Criminal Law Policy to the Perpetrator of Data Leakage in Indonesia

Bryan Terra Alderino Sianipar[1*], Pujiyono[2], Nur Roechaeti[3]
{bryansianipar18@gmail.com[1*], pujifhundip@yahoo.com[2]}

Faculty of Law, Diponegoro University, Semarang, Indonesia[1,2,3]

Abstract. The passage of time has resulted in abuses of the right to privacy occurring not just in the offline realm but also in the public sphere. Efforts to combat leakage of private data can be made through a criminal law policy, such as the enactment of a statute that particularly governs the Protection of Private Information. The method employed is normative legal research. This study also employs a comparative method to examine criminal law regulations against personal data leaking in Indonesia and surrounding countries such as the United Kingdom, Hong Kong, Malaysia, and Singapore. According to the findings of this study, Indonesia's legal protection policy for individual rights in the leakage of personal data is currently dispersed among multiple laws and regulations. It has not been able to provide optimal and effective protection for private information as part of the right to privacy. Digital networks are now implementing this legal protection strategy in the form of a personal data leakage avoidance policy, personal data theft prevention policy, personal information security policy, and private data security policy.

Keywords: Personal Data, Data Leakage, and Criminal Law Policy.

1 Introduction

Advances in communication and information technology positively impact human life with various advantages and conveniences that contribute to improving human civilization's welfare and progress. Rapid technology advancements are also being exploited as an effective technique of committing "cybercrime" crimes [1].

In addition to initiating "cybercrime" offenses, the use of information technology has a high potential for crimes involving the management of personal data, which necessitates data protection [2]. Crimes against the management of personal data, such as violations of the right to privacy, are becoming more common as technology improvements make privacy barriers thinner, allowing diverse personal data to be more easily distributed [3][4].

Violations of privacy rights are growing not only in the offline realm but also in the online realm in the form of data leakage; abuse of power over personal data (abusive of power)[5]; data theft by means of (skimming); and data theft by malware (hacking) or system software. Data from ELSAN (Institute for Community Studies and Advocacy) from 2013 to 2017 relate to cases of violation of privacy rights, 5 cases (15%) of personal data leaks; 13 cases (37%) of abuse of power over personal data; 6 cases (18%) of theft through (skimming) and 10 cases (30%) of data theft with system malware [3].

In Indonesia, there will be incidents of personal data leakage until 2020. For example, nineteen million user data and over seven million Tikopia vendor data were purchased on the dark web site; (2) an organization of hackers Shiny Hunters claims to have sold 1.2 million

ICOSTELM 2022, November 04-05, Bandar Lampung, Indonesia

DOI 10.4108/eai.4-11-2022.2329675

Bhinneka.com client records; (3) millions of demographic information belonging to Indonesian citizens, allegedly obtained through a hacker community forum and claimed to be DPT data for the 2014 election; and (4) dubious data, allegedly leaked and freely sold on the internet in August 2020 [6][7]. Another personal data leak occurred in May 2021, with the BPJS Kesehatan data leak. This problem was discovered after an account called Kotz promoted himself as both a purchaser and a vendor of personal data (reseller) on Raid Forums [8].

Personal data spilling is currently a major concern in Indonesia. One of the reasons that personal data spilling is difficult to manage is that Indonesia now lacks laws and regulations that particularly regulate safeguarding private information. Privacy-related legal protections are still limited and sectoral, making it impossible to guarantee optimal and effective personal data protection as part of the right to privacy. As technology advances, the need for a law to protect the privacy and personal data becomes more pressing, requiring the Indonesian government to protect the public and regulate the issue of protecting privacy rights, particularly for personal data, and to prepare various forms of legal protection, one of which is the establishment of a draft law. The Personal Data Protection Act.

2 Research Methods

This study employs secondary data sources such as laws and regulations, judicial decisions, legal theory, and the opinions of various legal scholars [9]. This study also employs a comparative method to analysis, comparing countries in terms of legislative regulations against personal data leakage between Indonesia and other countries such as Singapore, Malaysia, Hong Kong, and the United Kingdom. The data was analyzed utilizing qualitative data analysis techniques [10]. The data was analyzed qualitatively using a study of the logic of deductive reasoning. [10][11].

