Justitia Jurnal Hukum, 9 (2), 2025: 205-215
ISSN: 2579-9983, E-ISSN: 2579 6380
DOI: 10.36501/justitia.v1i2.

Ensuring Legal Protection of Personal Data in Indonesia's Digital Identity System

Rizky Dwi Priyantiwi
Universitas 17 Agustus 1945 Surabaya, Indonesia
email: rzkydwipryntiwi@gmail.com

Hufron
Universitas 17 Agustus 1945 Surabaya, Indonesia
email: hufron@untag-sby.ac.id

Abstract

Personal data is a person's privacy right that must be protected from various aspects of life. Many people are deceived regarding falsified electronic ID cards, both data falsification and falsification using other people's data. The state is obliged based on its constitutional rights to provide legal protection for various aspects of the lives of Indonesian citizens. The purpose of this study is to determine and analyze the urgency of legal protection for personal data of digital population identity owners as a privacy right in Indonesia and to determine and analyze the concept of legal protection for personal data of digital population identity owners as a privacy right in Indonesia. This type of research is normative legal research. The results of the study obtained that the urgency of legal protection for personal data of digital population identity owners (Digital ID Cards) includes protecting privacy rights and human rights, preventing misuse of personal data, building a safe and trusted digital ecosystem, impacts on social life and diversity, and ensuring legal certainty. The concept of legal protection for digital population identity holders (Digital ID Cards) is by implementing Law Number 11 of 2020 concerning Electronic Information and Transactions (ITE Law), Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection in Electronic Systems, regulation of personal data protection in sectors, supervision and sanctions, public awareness campaigns, development of data security frameworks, and international cooperation.

Keywords: Legal Protection, Personal Data, ID card, Privacy Rights

INTRODUCTION

Every citizen holds constitutional rights, fundamental liberties safeguarded by law. In recognizing these rights, the state simultaneously inherits a constitutional duty: to protect its people. This responsibility is clearly stated in the Preamble (UUD 1945), particularly in the fourth paragraph. It affirms that the state must safeguard all Indonesians, promote the general welfare, cultivate an educated and enlightened society, and contribute to a global order founded on independence, peace, and social justice. Development technology information and communication show quite an improvement significant. Increase quality Indonesian society as a whole sustainable

that utilizes technology information as well as knowledge knowledge is one of objective development national at a time become a global challenges (Priscyllia, 2019) Progress technology information and communication is increasingly rapid cause change behavior as well as pattern think without recognized by the Indonesian people as well as global society. (Arrasuli & Fahmi, 2023).

The internet, or interconnected networks, serves as a powerful platform for a wide range of activities, both positive and diverse, offering services and products in various sectors. These include e-commerce (online trade and business), (learning), (healthcare), (public administration), (financial services), as well as innovations in transportation, tourism, and the growing field of cloud computing. Cloud computing services, such as Google Drive, iCloud, Dropbox, and YouTube, allow users to store data securely and access it remotely (Kurniawan et al., 2022). The Big Indonesian Dictionary, personal data refers to information that identifies or reflects an individual's unique characteristics, such as their name, age, gender, education, occupation, home address, and familial role. This notion aligns with the legal definition found in Article 1, paragraph (1) of the Permen 20 of 2016. The regulation defines personal data as any information about an individual that must be securely stored, carefully managed, and kept confidential. Moreover, Article 2 of the same regulation broadens this protection by requiring safeguards across every phase of personal data handling from the moment it is obtained and collected, through its processing and storage, to its eventual usage, transmission, and even destruction. This comprehensive approach underscores the principle that personal data protection is not just a technical requirement, but a critical aspect of respecting and upholding individual privacy rights.

