Ethico-Legal Aspects Of Personal Data Protection In Indonesia

Yovita Arie Mangesti[1], Slamet Suhartono[2*], Ahmad Mahyani [3]

[1,2,3] Lecturer at the Faculty of Law, University 17 August 1945 Surabaya, Indonesia
* Corresponding author:
Email: slamet@ untag-sby. ac.id

Abstract.
*Protection of personal data is a manifestation of the state's role in protecting human rights. The use of electronic data on the one hand provides convenience, especially in terms of accessibility of public services, but on the other hand electronic data leakage is a violation of ethics and law. This paper is a normative legal research that examines the ethical aspects of personal data protection in Indonesia with a statutory approach and a conceptual approach. There is an ethical and legal correlation that should be the legal ratio of personal data protection, so that in order to provide legal protection not only through the formation of laws but also the efforts of the information commission agency to educate the public that ethically the misuse of one's personal data for commodities is a non-legal act. ethical behavior that exploits and demeans human dignity, which must be accounted for. Protection of personal data is realized by making crimes against personal data a common offense, and providing public accessibility to obtain advocacy when*personal data is misused in order to achieve the value of justice and legal protection.

Keywords: *ethical, personal data protection*

I. INTRODUCTION

Personal data is data attached to owner, whose confidentiality should be protected because personal data is one of the embodiments of human rights. In the current digital era, this data can be transformed into electronic data. However, the digitization of personal data is still holds the potential loss of privacy, because the shape of digitizing such as e-ID, the collection of personal data in bulk (digital dossier), social media, direct marketing *(direct selling)* and activities cloud computing *(cloud computing),* may accessed *online* by anyone who has digital technology capabilities. The Association of Indonesian Internet Service Providers reported that 92% of respondents stated that they easily entered personal data information in the form of names into applications on the internet, 79% provided information about their place and date of birth, and 65% even provided personal addresses. Mid-2020 there was a leak of 91 million personal data of Tokopedia application users, as well as a leak of 13 million users' personal data *online place* another market-, namely Bukalapak. In addition, there is also the weakness of personal data protection in the health sector during the pandemic, which is suspected to have caused 230,000 data leaks. (two hundred and thirty thousand) data on Corona Virus Disease 2019 (Covid-19) patients in 2020, and data leaks of 279,000,000. (two hundred seven nine million patients

participating in the Social Security Administering Body (BPJS) Health. [1].Normatively, the owner of personal data has the right to keep it confidential.

This right is reflected in the Regulation of the Minister of Health Number 269 of 2008 concerning electronics medical record, (patient) stipulates that the owner of personal data has the right to the confidentiality of his data and has the right to file a complaint in the context of resolving personal data disputes; has the right to get access to obtain historical personal data and has the right to request the destruction of certain personal data belonging to him in the electronic system. The accuracy of personal data protection in electronic systems is not optimal, and is only protected if the electronic system has been certified. Personal data accurately is not understood and not realized by the public. People only know that when they use the electronic system stored on the device electronics gain security. Including when they seek treatment and are recorded in the electronic medical record, then their entire condition is considered safe and confidential. Weak personal data protection actually cannot be separated from the ethical and legal issues that are injured. Indonesian culture which has the characteristics of the community, communal and open, does not mean that a person's data can be opened and used for the benefit of certain parties.

Sinta Dewi's research concludes that legal protection of personal data privacy in the use of cloud computing, which was originally a secure data storage and processing method, however, still requires regulations that protect personal data in national and international contexts. [2]. Hanifan Niffari's research concludes that the protection of personal data is the mandate of Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which until now still requires regulation, given the large number of misuses of personal data that are not in its initial designation, such as being traded. personal data to fulfill commercial aspects. [3] The author in this study uses an ethical perspective to provide an overview of the relationship with ethics and law in terms of personal data protection, as part of fundamental human rights. The adage that law floats in the ocean of ethics is an early illustration of the relationship between ethics which is a source of material law, which has not been positivated, but functions as a guide to life behavior in Indonesian society. The ethical and legal correlation in the protection of personal data is the concern of this study.

II. METHODS

Based on the legal issues above, the type of research above is normative legal research using two approaches, namely: *first,* the statute approach, which is carried out on Law Number 11 of 2016 concerning Regarding Electronic Information and Transactions (UU ITE), Ministerial Regulation Number 20 of 2016 concerning Personal Data Protection (Permen PDP); and *second,* a conceptual approach with an analysis of the ethical aspects of personal data protection, guarantee the private rights

of citizens as constitutional rights; and *third,* a comparative approach by comparing the practices of several countries to data protection.