3 Results and Discussion

3.1 Legal Policy Against Leaking of Personal Data in Indonesia

Current Legal Provisions for Protection of Privacy Rights and Personal Data

The most fundamental protection of privacy rights in Indonesia is outlined in Article 28 G paragraph (1) of the Republic of Indonesian Constitution of 1945, which states:

> *"Each has the right to defend himself, his family, his honor, respect, and property under his control, as well as the right to the feeling of security and protection from the threat of fear of doing or not doing anything that is a human right."*

This article emphasizes the importance of establishing laws and regulations to protect personal data. The Human Rights Law No. 39 of 1999 expressly controls the freedom of speech and access to private data, as well as privacy guarantees. For this violation of personal data, criminal sanctions are imposed as referred to in Article 95A, which reads:

> *"Anyone who does not have the right to disseminate This Data as defined in Article 79 paragraph (3) and private information shall face a maximum imprisonment of 2 (two) years and/or a maximum fine of a price of R 25,000. 0000.00 (twenty-five million rupiahs)".*

The criminal regulations in Article 95A, according to Articles 79 and 86, only apply to local officials and personnel of implementing organizations, as defined in the two Articles. Criminal penalties are not imposed on all violations and are only limited to what is specified in the statute.

Modifications to Information and Electronic Transactions Law No. 11 of 2008 (Law No. 19 of 2016). Article 26 states that one of a person's rights is the protection of his confidential information. This article additionally contends that the use of private information through electronic media must be done with the permission of the individual, and that damage caused by the misuse of personal data can be resolved with non-litigation channels such as deliberation, or through litigation such as lawsuits in court to seek compensation.

The protection of privacy rights, particularly personal data, is governed by Government Regulation No. 71 of 2019 about the Implementation of Electronic Systems and Transactions, which states in Article 14 that when analyzing private information, electronic system operators must adhere to personal data protection principles. Personal data processing includes the following activities: acquisition and collection, processing and analysis, storing, repairing, and updating; collection, declaration, transfer, dissemination, or disclosure; and deletion or annihilation. All of this is done to achieve the purpose of personal data protection by also requiring the consent of the person who owns the identifiable information in question.

Personal data violations, particularly breaches of Article 14, may result in administrative consequences under Article 100 paragraph (2);

> *" Regulatory punishments, as defined in paragraph (1), may take the following forms: written alerts, administrative penalties, temporary being suspended, connection termination, and/or deletion from the list of users."*

Personal information privacy rights are also protected under the Rules of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016, especially Article 36. The provisions in Minister of Communication and Information Regulation No. 20 of 2016 are similar to civil penalties as stated in Article 100 paragraph (2) and paragraph (4) Protection of privacy rights, particularly personal data, as regulated in Government Regulation No. 71 of 2019 regarding Although it Operations and Digital Transactions.

Ordinance No. 20 of 2016 of the Minister of Communication and Information of the Republic of Indonesia on the Protection of Private Data in Electronic Systems is a law regulation that governs data management in Indonesia. The Ministerial Regulation does not specifically control standardization rules that delegate authority to other nations, such as Malaysia and the United Kingdom, which demand standardized equality with data-requesting countries.

Legal Policy Against Personal Data Leakage

The policy of preventing the leakage of personal data is the prevention of crime through a penal policy [11]. The operationalization is through policy formulation, namely the stage of formulating criminal law by executive and legislative legislators in formulating policies which are the formulation or legislation stage.

> *"Under State Regulation No. 71 of 2019, removal is separated into two distinct categories, namely deletion (right to erasure) and removal from indexing lists (right to delisting), and it is carried out based on court judgments on digital information and/or online documents."*

To begin, the policy of deleting irrelevant information on computers and/or digital files is a policy about another individual's personal data or documents obtained against the permission of the private information owner or whose authorization to use of the private data by the owner has been withdrawn. When the use of personal data breaches the law, the data acquisition violates the agreement or the provisions of the legislation, the display causes loss, and the utilization of personal data exceeds the agreed-upon time limit. This deletion policy cannot be applied if statutes or regulations prohibit the deletion of such electronic information and/or documents.

Second, the policy of removing search engines from the list (right to delisting). The policy of deleting information by removing it from the search engine (right to delisting) is based on a request from the proprietor of the personal data to the court, and if the request is granted, The organizer of the electronic system that controls private data is obligated to remove obsolete technological data and/or digital files.

Any use of identifiable information in electronic form must first obtain authorization from the data owner concerned, according to the Personal Data Protection Policy of Electronic System Operators. Someone who breaches this provision may be held liable for their losses. Personal information is an important corporate asset. Personal data is part of a person's personal rights, according to Article 26 of the ITE Law, as well as Articles 30 and 32 of the ITE Law. contained in Articles 46 and 48 of the ITE Law.

