Edunity

Volume 3 Number 6 June 2024

p- ISSN 2963-3648- e-ISSN 2964-8653

THE URGENCY OF PERSONAL DATA PROTECTION AGENCIES IN SUSTAINING THE RESILIENCE OF THE DIGITAL WORLD

Dhea Yulia Maharani[1], Suparno[2]
Universitas Borobudur, indonesia
Email: dheayuliamm@gmail.com[1], suparno@borobudur.ac.id[2]

ABSTRACT

The Industrial Revolution had a significant impact on human life, demonstrated by the quick use of enormous amounts of information. The peculiarity is in this manner directed by Regulation Number 27 of 2022 concerning Individual Information Assurance (UU PDP). The legal framework and foundation for data are provided by the law and/or information exchange activities in Indonesia. Article 58 Paragraph (2) of the UU PDP mandates the establishment of an institution tasked with implementing security for individual data. Because of the powerful idea of information and additional data exchanges, there is an earnestness to lay out a foundation for individual information security. The research will focus on exploring the role and actions of the Government thus far within the framework of individual information insurance before the foundation of the individual information assurance establishment. Moreover, this concentrate likewise assesses the criticalness of laying out an individual information security establishment in keeping up with computerized world versatility. The technique utilized in this examination is regularizing juridical, explained through a rule approach.

Keywords: Urgency; Personal Data Protection Institution; Personal Data Protection; Cyber Law.

Introduction

The fourth industrial revolution has had a significant impact on human interaction patterns. The fourth industrial revolution also reshaped government systems, education, health services, and trade (Savitri, 2019). The development has resulted in massive data collection so that governments and private companies compete to dominate data management. This data collection is known as "Big Data" which has high economic benefits. TechAmerica Foundation's Federal Big Data Commission defines Big Data as "a term that describes large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information (Mills et al., 2012)."The rapid development of technology has had positive and negative impacts because apart from contributing to the welfare of human civilization, it has also become a means for committing criminal acts known as "cybercrime."

Based on history, cybercrime developed rapidly in 2003, including carding, ATM/EDC skimming, hacking, cracking, phishing, malware, online gambling, human trafficking, and transnational crime (Rumlus & Hartadi, 2020). All of these criminal acts can be carried out through accessing personal data. Janice Kall explains “Data, however, is an object that can produce and govern effects at the same time. It is apparent in the

way that data is often collected to be repackaged as information about the consumers' behavior to further nudge that behavior in a certain direction (Käll, 2020)."The idea has prompted the international community to recognize a constitutional right to personal data protection in the form of "habeas data," which refers to a person's right to obtain protection for the data they possess and as a justification in the event that their data is compromised (Nadia, 2020).

Conversations with respect to the security of individual information in Indonesia started to be examined after private freedoms were perceived as basic liberties in Article 28G section (1) of the 1945 Constitution of the Republic of Indonesia. Article 28G Section (1) expresses that each individual has the privilege to insure himself, his family, honor, nobility, and property under his influence, and has the option of a feeling of safety and security from the danger of dread of doing or not accomplishing something which is a common liberty. Even though the right to privacy, as well as the right to freedom of thought, opinion, religion, and expression, are inextricably linked, there are distinct characteristics that indicate that the right to protect personal data is a separate and distinct right (McDermott, 2017).

The acknowledgment of legitimate sureness in regard to the security of individual information in Indonesia is the death of Regulation Number 27 of 2022 concerning Individual Information Assurance (UU PDP), and it goes about as a lawful umbrella for the insurance of individual information in Indonesia. The execution of individual information assurance can't be carried out ideally in light of the fact that there are no establishments commanded by the PDP Regulation. In view of Article 58 of the PDP Regulation, it is stressed that the Public authority plays a part in understanding the execution of individual information security through a foundation that has been laid out and is mindful to the President.

