



Reconceptualization of Population Data as a Human Right under Indonesian Positive Law

Ana Aniza Karunia^{1*}, Mohammad Jamin², Adriana Grahani Firdausy³

Universitas Sebelas Maret Surakarta, Indonesia

Corresponding Author: Ana Aniza Karunia anaanizak3@student.uns.ac.id

ARTICLE INFO

Keywords: Population Data, Data Protection, Human Rights, Sui Generis Rights

Received : 23 March 2026

Revised : 27 April 2026

Accepted: 28 May 2026

©2026 Karunia, Jamin, Firdausy: This is an open-access article distributed under the terms of the [Creative Commons Atribusi 4.0 Internasional](https://creativecommons.org/licenses/by/4.0/).



ABSTRACT

The rapid digitalization of public services has significantly increased the use of population data as a key instrument in governance, public services, and development planning. However, this expansion also raises serious concerns regarding the legal status and protection of such data. This study aims to analyze the nature of population data. Using a normative legal research method with statutory, conceptual, and historical approaches, this research relies on secondary data obtained through documents study. The findings show that population data constitute personal data inherent to individuals, derived from life events, and closely related to identity, privacy, and human dignity. At the same time, it is managed by the state and utilized for public interests, placing it in a sui generis position, both personal and public in nature. The increasing economic utilization of population data further intensifies the tension between public interest and privacy protection. This study concludes that strengthening legal foundations, harmonizing regulations, and developing a comprehensive data protection system are essential to ensure that the use of population data remains aligned with the protection of human rights, particularly the right to privacy.

INTRODUCTION

The continuous growth of information and communication technology in the digital era has significantly reshaped many areas of human life. One of the implications of the development is the increasing intensity of interactions between individuals and information services providers (<https://dinpendukcapil>, 2025). A wide range of fields has increasingly adopted digital systems to facilities and enhance their activities, including within the sphere of public administration (Mohammad, 2025). The steady integration of digital technologies has reshaped the way the state performs its functions, including through the advancement of governance processes into a more digital based system. Digitalization in government is understood as a transformative process aimed at improving efficiency, effectiveness, and the quality of public services (Disdukcapil Banyumas, 1954). Various academic studies indicate that the implementation of digitalization in government contributes to improving governance. Panggabean and Meilani, in their academic study, explain that government digitalization, realized through the development of digital, based public serviced, has brought significant changes to governance practices (Directorate General of Taxes, 2022).

The digitalization of public services refers to the process of converting information or data from physical forms into digital formats, enabling their management and utilization through information technology. This process is expected to support the delivery of public services that are more effective, efficient, and transparent, while also expanding the scope of interaction between government and society (Disdukcapil Tegal, 2023). Moreover, digitalization is directed at providing accurate and timely information to stakeholders as part of efforts to achieve better governance systems. Through digitalization, the government has the opportunity to deliver public services in a more coherent and coordinated manner, thereby minimizing the potential for duplication of work and unnecessary bureaucratic complexity. The digitalization of public services also supports the implementation of transparency and accountability principles in governance. This is intended to enhance public trust in state institutions (Dinpendukcapil Buleleng, 2018). In its development, the digitalization of public services has encouraged the state to extensively utilize population data across sectors as a key supporting instrument in efforts to improve the quality of public services (Tempo Administrator, 2024).

Population data serves a strategic role as the basis for identifying and verifying individuals in the delivery of various public services. Its utilization can enhance data accuracy, minimize identity errors, and prevent duplication and identity fraud. In addition to accelerating administrative processes, the use of integrated population data contributes to increasing public trust in government, provided services (Administrator of the Directorate General of Population and Civil Registration, 2025). Currently, the utilization of population data has been widely implemented across various public service sectors. It is used, among others, for the issuance of driver's licenses (Ditjen Dukcapil, 2025), business permits (Disdukcapil Soppeng, 2025), taxpayer services (Fadhilla & Nina, 2022), banking services (Nadeak, 2014), land certificate issuance, insurance services,