In order to save budget government related service administration population, issued Regulation Government Regulation No. 109 of 2019, namely arrange provision about printing document population certificate birth certificate death, card family, letter move No Again use blank, society can print independent use HVS colored paper white 80 grams and can be printed independent. Efforts to reduce cost the Director General Population and Registration Civil The Ministry of Home Affairs implements Identity Digital Population. Concept from identity digital population is public No need own physical electronic ID card However Enough only with application population installed on smartphones. (Trisna & Meirinawati, 2023) Electronic ID card is document population that contains system security / control Good from side administration or technology information with based on population database national with objective For realize ownership One identity (KTP) for One residents who have code security and recording electronic population data based on NIK nationally (biodata, photos, fingerprints) fingers, iris and marks hand) stored in Electronic KTP physical form. Validity UU 23 of 2006 with objective For to materialize orderly administration population in scale national and guarantee certainty law right civil residents, also for interests of national development programs, so that required population data update, publication Number Parent Population (NIK) and the implementation of electronic KTP.

Electronic Population Identification Card is very vulnerable and frequently used documents done forgery and abuse. Many people are deceived related to forged electronic ID cards Good data falsification or forgery using other people's data. from 2019 to May 2024, there were a total of 124 cases suspicion violation personal data protection. Of the total of these, 111 cases is personal data leaks. (Sinaga & Putri, 2020)

Data breaches are highly susceptible to misuse, potentially leading to serious criminal activities like identity theft and fraud issues that have become more pressing in today's rapidly developing digital economy. In this digital age, personal data is a crucial asset for businesses, especially as the creative economy continues to expand (Fikri & Alhakim, 2022). According to data from Norton, the potential for criminal activity in Indonesia's online space has reached an emergency level, with risks showing a concerning upward trend, as reported by Id-SIRTII/CC.

The increasing number of personal data breaches highlights the vulnerability of Indonesian citizens' privacy, making it clear that misuse of this data poses significant risks to society. Moreover, personal data violations aren't limited to breaches alone; they can also stem from irresponsible handling of personal information. For instance, when personal data is used for unauthorized sales or exchanges without a legitimate basis. In the context of UU 36 of 1999, while there are provisions regarding the general protection of personal data, they do not explicitly address it in a detailed manner. Article 42, (1) of the Telecommunications Law emphasizes that telecommunication service providers must maintain the confidentiality of information transmitted by their customers. This legal obligation ensures that service providers must secure all information sent or received through their telecommunications network or services.

Criminal acts that arise consequence spread some personal data happen Good in network (online), for example fraud committed through social media, computing cloud (*cloud computing)* or outside network, for example personal data collection in a way mass (*digital dossier)*, marketing direct selling, and *so* on. (Benuf et al., 2019) With the occurrence misuse of personal data, then Can known in a way direct about weakness system and its weaknesses supervision so that his personal data misused, thing this is what can cause loss material and immaterial for data owner. Misuse, theft and sale of personal data is A action oppose law that utilizes technology and information and can also classified as abuse on right basic human beings. On the basis of this, research This will answer and give understanding to public wide will importance role Constitution about personal data protection in Indonesia. (Fikri & Alhakim, 2022) Article 26 Paragraph (1) is the only one article with clear confirm personal data protection must carried out. The ITE Law also regulates about prohibited acts related with field information electronics that are not in a way specific in personal data that is in Article 27 to with Article 37. In general articles the forbid existence action without rights and with on purpose abuse information electronics that can harming others especially owner information.

Indonesia has not yet own regulation legislation special that regulates protection personal data law that can become solution in various type related cases with misuse of personal data. Absence rule special in arrangement personal data protection in Indonesia so that set on several regulation legislation that regulates No in a way comprehensive emphasize on the principles from data protection (Kusnadi & Wijaya, 2021)· Based on description above, then become important For to study in a way deep issue related laws with personal data protection specifically related to electronic ID cards. So that researcher interested For lift title" Legal Protection of Personal Data Owner Identity Digital Population"

Research conducted by (Umi Mutiara & R. Maulana, 2020) discusses how personal data protection is part of human rights that must be guaranteed by the state. The research emphasizes the human rights aspect and the need for national law to immediately establish personal data protection regulations. Research conducted by

T.D. Purnama & A. Alhakim, 2022). This research focuses on the importance of specific regulations regarding personal data amidst the increasing number of data breaches on digital platforms. This research analyzes the urgency and challenges of implementing the Personal Data Protection Law.

