Misuse of Personal Data as a Crime from a Cyber Law Perspective

I Gusti Bagus Yudas Swastika[1], Anak Agung Ayu Ngurah Sri Rahayu Gorda[2], AAA. Ngr. Tini Rusmini Gorda[3], I Gede Agus Kurniawan[4]
gusyudha0@gmail.com

[1,2,3,4] Universitas Pendidikan Nasional

Article Info
Received: 2023-05-22
Revised: 2023-06-29
Accepted: 2023-06-29

Keywords:
Legal Liability; Personal Data; Cyber Law..

Abstract
The purpose of this research report is to establish legal protection rules for the use of personal data to ensure legal certainty for the community and the role of law enforcement in preventing future crimes related to misuse of personal data. on personal criminal law the right to reform. The research method uses normative legal research. Opinion of these comments, to guarantee legal certainty, it is necessary to stipulate a special Perpu that establishes and harmonizes the protection of personal data in a detailed, clear, systematic and comprehensive manner, in order to create a coordinating mechanism. law enforcement agency. In this context, the researcher proposes to make rules governing the application of criminal sanctions with a warning effect, as well as restructuring and drafting rules related to current regulations in the field of personal data.

I. Introduction

Advances in information technology in the IT field can be felt in various activities. Since the SARS-CoV2 pandemic, with the increase in the use of electronic copies and internet networks, personal data protection has become increasingly important in the digital world, so that most people have internet access to work from home in carrying out their activities (Sahat, 2021). The benefits of technology and statistics can be seen in areas such as education and economics. The ability to process large amounts of data quickly and efficiently and with fewer errors makes it easier to solve technical and other development-related problems. Where IT progress not only brings benefits, but also causes dilemmas that are detrimental to

citizens, such as illegal use of information, identity theft, and human trafficking.

Business owners or electronic system operators may collect personal information from customers or potential customers offline or online, in which case digital information may be exchanged or misused. It can be stolen (for purposes other than sharing or transmitting digital personal data) without the knowledge and consent of the data controller and can be stolen from third parties. The research which raises the issue of personal data protection in Indonesia says that (Glenn, 2020): If there is misuse of personal data, it can be seen that there is an error in the system, there is no supervision, so that personal data can be misused and harm the data owner. Misuse, theft, sale of personal data are violations of IT law and can be classified as human rights violations, because personal data is part of human rights that must be protected.

Misappropriation of personal data is an act that is characteristic of crimes such as embezzlement and fraud, as well as other crimes, both objectively and subjectively. By implementing these elements, administrative, civil and criminal sanctions will not be sufficient to determine the crime of misuse of personal data which is a comprehensive form of crime. According to research on banking victim crimes from a legal and victimological perspective (Indra, 2019) that: A criminal act is an act of someone who violates or contradicts what is stipulated in the rule of law, or violates the prohibition of the rule of law, is illegal or unconstitutional. regulation. founded in a rule of law. law, law. applicable law in the region where the applicant resides.

Several previous studies that refer to the title or approach and raise questions to support this work include: (1) Mohammad Ramabayu Sutan Hassanudin Yussuf, University of 17 August 1945 Surabaya in 2019 with the title: Legal Protection of Personal Data Users of Financial Technology Fund Loan Applications. (2) Masitoh Indriyani, Nilam Andaria Kusuma Sari, Satria Unggul W.P., Airlangga University

in 2017 with the title: Protection of Privacy and Personal Data of Online Consumers in the Online Marketplace System and (3) A.A. Ngurah Deddy Hendra Kesuma, I Nyoman Putu Budiartha & Putu Ayu Sriasih Wesna, Warmadewa University in 2021 with the title: Legal Protection of Financial Technology Consumer Personal Data Security in Electronic Transactions.The main difference between this article and the three articles above is that the first study looks at the legal consequences of misusing consumer personal data in fintech-based loan applications, and the second is about regulation. Protection of internet user privacy in the marketplace system. The third study concerns the legal protection of personal data of fintech users and legal channels that can be used by fintech users in the event of misuse of personal data by providers. This article examines legal protection against misuse of personal data and the role of law enforcement in preventing crimes involving the use of personal data.

II.Research Method

The research method used in this paper is the normative juridical method or normative legal research. This research uses secondary data consisting of primary legal materials and secondary legal materials. Primary legal material consists of norms, laws and regulations related to the problem under study, while secondary legal material refers to literature reviews from previous research (Rizki and Andika, 2020). Where this research is categorized as doctrinal legal research. Information from various aspects of the issues discussed using various approaches, such as conceptual, constitutional and comparative approaches. Data was collected through a literature study, then analyzed descriptively-qualitatively.

