



Securing Personal Data: Unveiling the Crucial Role of Legal Education in Non-Fungible Token Sites

Ninne Zahara Silviani¹, Farhan Rabbani Abrar²

¹Faculty of Law, Universitas Internasional Batam, ninne@uib.ac.id

²Faculty of Law, Universitas Internasional Batam, farhanrabbaniabrar@gmail.com

ABSTRACT

With the rapid advancement of technology, the emergence of Non-Fungible Token (NFT) platforms has revolutionized digital buying and selling. However, this innovative platform has also given rise to a concerning issue: the unintentional trade of personal data instead of artwork. This problem poses a significant challenge in protecting individuals' personal information, especially when items like National Identity Card (KTP) photos are sold as NFT assets. This research aims to explore the critical importance of legal education in safeguarding personal data, thus preventing such transactions that may lead to self-harm. Employing a normative juridical method and a conceptual approach, this study extensively analyzes legal aspects and regulations related to personal data protection. The findings underscore the urgent need for legal education to effectively address personal data transactions on NFT sites within marketplace platforms. Despite the implementation of the Personal Data Protection Act (Law Number 27 of 2022), it is clear that the legislation alone is insufficient. Given the gravity of the issue, comprehensive public education initiatives involving various segments of society are crucial. Protecting personal data has become a matter of utmost concern for the government, the state, NFT platform users, and internet users at large. Individuals must adopt a vigilant and proactive approach in safeguarding their personal data. Legal education programs, including outreach activities conducted by governmental and non-governmental entities, along with the involvement of students and academics in community counseling, can effectively support this objective.

Cite this paper

Silviani, N. Z., & Abrar, F. R. (2024). Securing Personal Data: Unveiling the Crucial Role of Legal Education in Non-Fungible Token Sites. *Widya Yuridika: Jurnal Hukum*, 7(1).

MANUSCRIPT INFO

Manuscript History:

Received:

2023-06-09

Accepted:

2024-03-12

Corresponding Author:

Ninne Zahara Silviani,

ninne@uib.ac.id

Keywords:

Non-Fungible Token;

Personal Data Protection;

Legal Education, Self-Harm

Prevention



Widya Yuridika: Jurnal Hukum is Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Layout Version:

v.7.2024

PRELIMINARY

The ratification of Law No. 27 of 2022 on the Protection of Personal Data represents a significant milestone in Indonesia's digital landscape and electronic commerce. With the exponential growth of digital trade, numerous challenges have emerged pertaining to the unauthorized sale of personal data, which should be strictly protected.¹ This issue has been exacerbated by the rapid development of information technology, leading to the emergence

¹ Raihan, M. (2023). Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). *Jurnal Inovasi Penelitian*, 3(10), 7847-7856.

of new legal complexities, specifically concerning the security and protection of personal data transmitted through electronic media.² The extensive reliance on electronic platforms for communication and transactions has further compounded the problem, resulting in the widespread misuse of personal data. In this context, the ratification of Law No. 27 of 2022 is a breath of fresh air, heralding a transformative approach towards addressing these concerns and establishing comprehensive safeguards to protect personal data in the digital realm.

Prominent nations, including the European Union, the United States, the United Kingdom, Hong Kong, Singapore, and Malaysia, have enacted specific and comprehensive regulations governing the handling of personal data. In contrast, Indonesia currently lacks a dedicated legislation addressing the protection of personal data. The regulations pertaining to this issue are primarily outlined in Article 26 of Law No. 11 of 2008 concerning Information and Electronic Transactions, supplemented by several other independent laws and regulations. However, the aforementioned article remains rather broad in scope. Consequently, there is an urgent need for the enactment of a distinct legislation specifically aimed at guaranteeing the security and protection of personal data. Such a law would entail the establishment of both criminal and civil penalties for individuals or entities found guilty of abusing personal data.³