Before the death of the PDP Regulation, guidelines with respect to the insurance of individual information were spread across a few government establishments, for example, the Service of Correspondence and Data of the Republic of Indonesia, the Overall Political Race Commission of the Republic of Indonesia, the Service of Home Issues of the Republic of Indonesia, the Monetary Administrations Authority, Bank Indonesia and the Police of the Republic of Indonesia. The abnormality of these guidelines causes irreconcilable situations between foundations in executing individual information assurance. Personal data protection will also be difficult to implement in Indonesia because there are no law enforcement agencies to protect personal data.

Research Method

This examination utilizes standardizing juridical strategies which are done by looking at library materials (auxiliary materials) connected with individual information security organizations and the execution of individual information assurance in Indonesia. The information utilized in this examination is essential to legitimate materials such as legal guidelines, auxiliary lawful materials such as books, diaries, reports, classes, and tertiary legitimate materials, to be specific word references as well as reference books. The information that has been obtained is then examined utilizing a subjective illustrative technique, to specifically portray the lawful realities found and

afterward connecting them to important positive legitimate standards (Syamsudin, 2021).

Approach

By examining and analyzing legislation and regulations related to the legal issues under investigation, this research employs a statute approach. The resolution approach in this exploration is utilized to survey the direness of an information security authority and to exhaustively audit government activities connected with individual information security in Indonesia.

Result and Discussion

Government Roles and Actions in Protecting Personal Data

The security of individual information is important for the insurance of protection privileges, which is the right of an individual (individual) or a group to determine whether or not information relating to themselves can be processed and communicated to other parties (Syamsudin, 2021).The emergence of these rights is in line with the various rights granted by law to humans, including:

1. Human rights, are natural rights that are inherent in humans from birth and cannot be reduced, eliminated, or ignored for any reason. A person must be protected by his natural rights by the state.
2. Material rights, these rights relate to a person's ownership or control of an object, whether movable or immovable. Everyone is obliged to respect the existence of material rights because they are absolute.
3. Individual rights, these rights relate to a person's right to sue and/or charge someone and can only be defended against other people..

Assurance of individual information is firmly connected with Regulation Number 39 of 1999 concerning Basic liberties (Common freedoms Regulation) which is perceived by the State. In view of Article 2 of the Human Rights Law, is to recognize and uphold human rights and basic human freedoms as natural rights that are inherent in the self and cannot be separated from humans, so they need to be protected, respected, and upheld to increase human dignity, welfare, happiness, and intelligence and justice. Security of individual information inside the system of the right to protection can be found in the definition of Article 32 of the Basic Freedoms Regulation which makes sense that autonomy and privacy in correspondence, including correspondences through electronic means, should not be upset by request of an adjudicator or other genuine power by the arrangements of legal guidelines. - greeting.

In light of the portrayal over, the State should safeguard individual information. Before the issuance of the PDP Regulation, the commitment to safeguard individual information was managed in Unofficial Law Number 80 of 2019 concerning Exchanging through Electronic Frameworks. In light of Article 58 of the guideline, it makes sense to:

"(1) Any personal data is treated as the personal property of the person or Business Actor concerned;

(2) Every Business Actor who obtains personal data as intended in paragraph (1) is obliged to act as a mandate developer in storing and controlling personal data by the provisions of statutory regulations."

Personal data is classified as property rights in the realm of Indonesian civil law which does not limit personal data as objects, because its nature can be called an intangible object. If it has been processed in such a way, personal data can become big data that will have economic value to the owner and can be maintained by other parties (Niffari, 2020). The state carries out its obligations to recognize and be considerate of the rights and liberties of others in order to meet reasonable demands while taking security and public order into account. In view of this, the government provided Regulation Number 11 of 2008 concerning Data and Electronic Exchanges ("UU ITE") which characterizes individual information as electronic data as in Article 1 number 1 of the ITE Regulation which makes sense as follows:

"Electronic Information is one or a collection of electronic data, including but not limited to writing, sound, images, maps, plans, photos, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, Access Codes, symbols, or processed perforations that have meaning or can be understood by a person capable of understanding them."