Personal data protection in Indonesia is still relatively new when compared to international practices, especially the European Union through the General Data Protection Regulation (GDPR). The regulation puts forward the principles of lawfulness, fairness, and transparency which requires every data controller to guarantee the rights of the data owner, including the right to access, correct, and delete personal data. GDPR also emphasizes the accountability principle, where the electronic system organizer is fully responsible for every form of data processing, including if a leak occurs. The sanctions given within the framework of GDPR are very strict, with administrative fines that can reach 20 million Euros or 4% of the company's total annual revenue globally. This is different from Indonesia which has just had Law Number 27 of 2022 concerning Personal Data Protection, whose implementation is still in the transition stage and faces challenges in law enforcement, including limited resources of law enforcement officers and public awareness (Purnama & Alhakim, 2022).

In addition, several ASEAN countries have also adopted more mature data protection regulations. For example, Singapore with the Personal Data Protection Act (PDPA) 2012 has first established an obligation for organizations to obtain consent before collecting or using personal data. Malaysia through the Personal Data Protection Act (PDPA) 2010 also provides relatively strict protection, especially in a commercial context. This comparison shows that Indonesia needs to accelerate the harmonization of regulations with international standards in order to ensure the security of its citizens' personal data, especially in the face of cross-border threats in the era of global digitalization.

From a victimology perspective, personal data leakage can cause real losses for data owners, both in the form of economic losses (fraud, identity theft, credit card abuse), and non-economic losses such as insecurity, psychological pressure, and loss of trust in digital services. Data owners often become double victims, namely suffering direct losses due to leakage as well as difficulties in obtaining recovery (remedies) due to the weak accountability mechanism from the electronic system organizer. In addition, in the framework of modern criminal law, the leakage of personal data can also be associated with corporate criminal liability. Electronic system providers, both private companies and government agencies, can be held accountable if they are proven to be negligent or deliberately leave the system unsafe, causing data leakage. This principle is in line with the doctrine of corporate criminal liability, where corporations are not only civilly responsible, but can also be subject to criminal sanctions in the form of fines, restrictions on business activities, and even dissolution if proven to endanger the public interest. Thus, the criminal aspect of the corporation is important to be integrated into the Indonesian data protection system, so that the electronic system operator has a strong legal incentive to protect the user's personal data.

Based on the above description, it is important to thoroughly examine the legal issues related to personal data protection, particularly regarding electronic ID cards (e-

KTP). Therefore, the researcher is interested in developing the title "Legal Protection of Personal Data of Digital Population Identity Holders."

METHODS

This type of research is normative legal research.(Ariawan, 2013) In this normative legal research, researchers conduct research on legal principles, starting from existing law. This research uses a statutory approach, which is carried out by examining all laws and regulations related to the legal issue being addressed, and a conceptual approach, which is an approach that starts from the views and doctrines that have developed within legal science. The legal materials obtained include primary legal materials, secondary legal materials, and tertiary legal materials. The primary legal materials in this study include the 1945 Constitution of the Republic of Indonesia, Law Number 23 of 2006 concerning Population Administration which has been amended into Law Number 24 of 2013 concerning Population Administration, Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 1 of 2023 concerning the Criminal Code, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 39 of 1999 concerning Human Rights, Government Regulation No. 82 of 2012 concerning Electronic System and Transaction Organizers, Regulation of the Minister of Home Affairs Number 72 of 2022 concerning Standards and Specifications for Hardware, Software, and Electronic Identity Card Forms and the Implementation of Digital Population Identity. Secondary legal materials include scientific works from legal circles, books, journals, jurisprudence. As well as tertiary legal materials include the Big Indonesian Dictionary, Legal Dictionary, the internet and others. The collection of these legal materials was carried out using library research methods which were then analyzed using descriptive analysis. This research uses juridical normative analysis with a comparative approach and a critical approach. Comparative analysis is used because this study discusses how legal protection in Indonesia is applied to personal data, then assesses it with other more advanced regulations such as the European Union GDPR or regulations in other ASEAN countries. By comparing, researchers can find the strengths and weaknesses of the Indonesian legal system, and offer a more effective model. Meanwhile, the critical approach is also important because the issue of data protection is not only about written legal norms, but also concerns the gap between regulation and practice weak law enforcement, and losses suffered by the community as victims of data leakage. Hermeneutic analysis can complement, but its nature is more on the interpretation of legal texts, so that in this study it is more appropriately positioned as an aid. Thus, the combination of comparative analysis and critical approach provides a more comprehensive foundation to examine the effectiveness of personal data legal protection in Indonesia.