public health coverage (Jaya, 2021), and employment social security (Law No. 24, 2013). In addition, population data is also utilized to verify the identity of prospective spouses, ensuring the accuracy of population data and marital status, thereby effectively preventing identity fraud and discrepancies in marital status during the marriage administration process (Constitution of Indonesia, 1945). As of now, the number of users granted access to utilize population data has reached 7.360. These users include ministries, non-ministerial government agencies, law enforcement institutions, as well as sectors such as education, healthcare, banking, capital markets, insurance, payment services, transportation services, cooperatives, financing institutions, and mobile telecommunications services providers. In addition, population data is also utilized by various other users, including commodity futures trading providers, electronic signature providers, fintech financial services, tax application service providers, zakat services, pawnshop services, and user institution at the regional level (ELSAM, 2020).

Population related information refers to records administered by the Directorate General of Population and Civil Registration, derived from the documentation of demographic occurrences and significant life events experienced by individuals (House of Representatives of the Republic of Indonesia, 2023). These events include births, deaths, marriages, divorces, adoption, as well as other events that affect an individual's legal status and population administration (Tommy and Nasution, 2025). Each population and vital event is reported by residents to the implementing agency to be recorded and processed in the Population Administration Information System (SIAM) (Soemartono, 2017). The data collected and managed in SIAM is what is subsequently referred to as population data and is utilized for various purposes in the administration of government (Sutikno and Stiawan, 2022). Thus, population data essentially originates from events that occur throughout an individual's life as a legal subject. Therefore, population data contains personal and sensitive information, as it reflects identity and life dynamics that are directly attached to the individual. This nature of population data makes it not merely an administrative instrument, but also part of an individual's private sphere that deserves legal protection. Such characteristics of population data give rise to fundamental legal issues, particularly concerning the clarity of its legal status.

Within the framework of national law, Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 on Population Administration places population data under state control through the Directorate General of Population and Civil Registration as the authority responsible for the issuance, management, storage, and utilization of such data. However, this regulation doesn't explicitly clarify the legal status of population data, particularly regarding its nature and the relationship between the state's authority as the data manager and citizens' rights as the owner of the data (Nugraha, 2025). This regulatory ambiguity creates uncertainty in the practical use of population data. On the one hand, the state has the authority to manage and utilize population data to support public services, development planning, and other public interests (Sugiyono, 2019). On the other hand, population data originated from the personal life events of citizens and contains information inherently attached to

the individual, thereby giving citizens a legitimate interest in obtaining protection over such data (Renggong et al, 2021). This condition reflects a tension between the state's authority in managing population data and citizens' interests in protecting data that is directly related to their private lives. This tension has intensified alongside the increasingly, widespread, massive, and cross-sectoral use of population data in the era of public service digitalization, which simultaneously raises the risk of data misuse and breaches. As the statutory level, this issue fundamentally stem from a more basic problems, namely the absence of a clear constitutional foundation regarding the right to be protection of population data. From a constitutional perspective, the 1945 Constitution of the Republic of Indonesia, through Article 28 G paragraph (1), guarantees every person the right to protection of their personal self, family, honor, dignity, and property under their control, as well as the right to a sense of security and protection from threats of fear to act or not act, which constitutes a human right (Universal Declaration of Human Rights, 1948). However, the Constitution doesn't explicitly regulate the right to population data. as a standalone right. This absence of explicit norms raises a fundamental legal question regarding how the right to protection of population data should be interpreted and positioned within the framework of human rights recognized and guaranteed by the 1945 Constitution of the Republic of Indonesia. This lack of regulatory clarity has implications for the weak normative protection of population data in its implementation. When the right to the protection of population data is not affirmed as an integral part of human rights, data governance tends to be viewed merely as an administrative and technical matter, rather than as a constitutional obligation of the state to protect citizens' rights. Such ambiguity in regulation and interpretation contributes to the weak protection of population data, as reflected in the increasing number of data breach cases in recent years.