Protection against leakage of private data has been regulated in numerous existing rules in Indonesia, according to the description of the policies that are currently in effect. But these rules have not proven effective in preventing leakage in Indonesia. Because victims can only solve problems through deliberation and lack adequate further protection for their personal data, it is still necessary to update criminal law against data leakage to provide a feeling of safety and ease to the community, as well as provide protection for victims and strict sanctions to perpetrators and related companies.

3.2 Criminal Law Policy Against Leaking of Personal Data in Indonesia in the Future

The Privacy Protection Bill's Criminal Statute Policy Against Personal Data Leakage is a comprehensive statute that governs personal data [12]. The country currently has Minister of Information and Communications Regulation No. 20 of 2016, which governs the Security of Personal Data in Technology Devices, but it differs from the Personal Data Protection Bill, which governs more details about personal data, such as types of private data, sending personal data to Indonesian or overseas jurisdictions, controllers, processors, or personal data protection officers, and vi. is located in Indonesia. Criminal law reform is required since it affects various crucial areas [13][14].

Everyone's privacy is viewed as the embodiment of Pancasila's second precept, namely a Just and Civilized Humanity, in the study of philosophy in Indonesia. Personal privacy is likewise governed under Article 28G paragraph (1) of the Republic of Indonesia's 1945 Constitution. Article 32 of Human Rights Law Number 39 of 1999 guarantees independence and secrecy in communication relationships and electronic methods. Currently, Indonesia does not clearly and thoroughly regulate the leakage of sensitive information that occurs. This, of course, contradicts the state values enshrined in Pancasila and the 1945 Constitution. And it contradicts what is stated in the 1945 Constitution. Personal data protection requires more attention right now because it affects so many people in Indonesia.

From a legal standpoint, various regulations in Indonesia discuss personal data, although these policies have not directly addressed personal data. Permenkominfo No. 20 of 2016

respecting private information in Electronic Systems is the closest regulation to the current Privacy Bill. The Minister of Communication and Informatics has not created specific criminal provisions relating to data leakage, and victims of personal data leakage can only be protected through consideration based on the provisions in Article 29. This protection is unquestionably insufficient for offering a sense of privacy and safety for the people whose data is being collected; thus, the provisions of the Personal Data Bill specifically regulate dispute resolution based on Article 56, which states that argue resolution can be carried out by conciliation, court, or alternative dispute resolution institutions. The Personal Data Bill also governs victim protection, with criminals facing criminal penalties and authorities and organizations facing penalties ranging from fines to operational termination to criminal sanctions.

Other regulations can be found in Law No. 23 of 2006. Based on Article 95A, Law No. 24 of 2013 concerning the management of populations only imposes criminal sanctions against personnel involved in population administration. This is not the same as the Personal Data Protection Bill, which governs individual and institutional sanctions. Law No. 19 of 2016 concerning Information and Electronic Transactions also regulates personal data, with Article 26 explaining that if our personal data is used without the permission of the data proprietor, we can file a civil lawsuit, and Articles 30 and 32 explaining electronic system leakage/hacking. The current Personal Data Bill regulates the perpetrators and the settlement of personal data leaks in more detail. The settlement can be carried out in various ways, such as arbitration, criminal and civil courts, and other alternative institutions, with the existence of the Draft Protection Act. This Personal Data will certainly lead to more varied dispute resolution in several ways. In this case, data leakage or theft is not only carried out in electronic or computer systems but can also ensnare perpetrators who leak data offline. This is not regulated in the Law on Information and Electronic Transactions (UU ITE) provisions.

Article 100 of State Regulation No. 71 of 2019 Concerning the Execution of Electronic Systems and Transactions governs the establishment of an electronic system as well as legal penalties. The Personal Data Bill (RUU PDP) differs in that it regulates more details concerning private data controllers, personal data processors, and personal data controllers that were previously unregulated under the PP PSTE. Provisions regarding sanctions against violators in PP PSTE are also only subject to executive penalties in the form of written warnings, administrative fines, temporary suspension, restoration of availability, and expulsion from the list, which differs from the Draft Law, which specifically regulates violators in electronic systems who can face up to 0 criminal sanctions.

Sociological Studies

Data leaks that occur in Indonesia at this time bring a lot of harm to the community, where the leaked data can be used for various kinds of cybercrimes or cybercrime, one of which is falsification of data used by various kinds of crimes and also carding where the stolen personal data is used to drain the account balance. This crime is very dangerous to the community, so this crime regarding the leakage of personal information needs to be protected to provide a sense of security and comfort to the community [15].