DISCUSSION AND RESULT

Criminal acts of bribery in the PPPK case in Langkat Regency

In this case, the criminal act committed by the bribe giver to the bribe recipient with the aim of being approved/accepted as a Government Employee with a Work Agreement (PPPK) Teacher in Langkat Regency is categorized as bribery because the

act of offering or giving money to a state official to influence a decision that will benefit oneself or another person is a criminal act of bribery and is punishable by law.('Arafa, 2018) One form of bribery that is often committed is giving a sum of money to an influential person for the sake of one's own interests and desire to obtain something beneficial. In this study, the author examines a bribery case that occurred in Langkat Regency, namely the PPPK teacher bribery case. This bribery case involved officials, namely the Head of the Langkat Regency Education Office, the Head of the Regional Civil Service Agency, and the School Principal as the recipients of the bribe, while the perpetrators of the bribery were the participants of the 2023 PPPK Teacher test.

Urgency Legal Protection of Personal Data Owner Identity Digital Citizenship as a Right to Privacy In Indonesia

Legal protection of the personal data of digital population identity card (Digital ID Card) holders is crucial as it constitutes a fundamental privacy right stipulated in the 1945 Constitution of the Republic of Indonesia. This is not only about maintaining data confidentiality, but also about preventing misuse and ensuring individual security in the digital age.(Widodo et al., 2024) The Personal Data Protection Law serves as a legal basis for protecting individuals' rights to their personal data.

The right to privacy is a right inherent in every individual. It represents the dignity of every individual that must be protected. Personal data is data relating to a person's characteristics, name, age, gender, education, occupation, address, and family status. Personal data is a sensitive matter for everyone. Personal data is a person's right to privacy that must be protected in various aspects of life. The reason the right to privacy must be protected in building relationships with others, a person must conceal parts of his or her personal life so that he or she can maintain a certain level of position. Privacy is a right that stands alone and is not dependent on other rights, but this right will be lost if the person publishes personal matters to the public.

Another reason why privacy deserves legal protection is because the harm suffered is difficult to quantify. The harm is felt to be far greater than physical harm, as it disrupts a person's private life. Therefore, if any harm is suffered, the victim is obliged to receive compensation. Data protection implies that individuals have the right to determine whether or not to share or exchange their personal data. Furthermore, individuals also have the right to determine the conditions under which such personal data will be transferred. Furthermore, privacy protection. The right to privacy has evolved to be used to formulate the right to protect personal data. Personal data protection emphasizes that everyone has the right to determine their own destiny, such as whether or not to share data. If data sharing occurs, they also have the right to determine the conditions that must be met within a community (Hanafi & Lubis, 2023).

Personal data protection in Indonesia has several differences and similarities with other countries, particularly the European Union's General Data Protection Regulation (GDPR). Indonesia's Personal Data Protection Law adopts international standards such as the Convention and the GDPR, but there are some differences in the details of the regulations and enforcement mechanisms. Indonesia's Personal Data Protection Law focuses on protecting citizens' personal data, both within and outside Indonesia. It regulates the rights of data subjects, the obligations of data controllers and processors, and international data transfers. Meanwhile, in the European Union (GDPR), it applies to all EU member states, with broader coverage and more detailed

principles, including "by design" and "by default" data protection, as well as robust oversight mechanisms.