The legitimate instruments as executing guidelines for the ITE Regulation were then carried out in Unofficial law Number 71 of 2019 concerning the Execution of Electronic Frameworks and Exchanges (PP PSTE). In view of Article 1 number 29 PP PSTE makes sense that individual information is any information about an individual, whether recognized or potentially recognizable exclusively or joined with other data, either straightforwardly or in a roundabout way, through electronic as well as non-electronic frameworks. Security of individual information in the ITE Regulation incorporates security from unapproved use, assurance for electronic framework administrators, as well as assurance from unlawful access (SAFIRA, 2021).

As stipulated in PP PSTE, the Ministry of Communication and Information (Kemkominfo) fulfilled the government's obligations to safeguard personal data. The Service of Correspondence and Information is given the task of carrying out supervision as stated in Article 35 PP PSTE as follows:

"(1) The Minister is authorized to supervise the operation of Electronic Systems.
(2) The supervision referred to in paragraph (1) includes monitoring, controlling, inspecting, investigating, and securing.
(3) Provisions regarding the supervision of the operation of Electronic Systems in certain sectors must be established by the relevant Ministries or Agencies after coordinating with the Minister."

The ITE Law classifies electronic system operators into two categories: "Public Scope Electronic System Operators" and "Private Scope Electronic System Operators." Public scope electronic system operators are those managed by state institutions or institutions designated by state institutions. Private-scope electronic system operators are those managed by people, business substances, and general society. In case of framework disappointment or serious disturbance brought about by different gatherings influencing the electronic framework, the electronic framework administrator is expected to get the data as well as electronic archives and quickly report it at the principal opportunity to police the Service of Correspondence and Data Innovation, as specified in Article 24 passage (1) of the PP PSTE.

The government has a role in the PP PSTE as stated in Article 90 of the PP PSTE as follows: "The Government's role in the operation of Electronic Systems and Transactions includes:

a. Facilitate the use of Information Technology and Electronic Transactions by statutory provisions;
b. Protecting public interests from all types of disturbances resulting from misuse of Electronic Information and Electronic Transactions which disrupt public order, under the provisions of laws and regulations;
c. Prevent the dissemination and use of Electronic Information and/or Electronic Documents which contain prohibited content under the provisions of laws and regulations; And
d. Determine agencies or institutions that have strategic electronic data that must be protected."

To fortify individual information security, the Public authority along with the Place of Agents of the Republic of Indonesia (DPR RI) authorized the Individual Information Assurance Regulation (UU PDP) in 2022. The UU PDP is a gathering of dispersed guidelines on private information, efficiently organized. The execution of individual information assurance through the UU PDP depends on a few standards, including (Faisal & Indriani, 2022):

a. Personal data must be obtained legally and honestly;
b. Personal data must be used for a specific and legitimate purpose, so processing personal data in ways that do not align with the established purpose is not allowed;
c. Personal data must be adequate, relevant, and specific about the processing purpose;
d. Personal data must be accurate and up-to-date, ensuring that any inaccurate or irrelevant data is deleted or corrected;
e. The processing of personal data must be by the rights of the data subjects as stipulated by laws and regulations;
f. Security measures must be taken to anticipate unauthorized data processing and prevent both expected and unexpected losses;
g. Data must not be stored for a long period or beyond the necessary duration for data collection and processing purposes;
h. Organizations must be held accountable for the principles and rights of personal data subjects.

These principles are expressly regulated in Article 16 of the PDP Law so that the implementation of personal data protection in carrying out roles and functions is guided by the principles as stipulated in the PDP Law. In order to strengthen the government's role in implementing personal data protection, the PDP Law mandates the establishment of an institution that plays a role in implementing personal data protection as stipulated in Article 58 of the PDP Law.

The Urgency of a Personal Data Protection Institution within the Framework of Digital World Resilience

Article 58 of the Individual Information Security Regulation orders the foundation of an establishment as a substantial sign of the Public authority's activity in executing individual information assurance. The establishment of a personal data protection

institution is required to symbolize the State's presence in society and achieve legal certainty in the area of personal data protection. Individual information security in Indonesia preceding the issuance of the Individual Information Insurance Regulation had a trademark highlight, to be specific being sectoral. Bank Indonesia and the Financial Services Authority, for example, were responsible for personal data protection in the banking industry. It prompted the execution of individual information assurance not being done completely and comprehensively. Rules connected with individual information security were as yet broad in nature, so the idea of individual information assurance was not explicitly and obviously directed and carried out (Makarim, 2005).