Articles such as Articles 47 and 49 regulate the transfer of personal data into Indonesia or abroad. Then Articles 51 to 54 regulate prohibitions and articles 61 to 64 regulate criminal sanctions

Based on Articles 66 to 69, criminal acts committed by corporations are subject to a fine with a maximum fine of 3 times the fine that is threatened and can also be given additional

penalties. Based on Article 67 paragraph 4, if the assets are not possible to be implemented or are not sufficient, it can be replaced with a maximum imprisonment per the threatened criminal provisions. Another provision is regulated in Article 68 paragraph 1 which refers to Article 67 paragraph 4, that if the assets are not sufficient to pay the criminal fine, the corporation may be subject to a substitute penalty, namely the suspension of part or all of the corporate business activities for a maximum period of 5 (five) years determined by the judge in court.

Future criminal law reform plans can be carried out by ratifying the execution of the Personal Data Protection Bill as harmonic and synergistic legislation respecting personal data protection. Legal mechanisms play an important role in protecting the public, commercial sector, and government from data theft and other types of cybercrime. To improve the protection of personal data, the Ministry of Communication and Information (Kemkominfo) has produced a Privacy Protection Bill. However, the Bill is still being debated in the DPR.

> *"The Private Data Protection Bill is a legal instrument that must be present in the legal system of Indonesia. The key difficulties that the bill governing personal data would solve are as follows: (a) in response to the need for comprehensive law to protect confidentiality as part of human freedoms; this safeguarding of personal data Bill will build a more robust and comprehensive regulatory framework for preserving human rights, particularly those pertaining to information about oneself; (b)The Personal Data Protection Bill will create a balance in the governance of sensitive information analyzing and ensure that user rights are respected, as well as provide legal principles and conditions in the processing of personal data that those in charge of personal data have to agree with; (c) prevention and treatment of sensitive information breaches; The Personal Data Protection Bill will become a crucial legal instrument in the prevention and managing of personal data breaches, which continue to occur and have become a common challenge; (d) Creating an ecosystem for the digital economy. By providing legal certainty for businesses and enhancing consumer confidence, the Personal Data Protection Bill will speed the development of a safe digital economy ecosystem and improve the investment climate; (e) International equity in Personal Data Protection legislation. The Personal Data Protection Bill will achieve equity in global privacy laws through abroad data flow regulation, thereby enabling the growth of the digital economy."*

Legal Policies on the Leakage of Personal Data in Some Countries

The Data Protection Act 2018, the UK's data security law, prohibits the activity of transferring personal data to countries outside the EU unless the recipient nation can provide the same data protection guarantee, and all activities involving personal data are overseen by an institution known as The Data Protection Commissioner. In comparison to the United Kingdom, Indonesia is still a long way behind in its attempts to secure identifiable information through the passage of legislation. Indonesia protects personal data through various regulations and rules, but there is no provision that mentions data transfer to countries outside of Indonesia's jurisdiction, and Indonesia also lacks a Board of Commissioners, which is the supervisor of the application of The Data Protection Act, as was done in the UK, despite the fact that the existence of This agency is critical as the party authorized to supervise personal data or information for various purposes.

1. HONGKONG

Personal data are governed in Hong Kong by the Personal Data Privacy Ordinance of 1995 (PDPO). Hong Kong also has a regulatory body, the Privacy Commissioner for Private Data (PCPD). The regulations in Hong Kong's PDPO, for example, control the principle of personal data protection, the prohibition of transmitting data abroad, and bans on the disclosure of a person's confidential information, as well as criminal sanctions, which are identical to and regulated in the Privacy Bill. They are from Indonesia and will be dating.

2. MALAYSIA
   Malaysia's Personal Data Protection Act, also known as the Personal Data Protection Act 2010 (PDPA 2010), establishes seven privacy-preserving principles that Malaysia's personal data protection must adhere to in order for data users to feel comfortable and their personal data to be protected. Personal data violations under the Privacy Protection Principles/PDPA 2010 will result in a minimum punishment of three million ringgit or two years in prison. In contrast to Indonesia, which primarily governs administrative sanctions.

3. SINGAPORE
   The provisions of the Personal Data Protection Bill are similar to or consistent with the provisions in Singapore's Personal Data Protection Act (PDPA). Article 26 of the Personal Data Protection Act (PDPA) governs the restriction of data transmission abroad or outside of Singapore's jurisdiction. Article 49 of the Personal Data Protection Act states the same thing. Similarly, under Personal Data Protection Act Article 48D. Article 61 paragraph 3 of the Personal Data Protection Bill is analogous to PDPA. Article 48E of the Personal Data Protection Act (PDPA) relates to Personal Data Protection Bill Article 61 paragraph 3, while Article 51 paragraph 5 corresponds to Human Data Security Bill Article 16 paragraph 1. Indonesia accepted regulations from as well as the GDPR, or General Data Protection Regulation, of the EU, which the nation of Singapore also embraced.