Personal data protection encompasses the legal measures in place to safeguard the collection, registration, storage, utilization, and dissemination of personal data.⁴ Within the realm of telematics law, the utilization of personal data through technology is governed by the provisions outlined in Article 26 of Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Information and Electronic Transactions. These provisions provide a comprehensive understanding of the concept of personal data protection and its application in the context of utilizing information technology.⁵ The absence of adequate regulations pertaining to personal data exposes it to potential abuse in the digital realm, thereby infringing upon personal rights, including the right to determine and control one's own personal data. Such violations can manifest in various ways, such as unauthorized collection and unauthorized distribution of personal data.⁶

The mentioned violations are intricately linked to cybercrime, an encompassing term that includes activities like carding, hacking, skimming, and phishing. It is undeniable that as technology advances and brings numerous benefits, it also brings along negative repercussions. Hence, utilizing technology for data protection becomes imperative to safeguard against cybercrime-related incidents.⁷ Several mass media outlets have reported numerous cases, including complaints raised by Facebook users regarding the proliferation

² Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, 2(3), 654-666.

³ Shahrullah, Rina, Syarief, Elza, AND Crystina Aprilia. "Pemberlakuan Aturan Hukum Pajak Terhadap Youtuber dan Penjual Online Shop " *Journal of Law and Policy Transformation (Online)*, Volume 4 Number 2 (20 December 2019)

⁴ Rosadi, S. D., Noviadika, A., Walters, R., & Aisy, F. R. (2023). Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?. *International Review of Law, Computers & Technology*, 37(1), 78-90.

⁵ Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, 5(2), 177-199.

⁶ Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 369-384.

⁷ Rizki, R., & Gultom, E. R. (2023). Differences in Data Protection Systems in Indonesia And Singapore. *Indonesian Journal of Law and Policy Studies*, 3(2), 150-159.

of individuals selling personal identities on the Opensea platform.⁸ This issue has also garnered significant attention on Twitter, where users have shared screenshots of an NFT collection called the "Indonesian Identity Card (KTP) collection." The collection comprises 38 NFTs featuring images of Indonesian Identity Cards (KTP), selfies, and selfies alongside KTPs. This revelation has sparked widespread discussions and concerns across social media platforms.

The lack of awareness regarding the consequences of selling personal data leads individuals to overlook the inherent dangers associated with such actions. Selling personal data, whether it is our own or that of others, carries numerous negative implications. The impacts of selling personal data include: (1) Accessible to Make Online Loans. The distribution of personal data on the platform allows unrestricted access to various groups, rendering it susceptible to being utilized for online loan applications. This vulnerability arises from the fact that the data belongs to a private individual but is misappropriated by others. Consequently, the onus of responsibility falls upon the owner of the personal data; (2) Accessed for Crime. As we all know, personal data (KTP) is extremely sensitive if it is used to break into a number of other people's accounts. This includes crimes against others; and (3) Profiling for Political Targets or Advertising on Social Media. Reporting from Solopos.com Scattered personal data will be used for political purposes such as political outreach and social media advertising.⁹

The voluntary sale of personal data by individuals, stemming from a lack of legal education, highlights the shortcomings of existing laws.¹⁰ The public, particularly concerning the sale of personal data, would greatly benefit from increased legal education. However, such education should be supported by public regulations (Government Regulation) and private initiatives (such as the Opensea company). Consequently, the significance of personal data protection becomes increasingly evident. Numerous earlier studies delving into personal data protection were frequently conducted during the formulation of the Personal Data Protection Bill. Noteworthy titles encompassed Personal Data as Transaction Objects in NFTs on the Opensea Platform¹¹ and Claims for Compensation regarding the Use of Personal Data in Electronic Mail as stipulated by Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Information and Electronic Transactions.¹² The author's research holds inherent novelty as it aligns with the enactment of the Personal Data Protection Act, emphasizing the significance of legal education for the general public concerning the vital aspect of safeguarding personal data. Based on the provided background, the research aims to explore the pressing need for regulatory mechanisms concerning the utilization of personal data within the draft law on the protection of personal data. The study addresses two primary research problems: (1) How does the Personal Data Protection Act address the issue of selling personal data, specifically in relation to identity

⁸ Deviyanti, P.A.S. (2017). *Tuntutan Ganti Rugi Penggunaan Data Pribadi Surat Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Universitas Udayana: Skripsi S1 Fakultas Hukum.