Indonesia is one of the nations with the biggest number of web clients on the planet, with a total of 212.9 million users. The Central Statistics Agency explains that Indonesia's population in 2022 was 275 million, with a conclusion that 77 percent of Indonesia's population has used the Internet (Utomo, Gultom, & Afriana, 2020). In light of this information, it tends to be seen that the quantity of individual information subjects in Indonesia is exceptionally high. The implementation of personal data protection is affected by the high number of personal data subjects in Indonesia. As a result, it is anticipated that the institution for the protection of personal data will be able to address the concerns regarding personal data in Indonesia, which has a large number of subjects.

Another nation with a high rate of personal data leaks is Indonesia. In light of information delivered by network safety organization Surfshark, Indonesia is the third country with the biggest number of information spill cases on the planet. It was recorded that 12.74 million records experienced information spills in Indonesia during the second from last quarter of 2022 (Yonatan, 2023). The high number of data leaks in Indonesia reinforces the fact that the enforcement and supervision of Indonesia still lacks adequate protections for personal data. Aside from that, this additionally makes sense of the way that administration foundations, for this situation, the Service of Correspondence and Data or related establishments, have not ideally completed their jobs and work in overseeing and administering the flow of electronic information as well as data.

In the Southeast Asia locale, the country that has great individual information security foundations is Singapore. Singapore has an individual information security foundation, in particular the Individual Information Insurance Commission and Organization which was framed by the Individual Information Assurance Demonstration of 2012. This organization was framed by the applicable clergyman with the accompanying obligations and capabilities (Annur, 2022a):

a. Empowering mindfulness in regards to the assurance of individual information for the general population;
b. Get grumblings, discussion, backing, specialized, arranging, and different administrations connected with individual information insurance;
c. Giving contribution to the public authority in regards to issues connecting with the assurance of individual information;
d. representing the government in international forums regarding personal data security;

e. Doing studies, examinations, training, and investigation connected with the assurance of individual information.

A legal regulation must be understandable and of concern to the public. So far, public awareness regarding personal data protection tends to be low. Based on the results of research between the Ministry of Communication and Information and the Katadata Insight Center in 2021 with a survey sample of 10,000 respondents from 34 provinces and 514 districts/cities throughout Indonesia, it was concluded that 53.6 percent of Indonesian people had a low level of personal data protection (Doly, 2021). The low level of awareness of the Indonesian people regarding the protection of personal data should be a concern for the government. There is a need for an institution that specifically provides intensive education to the public considering that in the current era, personal data is a commodity with economic value (Annur, 2022b).

The PDP Law as a rule and legal umbrella for implementing personal data protection requires the existence of a government regulation as an implementing regulation of the law. Several articles in the PDP Law explain that further provisions regarding an article in the PDP Law are regulated in government regulations. Until now, there are still no government regulations as stated in the PDP Law. Substantial matters regarding procedures for imposing compensation for violations of personal data processing are further regulated in government regulations, but due to the absence of government regulations, compensation efforts for violations of personal data processing cannot yet be implemented. The principle of protecting personal data is that it can be accounted for, so this principle cannot be implemented optimally.

The clarifications above are a portion of the issues in carrying out private information security in Indonesia. The presence of the PDP Regulation can't tackle the issue of safeguarding individual information as a whole but requires an institution that specifically monitors and takes action if there is a violation of individual information security according to the arrangements in the PDP Regulation. Given the significance of providing education on personal data protection, institutions for personal data protection are also required. Indonesian people with a low level of awareness.

Conclusion

In view of the depiction given, it tends to be reasoned that before the foundation of the individual information security establishment, the execution of individual information assurance was still sectoral in unambiguous fields. It resulted in regulations regarding personal data protection being confined to narrow scopes, thus not comprehensively and massively regulated. Additionally, the government's implementation of personal data protection was conducted by relevant institutions, namely the Ministry of Communication and Information Technology (Kemkominfo), which oversees the communication and information sector in Indonesia. The legitimate structure for the execution of individual information security before the order of the Individual Information Assurance Regulation (UU PDP) actually alluded to the Data and Electronic Exchanges Regulation (UU ITE), which in a general sense didn't explicitly and unequivocally manage individual information security in light of the standards of individual information protection.