III. Results and Discussion

a. Providing legal protection against misuse of personal data is a perfect form of crime to provide legal certainty to the public

The rapid advancement of technology in the millennial era, especially buying and selling online, is inevitable from problems, especially regarding the protection of personal data (Dewi, 2016). Misuse of personal data can be misused due to negligence of the recipient (company) in daily activities. For example, by buying a starter pack and then asking the meter to register, downloading an app, adding personal data to platforms or forms, the meter can be abused and tampered with. In addition, due to the rapid development of science and technology, the most popular technology today is related to big data. Big data is considered as an important data processing solution because it can process large and varied data and make simple applications such as the use of big data not only by the government but also by private companies. Large companies use this as an attempt to understand customer characteristics such as loyalty, visit factor, purchase history, etc. to help them buy a product or service. On the other hand, it cannot be denied that the misuse of big data threatens privacy. For example, confusion when having to register personal data such as identity cards (KTP) or family cards (KK). Another example is the history of online motorcycle taxi applications which have the potential to leak and lose data. Based on the results of research conducted (Rosalinda, 2014) states that: The government and non-governmental organizations as well as law enforcement and the public must maintain high integrity in order to obtain benefits, justice and legal certainty from data protection. Each country has different personal data requirements such as the United States, Canada and Australia use the term personal information, while countries in the European Union and Indonesia use personal data.Furthermore, the need to protect personal data can be considered as part of human rights regulated in law in article 12 no. 39 of 1999

where everyone has the right to protection for personal development in educating and improving the quality of life, being responsible, happy and prosperous in accordance with human rights (Day, 2021). When a crime occurs or a crime is reported, the reporter immediately conducts an investigation to find out the extent of the incident. Notifications can be made in writing, signed by the complainant, or can be given orally (Purnomo, 2020). Therefore, in case of irregularities, the two Indonesian citizens will be tried according to Indonesian law and subject to courts of Indonesian law.Protection of personal data, particularly regarding the use of personal data information through electronic media is regulated through article 26 of amendments to the ITE Law, which regulates the use of personal data by other parties must be subject to the approval of the owner of the personal data (Ni ketut et al., 2019). Therefore the Personal Data Protection Bill must be passed immediately, bearing in mind that many other countries have regulated the protection of personal data. As a comparison, in the UK the protection of a person's identity was regulated in 2000 through the Data Protection Act 1998, the implementing body is called the data protection commissioner which has the duty to pay attention to all people who use data who manage personal data. Based on Article 14 of the Data Protection Act 1998, it is explained that if the court finds that the personal data processed by the data controller is inaccurate, the court can order the correction, obstruction, deletion or damage of the data. Those who are directly affected by the processing of personal data can ask the Board of Commissioners to evaluate the process to determine if it complies with the provisions of the Data Protection Act 1998 (Sautunnida, 2018).There are internationally recognized privacy and personal data principles. These principles are the foundation for modern national data protection laws. One of the international instruments that protect privacy and personal data was issued by the Organization for Economic Co-operation and Development (OECD). In addition, the Council of Europe (CoE) adopted the European Convention for the Protection of Human Rights (ECHR) in 1950 (Dewi et al., 2018).

So far, there is no policy or regulation in Indonesia that specifically regulates the protection of personal data, where various laws and regulations have been regulated separately, so that a law is needed that regulates comprehensively regarding the misuse of personal data. Various laws and regulations now apply to the protection of personal data, including: Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning ITE; and Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operators; Given the regulation and protection of personal data in various countries, it is only natural that the Indonesian state compares and analyzes in detail the provisions for combating data misuse, which is the most appropriate form of crime from a cyber law perspective. This means that it is not enough just to examine the interaction of the parts in the legal system.Article 28 of the 1945 Constitution states: "Every person has the right to protection for himself, his family, honor, dignity and property, has the right to protection from fear and danger, to a sense of security". Meanwhile, Articles 26, 30 to 33, 35 of the ITE Law have been regulated. Where in article 26 of the ITE Law it is stated that the use of personal data in electronic form must be based on the consent of the data subject, and losses caused by misuse of personal data can be recovered unlawfully through negotiations, or settlement of cases with demands for compensation. As mentioned above where the provisions of Article 26 (2) of the ITE Law, criminal provisions have not been regulated, so it is necessary to formulate norms by adding criminal sanctions, so as to provide a deterrent effect even though the criminal sanctions are as a last resort (ultimum remediuArticle 26 of the Electronic Information and Transaction Law states that one of the rights of individuals is the protection of their personal information. Collecting information in accordance with government systems and regulations no. 82 of 2012 concerning Electronic Services; The care remains real and human life is protected.The ITE Law has regulated data protection including wiretapping, where wiretapping is an act that may not be carried out, not belonging to groups that have the right to do so in the context of legal action. When