In 2020, approximately 2.300.000 records of Indonesian citizens' population data, originating from the General Elections Commission (KPU) website in 2021, were reported to have been leaked and shared on a hacker community forum. The leaked data included full names, National Identification Numbers (NIK), Family Card Numbers, full addresses, places and dates of birth, ages, and gender. Subsequently, in 2021, 279.000.000 records of Indonesia citizens' population data, comprising full names, National Identification Numbers (NIK), phone numbers, email addresses, and residential addresses, originating from BPJS Kesehatan were leaked and sold on a hacker forum known as "Raid Forums" (ICCPR, n.d). A similar incident occurred again in 2023, when as many as 337.225.465 population data records originating from the Directorate General of Population and Civil Registration were reported to have been sold on the dark web. The leaked data included National Identification Numbers (NIK), full name, dates of birth, birth certificate numbers, blood types, religion, marital status, marriage and divorce certificate numbers, dates of marriage and divorce, physical conditions, disability status, last education level, type of occupation, mother's NIK, father's NIK, mother's full name, and father's full name (ECHR, n.d.). In 2024, Indonesian experienced a major cyberattack on the Temporary National Data Center (PDNS) 2, carried out by the Brain Cipher group, part of the Lock Bit

3.0 ransomware variant. The attack began on June 17, 2024, when security systems were disabled, allowing hackers to shut down services and damage critical systems (American Convention on Human Rights, n.d.). Population data breaches have significant impacts, not only disrupting public services but also triggering various forms of misuse, such as fraud, illegal online loan applications, identity forgery, and the unauthorized dissemination of personal data. This indicates that data breaches aren't merely technical issues, but also pose threats to public security and undermine trust in the government's ability to protect data, particularly amid rapid digitalization.

Various academic studies also show that population data serves a crucial role in the delivery of public services. It functions not only as an administrative identity for citizens, but also as a basis for policymaking, public services provision, and the integration of government services systems. However, as its utilization increases across sectors, the risk of data breaches has also risen and has occurred in several government institutions. Research by Triyuni Soemartono emphasizes that population data, as an official form of identity, is a fundamental element in ensuring effective and efficient public service delivery (Cairo Declaration on Human Rights in Islam, n.d.). Meanwhile, research by Tole Sutikno and Deris Stiawan reveals data breach incidents involving public officials' data and data from the Komisi Pemilihan Umum, indicating that Indonesia's population data management and protection systems still face serious challenges. These findings show that the government has not yet fully established adequate data security systems to protect population data from unauthorized access (ASEAN Human Rights Declaration, n.d.). Furthermore, research conducted by Dimas Aditya identifies several factors contributing to data breaches, including weak access control, low levels of cybersecurity awareness and education, suboptimal implementation of international security standards, and vulnerabilities in information technology infrastructure. These factors indicate that population data breaches aren't only caused by technical weaknesses, but also by issues of governance and institutional capacity in managing data securely and responsibly (Michael, 1994). Unlike previous studies that primarily focus on the technical and empirical aspects of data breaches, this research specifically examines the conceptual and normative aspects of the legal status of population data and how it should be protected. Accordingly, this study is expected to contribute both theoretically and normatively for clarifying the true nature of population data in the context of public interest and the state's obligation to ensure the protection of citizens' right over their population data.

LITERATURE REVIEW

The rapid expansion of digital governance and electronic public services has significantly increased the strategic importance of population data within contemporary state administration. Population data functions not only as an administrative instrument for identifying citizens but also as a fundamental resource supporting public service delivery, development planning, taxation, banking, healthcare, social security, law enforcement, and various digital government initiatives. The extensive utilization of population data has generated new legal concerns regarding its ownership, legal status, protection

mechanisms, and relationship with fundamental human rights. Although Indonesian law regulates population administration through Law Number 24 of 2013 concerning Population Administration and provides general personal data protection through Law Number 27 of 2022 concerning Personal Data Protection, uncertainty remains regarding the precise legal nature of population data and the extent to which it should be protected as a constitutional right.

The discussion concerning the protection of personal information is closely related to the broader development of privacy rights within modern constitutional and human rights frameworks. Privacy has evolved from a traditional concept protecting personal and family life into a broader legal principle encompassing informational privacy and personal data protection. International human rights instruments, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, recognize protection against arbitrary interference with privacy and personal information. Consequently, the increasing dependence of governments on digital databases has intensified scholarly debate regarding the balance between public interests in data utilization and individual rights to privacy, autonomy, and informational self-determination.