⁹ Prameswati, V., Sari, N. A., & Nahariyanti, K. Y. (2022). Data Pribadi Sebagai Objek Transaksi di NFT pada Platform Opensea. *Jurnal Civic Hukum*, 7(1).

¹⁰ Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti Jurnal Hukum*, 4(2), 79-93.

¹¹ Newswire. (n.d.). Ini Bahaya Yang Bisa Terjadi Bila Data Pribadi Kita Bocor. <https://www.solopos.com/ini-bahaya-yang-bisa-terjadi-bila-data-pribadi-kita-bocor-1126609> (diakses pada 18 Maret 2023, pukul 19.07 WIB).

¹² Prameswati, V., Sari, N. A., & Nahariyanti, K. Y. (2022). *Op.Cit.*

cards? (1) How can legal education serve as a solution to enhance the effectiveness of personal data protection laws?.

METHOD

This study employs a rigorous juridical-normative method complemented by a conceptual approach.¹³ Normative legal research involves a meticulous examination of literature and secondary data sources, surpassing mere legal doctrines.¹⁴ Furthermore, the conceptual approach adopted in this study delves into the efficacy of the Personal Data Law as a guiding framework for fostering education pertaining to the protection of personal data. This research relies on secondary data obtained through an extensive literature review. The secondary data encompasses primary, secondary, and tertiary legal materials. The primary legal materials utilized in this study include Law No. 27 of 2022 concerning Protection of Personal Data and Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Furthermore, the secondary legal materials consist of relevant research articles, books, and writings from popular media sources, providing valuable insights on related subjects. The collected data is subsequently subjected to descriptive analytical techniques, which involve presenting and interpreting the data through various means such as notes, visuals, and compilations of laws and regulations. In this research, the focus is on describing and analyzing the problems associated with cases, presenting the data in a systematic, factual, and precise manner. This approach enables the research to ascertain the significance of education concerning the protection of personal data, shedding light on its importance and implications.

RESULT AND DISCUSSION

The Law on the Protection of Personal Data and Addressing the Issue of Selling Personal Identity Card Data

In 2018, the comprehension of consumer data evolved into a novel form of business raw material, representing an economic input that rivals capital and labor. The economic significance of vast-scale data is often likened to digital currency.¹⁵ Initially, the concept of big data emerged within the academic realm of informatics. However, it has now gained significant popularity among policymakers as they shape policies, and it permeates various business disciplines that rely on data-driven approaches.

In the contemporary landscape, formidable companies like Facebook, Amazon, Alibaba, NFT, and Google have emerged as powerful entities engaged in the sale of personal data. Big Data, commonly referred to as a vast accumulation of diverse data types, is generated rapidly from numerous sources. Its handling and analysis necessitate the utilization of new and robust algorithms, acknowledging the complexities associated with processing such massive datasets. From a telecommunications standpoint, personal data concerns can arise due to various factors, one of which is the prevalent and intensive internet activity. This activity leaves behind traces in the form of location information, search records,

¹³ Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, 24(2), 289-304.

¹⁴ Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463-2478.

¹⁵ Marzuki, P.M. (2010). *Metode Penelitian Hukum*. Jakarta: Kencana Prenada.

application updates, and more. Without adequate protection, such data is susceptible to misuse or unauthorized exploitation over an extended period.¹⁶

Personal Data essentially encompasses information pertaining to an individual, encompassing aspects of their personal, professional, and public life.¹⁷ This can include details such as names, addresses, photographs, email addresses, account numbers, media information, or computer IP addresses that are associated with an individual or entity. Within personal data lies the fundamental right to privacy for individuals.¹⁸