III. RESULT AND DISCUSSION

1. Personal Data Protection in Indonesia

Personal data is a formal form of personal privacy that is universal and protected as a manifestation of morality. The concept of personal data protection is a form of protection for the rights to be alone, as part of human spiritual needs. Humans who actually live with other people, according to Allan Westin, still need the right to privacy, including to determine whether or not information about them will be communicated to other parties, so the definition put forward by Westin is called information privacy.[3]. The decision of the Constitutional Court No.5/PUU-VIII/2011, also states that the right to privacy is part of human rights (derogable rights), and the scope of the right to privacy includes information or right to information privacy, which is also called data privacy. data protection).

In the ITE Law, PP Number 82 of 2012 concerning Electronic System and Transaction Operators, contains the definition of personal data, namely certain personal data that is stored, maintained, kept true and protected for confidentiality (Article 1 number 27) [4] The development of personal data protection it is not enough, because the development of electronic data is increasingly diverse, not only population data, business transactions, but also data in the field of medical services. There are provisions regarding telemedicine, which is reflected in the Minister of Health Regulation Number 20 of 2019 concerning Telemedicine Services between Health Service Facilities (Fasyankes). However, the Permenkes only regulates between Fasyankes, not doctor services to patients. So that no one should be responsible for securing medical secrets and medical records.[5] Paying attention to these arrangements shows that the protection of personal data in Indonesia is very weak, so it does not guarantee the confidentiality of the owner.

2. Protection of Personal Data in Several Countries

Efforts to protect privacy rights at the international legal level started with the declaration of human rights on 10 December 1048. At the 2013 UN General Assembly, member states agreed on the right to privacy. Member countries are required to ratify and adapt it to the laws in force in their respective countries. IBR Supancana, in one of the events of the National Seminar on Personal Data Protection, stated that many countries have tried to provide personal data protection in positive legal instruments, Australia has set laws and regulations regarding privacy. Australia enacted the Privacy Act in 1988. Singapore enacted the Personal Data Protection Act in 2012. The European Union has the General Data Protection Regulation (GDPR) which was enacted in May 2018. The principles that apply to the EU GDPR are guidelines, with the principle of transparency, that citizens countries have the right to access, change and delete their personal data at certain times from the company's customer data.

Companies should transparently announce the purpose for which they collect data and how it will be used.

The Personal Data in question includes the applicable race, ethnicity, politics, health, gender, and sexuality. The OECD Guidelines 1980 have contained the basic principles in the PDP: collection limitation, data quality, purpose specification and notice, use limitation, data security, openness, data access, accountability. The OEDC was revised in 2013 to focus more on the practical implementation of PDP through a risk management-based approach; there is a need for greater efforts to cover the more global dimensions of PDP through improvements to its system inter-operability. This revision introduces new concepts, such as privacy management program, security breach notification, national privacy strategy, education and awareness, global inter-operability. On the plains of Asia, APEC Privacy Framework 2004: agreed at the APEC Ministers Meeting 2004 to encourage a consistent approach to PDP in Asia Pacific; there are 9 regulated principles; there are several options in the formulation of regulations (legislative, administrative, industry self-regulatory, combination).

APEC Privacy Framework 2015: focus on domestic and international implementation; formulated APEC Privacy Information Principles; there is guidance for domestic and international implementation; developed APEC Cross-Border Privacy Rules CBPR). Stipulated by the ASEAN Telecommunication and Information Technology Ministers Meeting (TELMIN) in Bandar Seri Begawan, Brunei Darussalam.The PDP principles adopted: Consent, notification and purpose; accuracy of personal data; security safeguards; access and correction; transfer to another country or territory; retention; accountability. Activities for its implementation: information sharing and exchange; workshops, seminars or other capacity building activities; joint research in areas of mutual interest. Furthermore, ASEAN Telecommunication and Information Technology Ministers Meeting (the 2018TELMIN) in Bandar Seri Begawan, Brunei Darussalam. The PDP principles adopted include: Consent, notification and purpose; accuracy of personal data; security safeguards; access and correction; transfer to another country or territory; retention; accountability. The implementation is through: information sharing and exchange; workshops, seminars or other capacity building activities; joint research in areas of mutual interest. [6]