General institutions cannot immediately resolve the personal data management issue in Indonesia. A specific foundation zeroed in on supervising the administration of

individual information is required, working as a device to smother infringement of individual information security. The large number of web clients, the elevated degree of information releases, the low familiarity with individual information security, and the shortcomings of government foundations in tending to infringement of individual information security highlight the direness of laying out an individual information security organization in Indonesia.

Bibliography

annur, Cindy mutia. (2022a). indonesia masuk 3 besar negara dengan kasus kebocoran data terbanyak dunia. retrieved from databoks website: https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia.

annur, Cindy mutia. (2022b). pelindungan data pribadi warga ri masih tergolong rendah. retrieved from databoks website: https://databoks.katadata.co.id/datapublish/2022/08/09/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah#:~:text=menurut survei kementerian komunikasi dan,tingkat pelindungan data pribadi rendah.

Doly, denico. (2021). pembentukan lembaga pengawas pelindungan data pribadi dalam perspektif pembentukan lembaga negara baru (establishment of a personal data protection supervisory agency in the perspective of the establishment of a new state institution). *negara hukum: membangun hukum untuk keadilan dan kesejahteraan*, *12*(2), 223–244.

faisal, bagus imam, & indriani, dian eka. (2022). pertanggung jawaban pidana uu ite terhadap pembobolan data pribadi di era serba digital. *civic-culture: jurnal ilmu pendidikan pkn dan sosial budaya*, *6*(2), 652–661.

käll, jannice. (2020). the materiality of data as property. *harvard international law journal*, *61*, 1–11.

makarim, edmon. (2005). *kompilasi hukum telematika*.

McDermott, Yvonne. (2017). conceptualizing the right to data protection in an era of big data. *big data & society*, *4*(1), 2053951716686994.

mills, steve, Lucas, steve, irakliotis, Leo, Rappa, Michael, Carlson, Teresa, & perlowitz, bill. (2012). demystifying big data: a practical guide to transforming the business of government. *TechAmerica foundation, Washington*.

nadia, syarifah. (2020). mengembalikan humanisme perlindungan data pribadi melalui perluasan yurisdiksi ekstrateritorial sebagai upaya diplomasi dalam mewujudkan keamanan siber. *antologi esai hukum dan ham afiliasi hukum dan ham dalam mewujudkan perlindungan hak asasi masyarakat indonesia*, *1*, 55.

niffari, hanifan. (2020). perlindungan data pribadi sebagai bagian dari hak asasi manusia atas perlindungan diri pribadi (suatu tinjauan komparatif dengan peraturan perundang-undangan di negara lain). *jurnal yuridis*, *7*(1), 105–119.

rumlus, muhamad hasan, & hartadi, hanif. (2020). kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *jurnal ham*, *11*(2), 285–299.

safira, dina islamiati. (2021). *perlindungan hukum terhadap kerahasiaan data pribadi pengguna marketplace berdasarkan hukum positif di indonesia*. universitas mataram.

savitri, astrid. (2019). *revolusi industri 4.0: mengubah tantangan menjadi peluang di era disrupsi 4.0*. penerbit genesis.

syamsudin, muhammad. (2021). *mahir meneliti permasalahan hukum*. prenada media.

utomo, handryas prasetyo, gultom, elisatris, & afriana, anita. (2020). urgensi perlindungan hukum data pribadi pasien dalam pelayanan kesehatan berbasis teknologi di indonesia. *jurnal ilmiah galuh justisi*, *8*(2), 168–185.

yonatan, agnes z. (2023). indonesia peringkat 4, ini dia 7 negara pengguna internet terbesar di dunia. retrieved from goodstats website: https://data.goodstats.id/statistic/indonesia-peringkat-4-ini-dia-7-negara-pengguna-internet-terbesar-di-dunia-flw6v.