In Indonesia, there is currently no specific law that comprehensively regulates the protection of personal data, despite the presence of positive legal provisions. Although the 1945 Constitution of the Republic of Indonesia does not explicitly guarantee the protection of personal data as an integral part of the respect, protection, and fulfillment of Human Rights (HAM), it remains a significant aspect to be addressed in ensuring individuals' privacy rights are safeguarded. Indeed, although not explicitly stated, Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia serves as the juridical foundation for the protection of personal data in Indonesia. The interpretation is that everyone has the right to personal protection, which encompasses the protection of personal data. In the context of Information Technology, the protection of personal data is considered as part of an individual's privacy rights, as clarified in the Explanation of Article 26 paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (referred to as the ITE Law). This interpretation solidifies the recognition of personal data protection as a vital component of an individual's rights in the digital age. In more specific terms, the scope of personal data protection in Indonesia is outlined in the Regulation of the Minister of Communication and Informatics No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems. This regulation encompasses various aspects of personal data protection, including safeguarding against unauthorized acquisition, collection, processing, analysis, storage, disclosure, dissemination, delivery, distribution, and destruction of personal data within electronic systems. The regulation serves as a framework to ensure the comprehensive protection of personal data throughout its lifecycle within electronic systems.

Legislators have recognized the significance of personal data protection as an integral part of an individual's privacy rights. Efforts have been made to address this through legislative provisions, including the following:¹⁹ Firstly, Article 85 paragraph (1) of Law No. 23 of 2006 concerning Population Administration in conjunction with Law No. 24 of 2013 concerning Amendments to Law No. 23 of 2006 concerning Population Administration (referred to as the Population Administration Law) stipulates that the personal data of residents, as mentioned in Article 84, must be securely stored and protected by the state. Moreover, paragraph (3) of the same article emphasizes that the personal data of residents, as mentioned in paragraph (1), must be accurately maintained and protected by the implementing agency in accordance with the applicable laws and regulations. The scope of

¹⁶ Cukie, K. (2010). Data Everywhere. <https://www.economist.com/special-report/2010/02/27/data-data-everywhere> (diakses pada 15 Maret 2023, pukul 10.30 WIB)

¹⁷ Kurniawan, Y., Santoso, S. I., Wibowo, R. R., Anwar, N., Bhutkar, G., & Halim, E. (2023). Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media. *Sustainability*, 15(4), 3814.

¹⁸ Djafar, W. (2017). Big Data Dan Praktik Pengumpulan Data Skala Besar Di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi. *Jakarta: Elsam*.

¹⁹ Anggraeni, S. F. (2018). Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia. *Jurnal Hukum & Pembangunan*, 48(4), 814-825.

personal data protection, as defined in Article 84 paragraph (1) of the Population Administration Law, encompasses information pertaining to physical and/or mental disabilities, fingerprints, irises, signatures, and other sensitive data elements. These provisions aim to ensure the proper handling and safeguarding of such personal data.

Secondly, Articles 56 and 57 of Government Regulation No. 40 of 2019 concerning the Implementation of Law No. 23 of 2006 concerning Population Administration, as amended by Law No. 24 of 2013, have regulated the procedures for obtaining and using Resident Personal Data. According to the provisions of Article 56 paragraph (1) PP a quo, the acquisition of Personal Data of residents of Indonesian ministries/agencies and legal entities requires approval from the Minister, Governor, or Regent/Mayor, depending on the scope of the data required. Provisions in the PP a quo for obtaining personal data of residents do not yet reflect the principle of openness or transparency regarding the collection, storage, and use of personal data in Indonesia, given that the government handles the entire administrative procedure for obtaining personal data. Similarly, in Indonesia, supervision of the collection, storage, and use of Personal Data is required. The Minister, Governors, and Regents/Mayors are the institutions authorized to supervise the implementation of population administration, according to Article 63 paragraph (1) of the PP a quo. Meanwhile, the supervision referred to in paragraph (1) includes monitoring of data in databases, utilization of Population Data, and human resources who carry out Population Administration matters, according to the provisions of Article 63 paragraph (4) PP a quo.

Thirdly, Law No. 14 of 2008 concerning Public Information Disclosure, in Articles 17(g) and (f), establishes exceptions to the open access of public information, specifically for cases where the disclosure could reveal sensitive details such as the contents of an individual's authentic personal deed and will, as well as the history and circumstances of their family members, medical treatment, physical and psychological health, financial condition, assets, income, and bank account details. Fourthly, according to Article 57(1) of Law no. 36 of 2009 concerning Health, individuals are granted the right to maintain the confidentiality of their personal health conditions shared with healthcare providers. These provisions aim to safeguard Personal Data by ensuring privacy for confidential health information.