viewed from the explanation of Article 26 of the ITE Law, there are weaknesses, namely the absence of legal protection for the owner of the data used by the organizers or service providers with the aim of making a profit. The Law on Information and Electronic Transactions only mentions the subject of personal data protection (general provisions) without following up on the implementation of said protection. These weaknesses are things that must be corrected for the realization of legal objectives, namely maintenance and assurance of order (certainty) and order, therefore it is necessary to reformulate existing legal norms. Through the provisions of Article 28J paragraph (2) of the 1945 Constitution and the Supreme Court Decision through decision No. 6/PUU-VIII/2010 and Number 006/PUU-I/2003 which stated their views regarding the protection of privacy that must be protected by the state. However, in terms of legal interests, these rights can be reduced as long as it is through a mechanism regulated in the law.

In Article 1 point 28 of Law no. 10 of 1998 concerning Banking explained that bank secrecy is everything with information about depositors and their deposits. Based on Article 40 of Law no. 10 of 1998 concerning Banking explains that information regarding depositors and their savings must be kept confidential by the Bank, except in the circumstances referred to in Article 41, Article 41A, Article 42, Article 43, Article 44, and Article 44 A. The exceptions referred to are tax purposes , settlement of bank receivables, trials in criminal cases, as well as based on request, approval or power of attorney from depositors, with certain procedures. In principle, bank secrecy is an asset of trust in the community, so that the community has an assessment for the bank about the ability to maintain the confidentiality of its customers, so that the community will feel safe to keep their funds in the bank (Marnia, 2014). In Article 22 of Law no. 36 of 1999 concerning Telecommunications stated that everyone is prohibited from carrying out actions without rights, illegal or manipulating: (a) accessing telecommunications networks; and/or (b) provide access to telecommunication services; and/or (c) provide access to special telecommunication networks.Furthermore, in point III. E.9 Bank

Indonesia Circular Letter No. 18/22/DKSP dated 27 September 2016 concerning the Implementation of Digital Financial Services regulates the implementation of digital financial services (LKD) for Banks and Non-Banks, a cooperation agreement between digital financial service providers and agents stating that all data obtained from digital financial institution agents must be kept confidential by the organizers of the digital financial institution. The word ownership in this provision results in an interpretation of the transfer of ownership from personal data holders to digital financial institution administrators. This becomes a legal issue because personal data should belong to the owner of the personal data, then point V.F.2 SEBI 18/22 regulates data confidentiality, so the registration form must have a statement regarding submission of personal data which may only be used for registration purposes by digital financial institution operators. only the agent of the digital financial institution and the approval of the prospective holder can disclose the identity to the organizer of the digital financial institution. These provisions can be used on the grounds that the notification has been fulfilled without requiring further action (Setyawati, 2018). Therefore, it is necessary to reformulate these regulations against legal norms, so that what is aspired to regarding legal objectives can be achieved.At present Indonesia also has a Personal Data Protection Bill, with the aim of combining privacy regulations on scattered personal data into a separate law with the aim of providing boundaries between rights and obligations regarding the acquisition and use of personal data. Article 29 of the Draft Law on Personal Data Protection states that (1) every owner of personal data and the operation of an electronic system can submit a complaint to the Minister regarding the failure to protect the confidentiality of personal data. (2) the complaint referred to in paragraph (1) is intended as an effort to resolve disputes through deliberation or through other alternative settlement efforts. (3) The minister can coordinate with the head of the supervisory agency and sector regulator to follow up on the complaints as referred to in paragraph (1). Furthermore, Article 30 states that (1) The Minister delegates the authority to resolve personal data disputes as referred