3. Ethical Aspects of Personal Data Protection Personal

Data protection is an ethical issue, because it relates to other people, as well as the fundamental human rights that other people have. Article 28 G point (1) of the 1945 Constitution, explicitly states that; "Everyone has the right to personal protection, family, honor, dignity and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something which is a human right." This article shows that the ethical and legal aspects of personal data protection are inseparable. [7]The ethical aspect of law (ethico legal) is very important to understand because ethics serves as a moral standard for the behavior of every human being in his nature as individual and social. Storing, maintaining, safeguarding

data, is an active behavior of everyone, even an ethical obligation for everyone to store, maintain, protect other people's personal data. When this is related to various human needs that are increasingly complex, there can be misuse of personal data as a commodity tool to seek profit for themselves or a group of people. There is a crime that uses personal data to threaten, deceive, use it for research purposes without ethical clearance, or certain political interests.

Positive law is often behind events. The development of technology raises the modus operandi of crime faster than the law. The positive law problem that often arises is the void of norms. For example, the protection of personal data of telemedicine patients, easily accessible to other parties, and used for certain purposes. The occurrence of medication errors is a form of malpractice that is difficult to prove because there is no standardization of products sold online. Transactions other than food and drug products, such as product quality in trading online, need to be improved so as not to harm consumers. In the property sector, the validity of electronic certificates is often questioned because the law has not confirmed which institutions are certified and may issue certificates. Electronic data, has not been protected with certainty with strong binding as a law.

Sanctions that provide legal certainty can be imposed on perpetrators only if they have been regulated. Often cases related to leakage or misuse of personal data are resolved non-litigation. Although there are laws that can be interpreted by analogy, by extrinsic nor restrictive, the law can not replace the analysis of ethics is the basis of values and instrument when legal vacuum. [8] On development, factors dominant influence personal data protection is technology, devices, and consumer awareness to protect their personal rights not for public consumption. But the trendd development, the *youtuber* spit various impressions concerning the private life, reap the value of commodities. Modern culture erodes the values of privacy so that the ethical responsibility to maintain traditional values begins to fade. Without realizing it, humans become objects of technological exploitation.

The ethical and legal orchestration in the context of personal data protection is based on the provisions of Article 28 G point (1) of the Constitution of the Republic of Indonesia, namely that everyone has the right to personal, family, and honor protection. dignity, and property under his control. Honor and dignity are constitutional rights, above any other rights, cannot be replaced by anything.[9] Safe personal data for legal subjects from the threat of fear, and gain the freedom to live and produce works.The ethical principles of personal data protection: 1) autonomy, namely the right to use personal data. Recording and publication must be with the permission of the data owner and based on the agreement of the data owner. Both the recording of personal activities, as well as electronic data. 2). The principle of the option for the vulnerable, meaning that personal data protection priority to the vulnerable person, so as not to be manipulated. [10] Vulnerable people are humans whose personal data are used as research subjects, human trafficking, patients whose personal data is stored in

hospitals, women, disabled people, children, and the elderly. 3). the principle of justice, meaning that in personal protection there is a balance of rights and obligations *before the law (equality before the law).* [11] This covers all aspects of life because people often do not realize that they are victims of personal data leaks.

4. Future Personal Data Protection Concept

The ethical aspect is a reflection and regulation internally and externally of human life. The increase in, crimes against personal data requires standardization of personal data protection. The current regulation places crimes against personal data as a complaint offense, because it usually involves the defamation of a person's reputation, or that the loss due to data leakage occurs around a business, which is within the framework of private law. This implies that legal protection is needed to integrate and coordinate various interests in society because in interests, protection of certain interests can only be done by limiting various interests on the other hand. The legal vacuum causes human rights to be unprotected. Referring to Satijipto Raharjo's opinion, legal protection is to human rights that have been harmed by others and that protection is given to the community so that they can enjoy all the rights granted by law. Law can be functioned to realize protection that is not only adaptive and flexible but also predictive and anticipatory. Law is needed for those who are weak and not yet strong socially, economically, and politically to obtain social justice.