As an embodiment of the rule of law, it is imperative to establish legal regulations pertaining to the safeguarding of Personal Data. Presently, the government is taking measures to ensure the protection of Personal Data in Indonesia through the Personal Data Protection Act (UU PDP), which is currently undergoing Level I discussions in the DPR. The Personal Data Protection Act comprises approximately 72 article formulations divided into 15 chapters, covering various aspects such as Types of Personal Data, Rights of Personal Data Owners, Processing of Personal Data, Obligations of Personal Data Controllers and Personal Data Processors in Personal Data Processing, Transfer of Personal Data, Administration of Sanctions, Prohibition of the Use of Privacy Policy Data, Establishment of a Code of Conduct for Personal Data Control, Dispute Resolution and Procedure Law, International Cooperation, Role of Government and Society, Criminal Provisions, Transitional Provisions, and Closing Provisions. These provisions will serve as the legal foundation for organizations to address internet-related issues. By implementing these provisions, it ensures security against cybercrime threats and serves as a vital legal instrument in tackling personal data protection issues amidst the escalating incidents of data leaks.²⁰

²⁰ Cukie, K. (2010). *Op.Cit.*

The PDP Law should explicitly and precisely define the legal foundation that establishes the authority's mandate, powers, and independence.²¹ Establishing an independent authority or institution is crucial as it will not only oversee data controllers and processors in the private sector but also govern those in public bodies (government), ensuring comprehensive supervision.²²

Drawing upon the principles of state administration to promote the welfare of the people within the framework of modern governance, efficient and effective management is of utmost importance. The one-door administration mechanism, a development in administrative science, presents a relevant adaptation for governing the utilization of Personal Data in Indonesia and safeguarding it through independent institutions. This is especially crucial given the intricacies involved in regulating Personal Data as outlined in the PDP Law. The one-door administration concept, as an integrated mechanism, facilitates effective and efficient monitoring of the collection, storage, and utilization of Personal Data by both the government and the private sector. Should there be any violations of Personal Data through government policies or citizen surveillance, individuals have the opportunity to file complaints with the designated independent agency, ensuring accountability and safeguarding privacy rights.

Through the implementation of the one-door mechanism, the future use of Personal Data will attain enhanced transparency and measurability. This is particularly significant when considering the utilization of Personal Data by multinational companies, whether within or outside the jurisdiction of the Republic of Indonesia. Such usage will carry legal ramifications within the territory of Indonesia and extend to the protection of Personal Data of Indonesian citizens beyond its jurisdiction, as outlined in Article 2 of the PDP Law. This independent institution holds the authority to oversee the collection, storage, and utilization of Personal Data by requiring data users to report the specifics of the gathered information, its intended purpose, as well as the methods and locations of data storage. Additionally, this institution can effectively monitor cases of company mergers or acquisitions involving the use of Personal Data, ensuring the protection of consumer rights as owners of such data. Similarly, it plays a crucial role in monitoring changes in company policies that pertain to similar data-handling practices in providing services.

The author concludes that the ratification and implementation of the Personal Data Protection Law is a crucial and decisive measure to establish a robust legal framework that ensures the protection of citizens' personal data by the state.²³ This is evident as the Personal Data Protection Law is anticipated to prioritize the perspective of personal data protection in all advancements in technology, thereby fostering ethical innovation and upholding human rights. In addition to addressing technological advancements and digital culture, the presence of the Personal Data Protection Law is also intended to promote new norms and practices within society, fostering a stronger commitment to personal data protection.

²¹ Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, 3(1), 33-69.

²² Pratana, I. W. A. W. (2021). Urgensi Pengaturan Mekanisme Pemanfaatan Data Pribadi Dalam Rancangan Undang-Undang Perlindungan Data Pribadi. *Jurnal Hukum Lex Generalis*, 2(8), 701-721.

²³ Amboro, F. Y. P., & Puspita, V. (2021). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia). In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, 1, (1), 415-427.