Many other countries, such as Singapore, Malaysia, Thailand, and other Asian countries, also have their own Personal Data Protection Laws, although the level of protection and enforcement mechanisms may vary. With the Personal Data Protection Law, Indonesia has a strong legal framework for protecting personal data. However, effective implementation and enforcement are key to ensuring that personal data protection objectives are achieved.

Based on the explanation above, the author provides a concluding analysis that the relationship between the theory of legal protection and the urgency of protecting privacy rights is closely interrelated, because legal protection aims to protect human rights, including the right to privacy, from violations. Protection of privacy rights is important because it is a basic right of every citizen guaranteed in the constitution. In addition, the theory of legal purposes also emphasizes that laws are created to achieve certain goals, such as justice, order, and social welfare. In the context of legal protection of privacy rights in Indonesia, the urgency is very great because the right to privacy is a fundamental human right and must be protected so that people can live safely and peacefully. And finally, the theory of legal benefits emphasizes achieving the greatest benefit for the greatest number of people, which in the context of privacy, means that strong privacy protection will provide greater social benefits, such as trust, security, and economic development. Effective privacy protection prevents the misuse of personal data, protects human dignity, and creates a safe and productive digital environment.

Draft Legal Protection of Personal Data Owner Identity Digital Citizenship as a Right to Privacy In Indonesia

Personal data, by its very nature, is increasingly vulnerable to misuse and privacy violations. The security of such data is not merely a technical issue but a fundamental human right that must be respected and safeguarded. In Indonesia, despite being a developing country experiencing rapid technological adoption, there remains a considerable gap in effectively protecting personal data as an extension of the right to privacy (Mutiara & Maulana, 2020). This gap has become especially urgent given the growing number of privacy violations and the widespread misuse of personal information. As the digital landscape expands, it is imperative for every nation, including Indonesia, to establish and enforce comprehensive legal frameworks that defend the privacy rights of its citizens.

In recent years, Indonesia has begun to recognize the critical importance of protecting personal data, particularly with the exponential rise of internet usage and digital platforms. The 1945 Constitution of the Republic of Indonesia explicitly acknowledges the right to personal protection. Article 28G, Paragraph (1), asserts that every individual is entitled to the security of their person, family, honor, dignity, and possessions. However, in the face of rapid advancements in information and communication technology, the interpretation of these rights must evolve beyond the constitutional text. Privacy today is not just a legal formality but a core aspect of personal identity—an intrinsic right that demands heightened recognition in digital interactions (Niffari, 2020).

In our increasingly digital world, the principle of privacy in relation to personal data has become more vital than ever. Daily interactions with technology often involve

the voluntary or automatic sharing of sensitive data—ranging from names, addresses, and contact details to financial records, health histories, and biometric identifiers. While this exchange facilitates convenience, it also heightens exposure to data misuse and potential breaches of privacy (Rosadi, 2009).

The ultimate aim of privacy protection is to uphold human dignity and individual freedoms by ensuring that personal data is processed responsibly, ethically, and transparently. This responsibility applies not only to private corporations but also to government agencies and any institutions handling data. The notion of privacy as a right—sometimes referred to as the "right to be left alone"—was famously articulated by Warren and Brandeis in their groundbreaking Harvard Law Review article, *The Right to Privacy*. Their work laid the foundation for understanding privacy as an essential component of human autonomy, particularly in an age where technological innovation continues to push the boundaries of personal space (Makarim, 2010).

In Indonesia, individuals have the legal freedom to decide whether to protect or share their personal data a right enshrined in national legislation. This constitutional guarantee affirms that Indonesian citizens are entitled to the protection of their private information. The state, in turn, bears the responsibility of ensuring that legal protections cover various dimensions of life, upholding the principles of justice, legal clarity, and societal benefit.