International instruments governing the protection of personal data : The Council of Europe Convention for the Protection of Individuals with regards to automatic Processing of Personal Data. In the business context, business actors are required to store personal data with the usual developing business practices. Elucidation of Article 59 of Government Regulation Number 80 of 2019 concerning Personal Data Protection Standards takes into account the existence of European Data Protection Standards and/or APEC in terms of *Privacy Framework.*Regarding personal data in medical services, the trend of telemedicine is growing, but no specific rules governing it.[5] In the current case handling, relying on Article 15 of Law Number 19 of 2016 concerning Electronic Information and Transactions, that the responsibility for the security of personal data rests with the provider platform or electronic system application. In telemedicine, it is necessary to secure patient data in the form of electronic medical records, namely the computerization of the contents of health records and the process of electronization related to medical services. This electronization results in a system that is specifically designed to support users with various facilities for completeness and accuracy of data; give a warning sign; as a warning; mark clinical decision support systems and link data with medical knowledge and other aids. This is also related to the need for standardization of the authority of legal subjects who affix Electronic Signatures, namely signatures consisting of Electronic Information that is attached, associated or related to other Electronic Information used as a means of verification and authentication.

The principle of legality in the adage *nullum delictum nuulla poena sine oprevia lege poenali, the requirements for legality of lex certa, lex stricta, lex scripta*, actually results in the law being confined in rigid positivism which always asks what the law is so that an act is considered an offense. If the law does not regulate it, an act cannot be punished. Whereas crime is still considered a step, deterrence, and the law as an instrument of protection loses its meaning. At such a level, the void in the law can be filled with ethics the values of public civility that have been preserved in the order of people's lives. Good and bad an action is based on the conscience and will of the communal community. Ethics provides an answer when the legislation has not explicitly regulated an act.Some critical notes related to the protection of personal data from the perspective of legal ethics: 1). it is necessary to stipulate regulations at the level of law in order to achieve legal unification that provides certainty on the existence of constitutional rights to personal data. 2). the principles that must exist include autonomy, protection of the vulnerable and access to justice for victims should be the main substance. 3). Crimes against personal data should be a normal offense and not a complaint offense with an integrated handler in an integrated criminal handling system. 4). accessibility for the community in obtaining justice.

IV. CONCLUSION

Ethics and law cannot be separated from one another. Legal certainty is obtained through efforts to formulate precise and explicit rules regarding the protection of personal data. The current legal problem is the void of the law because the pace of development of information technology runs faster than the law itself. The emptiness of this law can be answered with ethics, where the value of good/bad, right/wrong of an act is not solely determined by what is formulated in written law but comes from ethical values in society.

There is a need for periodic evaluations of the achievement of standardization of the validity of electronic data, monitoring systems for public service providers such as business centers, personal data management institutions, telemedicine services.The principles for constructing a rule of law are: autonomy, protection of the vulnerable and justice. There needs to be a paradigm shift that the leakage of personal data is not only a matter of private law but public law, crimes using personal data are ethical violations, which must be viewed as not a complaint offense, but an ordinary offense, which in its implementation is the responsibility of the government and the whole community.

V. ACKNOWLEDGMENTS

Sincerely thanks to fellow lecturers at the Faculty of Law, University of 17 August 1945, Surabaya, who have provided support so that this work can be completed properly.

REFERENCES

[1] M. Soleh, "The Urgency of Personal Data Protection," *Koran Sindo*, Jakarta, p. 1, 2021.
[2] S. Dewi, "The Concept of Legal Protection for Privacy and Personal Data," *Yustisia*, vol. Vol 5. No., 2016.
[3] H. Niffari, "Protection of Personal Data as part of Human Rights for Personal Protection (A Comparative Review with Legislation in Other Countries," *Juridical*, vol. 7, no 1, pp. 105–119, 2020.
[4] D. Supryadi, "Personal Data and the Two Legal Basis for Its Utilization."
[5] A. Anwar, "Legal Aspects of the Use of Telemedicine," *Fiki 2013*, p. 1 (1), 2013.
[6] I. Supancana, "Personal Data Protection in Various Countries," 2021.
[7] K. Bertens,, *Biomedical Ethics*Yogyakarta: Kanisius, 2011.
[8] S. Mertokusumo,, *Legal Inventions*Yogyakarta : Maha Karya Pustaka, 2020.
[9] J. Waldron, "Dignity, Rights, and Responsibilities," *SSRN Electron. J.*, no. 10, 2012.
[10] C. Kusmaryanto, *Bioethics*. Jakarta: Kompas, 2016.
[11] J. Waldron, "Clarity, Thoughtfulness, and the Rule of Law," *Vagueness Law*, no. 11, pp. 318–332, 2017.