to in Article 29 to the Director General. (2) The Director General may form a personal data dispute resolution panel. Pursuant to Article 32 which states that (1) in an effort to resolve disputes through deliberation or through other alternative settlement efforts that have not been able to resolve disputes over failures to protect the confidentiality of personal data, each owner of personal data and the operation of an electronic system can file a lawsuit over a failure to protect confidential personal data . (2) the lawsuit referred to in paragraph (1) is only in the form of a civil lawsuit and is filed in accordance with the provisions of the laws and regulations. From the provisions contained in the Draft Law on Personal Data Protection, the researcher believes that it is necessary to reformulate the legal norms contained in the articles, because the provisions regulated in the Draft Law on Personal Data Protection are seen as too bureaucratic. and the process to obtain legal certainty will be very long, convoluted and uncertai. In Indonesia, legal protection for personal data is still considered not optimal, this can be seen from the fact that there is still a lot of misuse of personal data without the knowledge of the owner due to the lack of strict security and supervision from data users.Regarding legal protection, the use of personal data is inseparable from the obstacles that will be faced, for example, difficulties in tracking down the main perpetrators and proving them, difficulties in handling them, etc. Boelewoekli is of the view that the direct involvement of the government and laws in personal data issues is something that is needed, especially in resolving disputes that arise in the field of telematics (Mega and Endang, 2017).Until now, there is no comprehensive specific law that regulates the protection of personal data, in the sense that these regulations are not scattered or regulated in several provisions or regulations as currently exist. Currently, if a case occurs, the legal arrangements will only refer to the law governing the misuse of personal data and several other laws and regulations, but generally what is always referred to is the ITE Law. The absence of a clear form of legal certainty regarding the misuse of personal data will result in financial security which impacts the welfare of the community (Rudi, 2019).Based

on the description above, the protection of personal data is a shared responsibility, both the community, both individuals and legal entities and the government. Because it is impossible to rely only on the prudential attitude of the people, but there must be a role for the government in making legal policies with the aim of providing protection to the community. These efforts can be through preventive efforts and repressive efforts. Preventive efforts, for example, are careful in providing personal data and monitoring efforts. There are two parties that are able and have the opportunity to carry out mass surveillance, namely the private sector and the government. Private parties can come from online content and service providers, internet service providers or internet infrastructure owners (Muhammad, 2019). This is because currently regulations related to personal data in general are still partial and sectoral.Protection of privacy data as part of respecting the right to privacy must begin by providing legal certainty. Therefore, guarantees for the protection of privacy data must be placed in a legal instrument that has the highest power, namely the constitution, because the Constitution or the Constitution is the highest legal instrument in a country. Legal certainty (legality principle) is necessary and cannot be ruled out in the context of law enforcement by every country. The state's step in providing legal certainty is to stipulate and guarantee these rights in the constitution, then through this instrument the character of a country can be seen about what matters are put forward, what legal system is used and how the government is regulated (Natamiharja, 2019), thus, it is time for the Indonesian state to have clear regulations on the protection of personal data. Based on this definition, three stages of criminal law enforcement are established: where the legislative power is to decide what can be punished, the judicial power is to apply criminal law and the executive power is to embody criminal law (Na'im, 2019).

IV. Conclusion

Based on the discussion above, it can be concluded that the implementation of

the current privacy policy seems bad. In the concept of personal data protection processing, we expect strict and comprehensive legislation that takes cultural, social, economic and political trends as well as moral, ethical and religious values more than standard. The reviewer hopes that this decision will not hinder the development of technology and information. In this case, the authorities and service providers must implement clear and lawful authentication mechanisms and take precautions or protect the confidentiality of all data. Governments should work hard to prevent data crimes, by harmonizing laws and regulations so that laws do not conflict with other laws, strengthening law enforcement capacity, and encouraging cooperation and mutual enforcement in accordance with international law. On the basis of the foregoing, the Petitioners are trying to develop laws and regulations that regulate the use of criminal sanctions as a deterrent.

Reference

Anggraeni, Setyawati Fitri. "Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia." *Jurnal Hukum & Pembangunan* 48, no. 4 (2018): 814–25. https://doi.org/10.21143/jhp.vol48.no4.1804.

Aprilia, Mega Lois, and Endang Prasetyawati. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Pengguna Gojek" 1, no. 2 (2017): 90–105. https://doi.org/10.30996/mk.v0i0.2202.

Budi Pramono, DRS. *Peradilan Militer Indonesia*. Bandung: Scopindo Media Pustaka, 2020.

Dewi, Sinta. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia Jurnal Hukum* 5, no. 1 (2016): 35–53. https://doi.org/10.20961/yustisia.v5i1.8712.

Dharmawan, Ni Ketut Supasti, Desak Putu Dewi Kasih, and Deris Stiawan. "Personal Data Protection and Liability of Internet Service Provider: A Comparative Approach." *International Journal of Electrical and Computer Engineering* 9, no. 4

(2019): 3175. https://doi.org/10.11591/ijece.v9i4.