To address these obligations, Indonesia has taken several steps to enhance its personal data protection framework. (ITE Law) includes specific provisions aimed at securing personal data in digital systems. Under this law, electronic data controllers are mandated to safeguard user information, with penalties imposed for breaches of privacy. Complementing this is the draft of a dedicated Personal Data Protection Law, which, although not yet passed, reflects the government's growing commitment to strengthening data privacy. Additionally, the Ministry of Communication and Information Regulation No. 20 of 2016 outlines the principles and procedures for handling personal data within electronic systems. Sector-specific regulations have also been implemented, particularly in critical areas such as banking, healthcare, and telecommunications. For instance, Bank Indonesia has established strict rules to ensure the confidentiality of customer data. Beyond regulation, the government plays a supervisory role over entities that collect and process personal data, with authority to issue sanctions for violations.

To support these legal and regulatory efforts, Indonesia also engages in public education campaigns aimed at raising awareness about digital safety and responsible data sharing. At the organizational level, steps are being taken to develop frameworks and best practices for securing personal data. Furthermore, Indonesia has begun participating in international cooperation efforts to align its data protection standards with global norms, demonstrating a clear intention to foster a secure and rights-respecting digital environment for all.

If the owner data Identity Digital Population (IKD) leaks, then owner must quick report it to the Population and Registration Service Local Civil Service (Dukcapil) or to The Republic of Indonesia Police (Polri) through office police closest or service online complaints are available. In addition, the owner Identity Population can also report it to the Ministry of Communication and Information (Kominfo) if data leak occurred in the system electronics managed by the government. The following is Steps you can take:

1. Report to the Dukcapil Service, report incident the to the Civil Registry Office place owner identity population registered. They have authority For handle problem population and can give help related data recovery or action prevention more carry on.
2. Report to Police, if owner identity population suspect has happen act criminal related data leak, aka can quick report to party police. They will do investigation and prosecution to perpetrator crime cyber.
3. Report to Kominfo, if data leak occurred in the system government - managed electronics, owners identity population as well can report it to Kominfo. They have authority For do action supervision and enforcement to problematic system.

As outlined in Article 46, Paragraph (1) UU 27 of 2022, "If a personal data breach occurs, the Personal Data Controller must issue a written notification to the affected Personal Data Subjects and relevant institutions within 3 x 24 hours." Therefore, once the breach is confirmed, the Surabaya City Government, as the Personal Data Controller, must notify the impacted individuals within this timeframe. This notification is part of the broader oversight of electronic systems, which falls under the authority of the Ministry of Communication and Information, as specified in Article 35 of PP 71 of 2019.

Government moment This specifically government area Already make an effort For realize that Identity Population This can walk as should be, and in fact government of course has succeed implement Identity Population the will but in matter This government Not yet give guarantee certainty security and assurance certainty law to user Identity Population Guarantee certainty security and assurance certainty law is One aspect very important Because precisely in carry out system recording administration government No may neglect security public special regarding personal data. So that moment this is very much needed regulations that can made into as runway government For determine attitude if there is incident which harm user Identity Population specifically if happen a personal data leak user Identity Population. Government must prepare step preventive and repressive to user Identity population.

Based on description explanation above, the author give analysis conclusion that connection between theory protection law with draft protection law against personal data owner identity digital population as right privacy in Indonesia is mutual related Because theory This give base law For protect right privacy, including personal data. Protection law give runway for society and government For organize and ensure right privacy, including personal data, is respected and protected. In addition theory objective the law also emphasizes protection right basic humanity and justice, have connection close with draft protection law against personal data as right Privacy in Indonesia. Personal data protection considered as an integral part of right privacy, which is right basic human beings who must protected. Legal purposes for protect rights basic humans, including privacy, to be runway main in effort arrangement law against personal data. And finally namely theory benefit law (utilitarianism) in context protection law against personal data as right Privacy in Indonesia emphasizes benefits the biggest for the largest number of people. This means that the law personal data protection must designed for give benefit most for public in a way overall, while also considering rights individual in guard privacy they.