The Personal Data Protection Amendment is required in society as a criminal law reform legislation that can increase data security. Based on the provisions of the 1945 Constitution and Pancasila, the Personal Data Bill seeks good and equitable policies. Victims can be protected in a variety of methods, including arbitration, civil and criminal courts, and alternative organizations that were previously unregulated by existing legislation. Individuals, agencies, and businesses who commit crimes may face punishments ranging from criminal penalties, fines, and activity suspension to other penalties. The Personal Data Protection Bill is also an attempt at international equity in personal data protection. Many governments restrict personal data transfers to countries that regulate or explicitly protect the privacy of private information.

4 Conclusion

Indonesia's legal protection measures for privacy rights in private information leaks are currently distributed among several statutes and guidelines, making optimal and effective data-related protection as part of transparency liberties unachievable. This legal protection plan currently takes the form of preventing confidential information leakage, preventing

personal data theft, a personal data misuse policy, and system operators protecting personal data.

Future criminal law policies against personal data leakage in Indonesia include ratifying the implementation of the Act on the Protection of personally identifiable information as harmonious and synergistic legislation regarding Personal Data Protection; the establishment of a separate entity authorized; and the development of personal data and information management through the Indonesian Data Protection System (IDPS) as a Digital Surveillance and Data Safety Efficiency. These three items are the State's duty and responsibility in ensuring human rights, specifically the right to privacy, as well as to protection, particularly in information and communication technology activities, to reduce various infractions in the practice of data privacy Protection.

The Draft Criminal Law regulates the formulation that regulates (1) the formulation regarding criminal acts, which regulates what actions are prohibited, and (2) the formulation regarding accountability to the perpetrators, which regulates accountability to the perpetrators, both individuals and corporations or agencies, in the Personal Data Safety Bill. (3) Punishment formulation in which forbidden conduct by people, corporations, or agencies may be liable to criminal sanctions.

References

[1] Koto, I.: Cyber Crime According to the ITE Law. International Journal Reglement & Society (IJRS). 2, 103–110 (2021)

[2] Situmeang, S.M.T.: Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. SASI. 27, 38–52 (2021)

[3] Rumlus, M.H., Hartadi, H.: Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. Jurnal HAM. 11, 285–299 (2020)

[4] Brown, R.: Rethinking Privacy: Exclusivity, Private Relation and Tort Law. Alta. L. Rev. 43, 589 (2005)

[5] Guelke, J., Sorell, T.: Violations of privacy and law: the case of stalking. Law, Ethics and Philosophy. 4, (2016)

[6] Stephanie, C.: 7 Kasus Kebocoran Data yang Terjadi Sepanjang 2020 Halaman all, https://tekno.kompas.com/read/2021/01/01/14260027/7-kasus-kebocoran-data-yang-terjadi-sepanjang-2020

[7] Indonesia, C.N.N.: Deretan Peristiwa Kebocoran Data Warga RI Sejak Awal 2020, https://www.cnnindonesia.com/teknologi/20200623160834-185-516532/deretan-peristiwa-kebocoran-data-warga-ri-sejak-awal-2020

[8] Widayati, L.S.: Kebocoran Data Pribadi dan Urgensi Pembentukan UU Perlindungan Data Pribadi. Isu Sepekan Bidang Hukum. Pusat Penelitian Badan KeahlianSekretariat Jenderal DPR RI. (2021)

[9] Sumgong, B.: Legal Research Methodology. Raja Grafindo, Jakarta (2015)

[10] Suteki, Taufani, G.: Metodologi Penelitian Hukum: Filsafat, Teori dan Praktik. Rajawali Pers, Jakarta (2020)

[11] Amiruddin, Asikin, Z.: Pengantar Metode Penelitian Hukum. Rajawali Pers, Jakarta (2018)

[12] Butarbutar, R.: Initiating new regulations on personal data protection: Challenges for personal data protection in indonesia. Presented at the (2020)

[13] Fatmawatia, N., Effendib, T., Ulfac, A.: The Urgency of Personal Data Protection Laws in Indonesia.

[14] Sujadmiko, B., Meutia, I.F., Kurniawan, D., Mardenitami, A.N.: The urgency of digital right management on personal data protection. International Journal of Research in Business and Social Science (2147-4478). 10, 253–258 (2021)

[15] Aswandi, R., Muchin, P.R.N., Sultan, M.: Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (Idps). Jurnal Legislatif. 167–190 (2020)