI*, 4, 1–2.