CONCLUSION

The urgency of legal protection for the personal data of digital identity card holders (Digital ID Cards), among other rights, includes protecting privacy and human rights, protecting private data, building a secure and trustworthy digital ecosystem, its impact on social life and diversity, and ensuring legal certainty. The relationship between the theory of legal protection and the urgency of protecting privacy rights is closely intertwined, as legal protection aims to protect human rights, including the right to privacy, from violations. Protecting privacy rights is crucial because it is a fundamental right of every citizen, guaranteed by the constitution. 2. The concept of legal protection for digital population identity holders (Digital ID Cards) is implemented through Law Number 11 of 2020 concerning Electronic Information and Transactions (ITE Law), Minister of Communication and Information Regulation Number 20 of 2016 concerning Personal Data Protection in Electronic Systems, sectoral regulations on personal data protection, supervision and sanctions, public awareness campaigns, development of a data security framework, and international cooperation.

The President and the House of Representatives (DPR) can revise the Population Administration Law (Law No. 24 of 2013) by adding a special chapter or article on IKD, explicit rules regarding the definition, function, rights, and obligations of IKD owners, as well as clarity regarding the legal status of digital data and the recognition of IKD as an official identity tool equivalent to a physical KTP. In addition, the President through the Ministry of Home Affairs and the Ministry of Communication and Information must develop a national IKD literacy program that targets the general public, ASN, and public service operators and explains the rights, risks, and how to use IKD safely. The proposal to strengthen legal protection for Digital Population Identity (IKD) owners should be carried out through two regulatory channels, namely the addition of Articles in the Population Administration Law (Law No. 23 of 2006 in conjunction with Law No. 24 of 2013) and adjustments/revisions to the Minister of Home Affairs Regulation No. 72 of 2022, so that the revision suggestions focus on adding articles in Chapter V-A (regarding IKD).

REFERENCES

'Arafa, M. A. (2018). White-collar crimes, corruption and bribery in Islamic criminal law: Lacuna and conceivable Paths. *Rule of Law and Anti-Corruption Center Journal*, *2018*(1), 3.

Ariawan, I. G. K. (2013). Metode Penelitian Hukum Normatif. *Kertha Widya*, *1*(1).

Arrasuli, B. K., & Fahmi, K. (2023). Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi. *UNES Journal of Swara Justisia*, *7*(1), 369–392.

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145–160. https://doi.org/10.24246/jrh.2019.v3.i2.p145-160

Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *Yustisi*, *9*(1), 1–13.

Hanafi, I., & Lubis, A. F. (2023). Protection of Privacy and Intellectual Property Rights in Digital Data Management in Indonesia. *The Easta Journal Law and Human Rights*, *2*(01), 33–40.

Kusnadii, ekaring A., & Wijaya, A. U. (2021). Perlindungan Hukum Data Pribadi

Sebagai Hak Privasi. *Al WASATH Jurnal Ilmu Hukum Volume*, *2*(1), 9–16.

Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi dalam Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 1–5. https://doi.org/10.29303/jatiswara.v34i3.218

Purnama, T. D., & Alhakim, A. (2022). Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *8*(1), 273–283.

Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi 4.0. *Jurnal RechtVinding*, *9*(2), 237–256.

Trisna, E., & Meirinawati, M. (2023). Analisis Penerapan Standar Pelayanan Publik Pembuatan KTP-el (Kartu Tanda Penduduk Elektronik) di Dinas Kependudukan dan Pencatatan Sipil (Dispenduk Capil) Kota Surabaya. *Publika*, 1461–1474.

Widodo, J. E., Suganda, A., & Darodjat, T. A. (2024). Data Privacy And Constitutional Rights In Indonesia: Data Privacy And Constitutional Rights In Indonesia. *PENA LAW: International Journal of Law*, *2*(2).