The Role of Legal Education in Enhancing the Effectiveness of Personal Data Protection Laws

The implementation of the PDP law has brought about legal effectiveness, impacting both the government and the community, thereby contributing to legal education. The effectiveness of the law is influenced by four aspects: the legal factors themselves (laws), law enforcement entities (parties responsible for formulating and implementing the law), supporting facilities and resources for law enforcement, and the society (the environment where the law is applicable and enforced). Currently, the effectiveness of the law on personal data protection is primarily observed through the imposition of criminal and administrative sanctions.

To begin, consider the legal factors themselves. In 2022, the status of personal data protection in Indonesian law will be clarified. The Indonesian Telecommunications Regulatory Body (BRTI) stressed that the sale and purchase of personal data is illegal. According to Indonesian law, the perpetrators and the parties involved may face legal action. However, the Indonesian government is currently working on a more comprehensive personal data protection regulation. According to Article 57 of the PDP Law, namely:²⁴ (1) Violation of the provisions of Article 20 paragraph (1), up to paragraph (4) is subject to administrative sanctions; (1) The administrative sanctions as referred to in paragraph (1) are in the form of written warning; temporary suspension of Personal Data processing activities; deletion or destruction of Personal Data; and/or administrative fine; (3) The administrative sanction in the form of administrative fines as referred to in paragraph (2) letter d is a maximum of 2 (two) percent of the annual income or annual revenue for the violation variable; (4) Administrative sanctions as referred to in paragraph (2) are imposed by the institution; and (5) Further provisions regarding the procedures for imposing administrative sanctions as referred to in paragraph (3) are regulated in a Government Regulation.

Furthermore, article 67 states:²⁵ (1) Any Person who deliberately and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which can result in loss of the Personal Data Subject as referred to in Article 65 paragraph (1) shall be punished with imprisonment for a maximum 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah); (2) Any person who intentionally and unlawfully discloses personal data that does not belong to him as referred to in Article 65 paragraph (2) shall be subject to imprisonment for a maximum of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000. 00 (four billion rupiah); and (3) Any Person who deliberately and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be subject to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000. 00 (five billion rupiah).

However, these regulations have not effectively addressed individuals who lack familiarity with the law, necessitating an approach to educate the general public about the risks associated with selling personal data. By raising public awareness about the dangers involved in the sale of personal data, the government, as the regulatory body, assumes the responsibility of safeguarding and enforcing punishments for those who engage in such activities, regardless of whether it involves their own data or that of others. To this end,

²⁴ Undang-Undang Perlindungan Data Pribadi

²⁵ Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. com). *Borneo Law Review*, 5(1), 46-68.

preventive measures are being implemented, primarily through educational initiatives. These preventive efforts can be carried out through two channels: the government's dissemination of information and the community's cultivation of a sense of curiosity and personal development, which in turn fosters a respect for privacy and guards against arbitrary infringements.

Next, let us consider the aspect of legal culture, which is a crucial component of the Theory of Legal Effectiveness. In the context of personal data protection, it is important to acknowledge the prevalent cultural phenomenon known as Fear of Missing Out (FOMO). This term describes an individual's apprehension of being excluded or falling behind when they observe emerging trends or particular activities. Building upon this observation, it is only natural to recognize that the widespread use of NFTs, without proper education and awareness, can potentially lead to the misuse of these digital assets for the purpose of buying and selling personal data.²⁶ As we all know, there was a social debate about personal photos (Ghozali) and the sale of KTPs. This confirms that the legal culture is out of sync, so the government's role in legal education becomes clear. At the local community level in the Sei Panas area, Batam City, for instance, the author took the initiative to conduct interviews with the community members. Meetings were held with various community groups as well as local sub-district representatives. The author sought opinions using a questionnaire method specifically addressing the issue of selling personal data in relation to NFTs.²⁷ However, to the author's surprise, the community members seemed confused and unaware of the specific case mentioned. Many individuals were unfamiliar with the existence of the Personal Data Protection (PDP) Law, which was enacted several years ago. The author's efforts had to be halted due to the discouragement expressed by the community, as they lacked an understanding of the concept of personal data protection.