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99. https://doi.org/10.25072/jwy.v5i2.460.

Herlambang, Indra Trinugraha. "Korban Kejahatan Perbankkan Dalam Perspektif Hukum Dan Viktimologis." *Negara Dan Keadilan* 8, no. 1 (2019). https://doi.org/10.33474/hukum.v8i1.4481.

Katrin, Desy Dwi, Diah Gustiniati, and Rini Fathonah. "Peran Kepolisian Dalam Penegakan Hukum Terhadap Pelaku Tindak Pidana Pembunuhan Berencana." *POENALE: Jurnal Bagian Hukum Pidana* 3, no. 3 (2015): 1–11.

Kurniawati, Husni, and Yunanto. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online." *Jurnal Ius Constituendum* 7, no. 1 (2022): 102–14. https://doi.org/10.26623/jic.v7i1.4290.

Latumahina, Rosalinda Elsina. "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya." *Jurnal GEMA AKTUALITA* 3, no. 2 (2014): 14–25. http://dspace.uphsurabaya.ac.id:8080/xmlui/handle/123456789/92.

Na'im Al Jum'ah, Muhammad. "Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi." *Cyber Security Dan Forensik Digital* 1, no. 2 (2019): 39–44. https://doi.org/10.14421/csecurity.2018.1.2.1370.

Natamiharja, Rudi. "Perlindungan Data Privasi Dalam Konstitusi Negara Anggota ASEAN." In *Hak Konstitusional*, 183–97. Lampung, 2019. http://repository.lppm.unila.ac.id/id/eprint/17440.

Ramadani, Rizki, and Andika Prawira Buana. "The Needed but Unwanted Independent Regulatory Agencies: Questioning Their Legitimacy and Control in Indonesia." In *The 2nd International Conference of Law, Government and Social Justice (ICOLGAS 2020)*, 674–84. Atlantis Press, 2020.

Rani, Marnia. "Perlindungan Otoritas Jasa Keuangan Terhadap Kerahasiaan Dan Keamanan Data Pribadi Nasabah Bank." *Jurnal Selat* 2, no. 1 (2014): 168–81. https://ojs.umrah.ac.id/index.php/selat/article/view/121.

Rosadi, Sinta Dewi, and Garry Gumelar Pratama. "Urgensi Perlindungandata

Privasidalam Era Ekonomi Digital Di Indonesia." *Veritas et Justitia* 4, no. 1 (2018): 88–110. https://doi.org/10.25123/vej.v4i1.2916.

Rosana, Ellya. "Kepatuhan Hukum Sebagai Wujud Kesadaran Hukum Masyarakat." *Jurnal Tapis: Jurnal Teropong Aspirasi Politik Islam* 10, no. 1 (2014): 61–84. https://doi.org/10.24042/tps.v10i1.1600.

Roza, Darmini, and Laurensius Arliman. "Peran Pemerintah Daerah Di Dalam Melindungi Hak Anak Di Indonesia." *Masalah-Masalah Hukum* 47, no. 1 (2018): 10–21. https://doi.org/10.14710/mmh.47.1.2018.10-21.

Sautunnida, Lia. "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia: Studi Perbandingan Hukum Inggris Dan Malaysia." *Kanun Jurnal Ilmu Hukum* 20, no. 2 (2018): 369–84. https://doi.org/10.24815/kanun.v20i2.10661.

Situmeang, Sahat Maruli Tua. "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber." *SASI* 27, no. 1 (2021): 38–52. https://doi.org/https://doi.org/10.47268/sasi.v27i1.394.

Tarigan, Bastanta, Mhd Nuh, and Alwan Alwan. "Peranan POLRI Dalam Pemberantasan Penyalahgunaan Narkotika (Studi Kasus Polsekta Pancurbatu)." *Jurnal Mahupiki* 3, no. 01 (2013). https://jurnal.usu.ac.id/index.php/jmpk/article/view/4189.

Wijaya, Glenn. "Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum." *Law Review* 19, no. 3 (2020): 326–61. https://doi.org/10.19166/lr.v19i3.2510.

Zulfadli, Muhammad, Kasman Abdullah, and Fuad Nur. "Penegakan Hukum Yang Responsif Dan Berkeadilan Sebagai Instrumen Perubahan Sosial Untuk Membentuk Karakter Bangsa." In *Prosiding Seminar Nasional Himpunan Sarjana Ilmu-Ilmu Sosial*, 2:265–84. Makasar: Universitas Negeri Makasar, 2017. https://ojs.unm.ac.id/PSN-HSIS/article/view/2751.