Essentially, legal education is carried out in order to produce good citizens, one of which is legal awareness.²⁸ According to Soekanto, legal awareness is an assessment of existing laws and laws that should exist. Furthermore, Soerjono Soekanto said about the indicators of legal awareness as follows:²⁹ 1) Knowledge of legal regulations (law awareness); 2) Knowledge of the contents of legal regulations (law acquisition); 3) Attitude towards legal regulations (Legal attitude); and 4) Patterns of legal behavior.

Legal education plays a crucial role in cultivating responsible and informed citizens who possess legal awareness. Soekanto defines legal awareness as the evaluation of existing laws and the recognition of laws that should be in place. Additionally, Soerjono Soekanto identifies several indicators of legal awareness, which include: 1) Knowledge of legal regulations (law awareness): Individuals should have a basic understanding of the laws that govern their society; 2) Knowledge of the contents of legal regulations (law acquisition): It is important for individuals to be familiar with the specific provisions and contents of legal regulations; 3) Attitude towards legal regulations (legal attitude): Developing a positive and respectful attitude towards legal regulations helps foster a culture of compliance and respect for the law; 4) Patterns of legal behavior: Individuals should exhibit behaviors that align with legal norms and follow the established legal procedures. By incorporating these indicators

²⁶ Tng, A., & Disemadi, H. S. (2023). Investasi dan Transaksi di Marketplace Non-Fungible Token: Peluang dan Risiko Hukum. *Halu Oleo Law Review*, 7(1), 129-148.

²⁷ Yongkie, Y., & Disemadi, H. S. (2022). Non-Fungible Tokens as Jurisdictionless Innovation: Legal Vacuum, Loopholes, Potentials and Solutions. *Widya Yuridika: Jurnal Hukum*, 6(1), 157-174.

²⁸ Fitriasari, S. Pentingnya Pendidikan Hukum bagi Warga Negara Indonesia. *JURNAL CIVICUS*, 10(2), 1-9.

²⁹ Soerjono, S. (1993). *Mengenal Sosiologi Hukum*, Jakarta: Rajawali Pers.

into legal education, individuals can develop a comprehensive understanding of the law and its significance in society, leading to the formation of responsible and law-abiding citizens.

Incorporating legal education on personal data protection into various subjects within the school education curriculum, such as citizenship education, culture, and professional ethics (at the higher education level), is an effective approach. Additionally, the implementation of legal education through direct socialization and the utilization of online media presents a viable solution that involves not only formal education institutions but also students and the government. Massive community service initiatives can be undertaken to further support this endeavor. The positive impact of comprehensive legal education extends beyond knowledge enhancement, influencing facilities, infrastructure, and, notably, legal culture, thus raising public awareness about the critical importance of safeguarding personal data.

CLOSING

The significance of legal education in the realm of personal data protection becomes evident when considering the prevention of personal data transactions on non-fungible token (NFT) sites within marketplace platforms. In light of ongoing technological advancements, it is imperative to engage in extensive public education efforts that encompass diverse segments of society. Despite the implementation of Law Number 27 of 2022 concerning the Protection of Personal Data, its effectiveness alone is inadequate in effectively addressing the issue of personal data transactions on NFT sites. The safeguarding of personal data has emerged as a critical concern for the state, government bodies, users of Non-Fungible Token (NFT) platforms, and other internet platforms. It is crucial for individuals to adopt a more vigilant and conscious approach to protecting their personal data, beginning with themselves. This objective can be substantially facilitated through legal education initiatives, which may manifest in the form of outreach activities involving both governmental and non-governmental entities. These initiatives can include the active participation of students and academics who offer counseling services to the community.

BIBLIOGRAPHY

- Amboro, F. Y. P., & Puspita, V. (2021). *Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia)*. In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, 1, (1), 415-427.
- Anggraeni, S. F. (2018). *Polemik Pengaturan Kepemilikan Data Pribadi: Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia*. *Jurnal Hukum & Pembangunan*, 48(4), 814-825.
- Cukie, K. (2010). *Data Everywhere*. <https://www.economist.com/special-report/2010/02/27/data-data-everywhere> (diakses pada 15 Maret 2023, pukul 10.30 WIB)
- Deviyanti, P.A.S. (2017). *Tuntutan Ganti Rugi Penggunaan Data Pribadi Surat Elektronik Menurut Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Universitas Udayana: Skripsi S1 Fakultas Hukum.

- Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, 5(2), 177-199.
- Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, 24(2), 289-304.
- Djafar, W. (2017). Big Data Dan Praktik Pengumpulan Data Skala Besar Di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi. *Jakarta: Elsam*.
- Fitriasari, S. Pentingnya Pendidikan Hukum bagi Warga Negara Indonesia. *JURNAL CIVICUS*, 10(2), 1-9.
- Kurniawan, Y., Santoso, S. I., Wibowo, R. R., Anwar, N., Bhutkar, G., & Halim, E. (2023). Analysis of Higher Education Students' Awareness in Indonesia on Personal Data Security in Social Media. *Sustainability*, 15(4), 3814.
- Marzuki, P.M. (2010). *Metode Penelitian Hukum*. Jakarta: Kencana Prenada.
- Newswire. (n.d.). Ini Bahaya Yang Bisa Terjadi Bila Data Pribadi Kita Bocor. <https://www.solopos.com/ini-bahaya-yang-bisa-terjadi-bila-data-pribadi-kita-bocor-1126609> (diakses pada 18 Maret 2023, pukul 19.07 WIB).
- Prameswati, V., Sari, N. A., & Nahariyanti, K. Y. (2022). Data Pribadi Sebagai Objek Transaksi di NFT pada Platform Opensea. *Jurnal Civic Hukum*, 7(1).
- Pratana, I. W. A. W. (2021). Urgensi Pengaturan Mekanisme Pemanfaatan Data Pribadi Dalam Rancangan Undang-Undang Perlindungan Data Pribadi. *Jurnal Hukum Lex Generalis*, 2(8), 701-721.
- Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.com). *Borneo Law Review*, 5(1), 46-68.
- Raihan, M. (2023). Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). *Jurnal Inovasi Penelitian*, 3(10), 7847-7856.
- Rizki, R., & Gultom, E. R. (2023). Differences in Data Protection Systems in Indonesia And Singapore. *Indonesian Journal of Law and Policy Studies*, 3(2), 150-159.
- Rosadi, S. D., Noviandika, A., Walters, R., & Aisy, F. R. (2023). Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?. *International Review of Law, Computers & Technology*, 37(1), 78-90.
- Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 369-384.
- Shahrullah, Rina, Syarief, Elza, AND Crystina Aprilia. " Pemberlakuan Aturan Hukum Pajak Terhadap Youtuber dan Penjual Online Shop " *Journal of Law and Policy Transformation (Online)*, Volume 4 Number 2 (20 December 2019)
- Soerjono, S. (1993). *Mengenal Sosiologi Hukum*, Jakarta: Rajawali Pers.

- Supriyadi, D. (2023). The Regulation of Personal and Non-Personal Data in the Context of Big Data. *Journal of Human Rights, Culture and Legal System*, 3(1), 33-69.
- Tan, D. (2021). Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum. *Nusantara: Jurnal Ilmu Pengetahuan Sosial*, 8(8), 2463-2478.
- Tng, A., & Disemadi, H. S. (2023). Investasi dan Transaksi di Marketplace Non-Fungible Token: Peluang dan Risiko Hukum. *Halu Oleo Law Review*, 7(1), 129-148.
- Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, 2(3), 654-666.
- Weley, N. C., & Disemadi, H. S. (2022). Implikasi Hukum Pemasangan CCTV di Tempat Umum secara Tersembunyi terhadap Perlindungan Data Pribadi. *Amnesti Jurnal Hukum*, 4(2), 79-93.
- Yongkie, Y., & Disemadi, H. S. (2022). Non-Fungible Tokens as Jurisdictionless Innovation: Legal Vacuum, Loopholes, Potentials and Solutions. *Widya Yuridika: Jurnal Hukum*, 6(1), 157-174.