Previous studies have emphasized the strategic role of population data in supporting public administration and public services. Soemartono (2017) explains that population data serves as an essential instrument for ensuring effective and efficient public service delivery by providing accurate citizen identification and facilitating administrative coordination among government institutions. Similarly, Sutikno and Stiawan (2022) argue that integrated population databases contribute significantly to governmental efficiency and policy implementation by enabling data interoperability across sectors. These studies demonstrate the importance of population data as a public administrative resource. Nevertheless, their analyses primarily focus on administrative effectiveness and technological implementation rather than examining the normative legal status of population data itself.

Academic attention has also been directed toward the growing risks associated with population data utilization. Aditya (2023) identifies several factors contributing to population data breaches, including weak cybersecurity infrastructure, inadequate access control mechanisms, insufficient public awareness regarding data security, and limited institutional capacity in managing digital information. Likewise, ELSAM (2020) highlights the increasing vulnerability of population databases due to extensive cross-sectoral data sharing practices involving government institutions, financial services, healthcare providers, and private sector entities. These findings indicate that population data is exposed to significant risks of misuse, unauthorized access, identity theft, and cybercrime. However, existing studies generally analyze these problems from technical and governance perspectives without comprehensively addressing their constitutional and human rights implications.

The legal dimension of personal data protection has also attracted considerable scholarly discussion. Rosadi (2022) argues that personal data protection constitutes an integral element of privacy rights recognized under

international, regional, and national legal systems. Similarly, Michael (1994) emphasizes that privacy protection encompasses not only physical and personal autonomy but also control over information relating to an individual's identity and personal life. The Constitutional Court of Indonesia has further recognized personal data protection as part of the constitutional right to privacy. These studies establish a strong theoretical foundation for treating personal information as a protected legal interest. Nevertheless, they primarily discuss personal data in general terms and provide limited analysis regarding the distinctive legal characteristics of population data administered by the state.

Several scholars have further examined the relationship between state authority and individual rights in the management of personal information. Nugraha (2025) observes that the Population Administration Law places population data under state control without explicitly clarifying the legal relationship between citizens as data subjects and the government as data manager. Sugiyono (2019) similarly notes that population data occupies a complex position because it is collected and utilized for public interests while simultaneously containing sensitive personal information belonging to individual citizens. Renggong et al. (2021) further argue that this dual character creates tension between governmental authority and individual privacy protection. These studies reveal the existence of conceptual ambiguity regarding the legal status of population data. However, they do not formulate a comprehensive legal framework capable of reconciling both dimensions.

Contemporary scholarship increasingly acknowledges that population data possesses characteristics that differ from ordinary personal data and conventional property rights. Several studies suggest that population data originates from life events such as birth, marriage, divorce, and death, making it inseparable from an individual's identity and legal existence. At the same time, population data serves essential public functions that require state management and utilization. This dual character challenges traditional legal classifications that treat rights as either purely private or purely public. Despite these observations, existing literature has not adequately developed a theoretical framework explaining the unique legal position of population data within Indonesian positive law.

Although previous studies have discussed public service administration, privacy rights, personal data protection, cybersecurity risks, and state authority over population information, most of them examine these issues separately and from fragmented perspectives. Existing scholarship generally focuses either on administrative effectiveness, technological security, privacy protection, or regulatory governance. Limited attention has been devoted to conceptualizing population data as a distinct legal category that simultaneously embodies elements of personal rights, public interests, and constitutional protection. Furthermore, there remains a lack of integrated analysis connecting population administration law, personal data protection law, constitutional rights, and human rights principles within a unified legal framework.

Accordingly, a significant research gap exists regarding the reconceptualization of population data as a human right under Indonesian

positive law. This study seeks to fill that gap by analyzing the legal nature of population data, examining its relationship with privacy rights and constitutional guarantees, and proposing a conceptual framework that recognizes population data as a *sui generis* right possessing both personal and public dimensions. The novelty of this research lies in its effort to position population data not merely as an administrative resource managed by the state but as a human rights object requiring comprehensive legal protection, thereby strengthening the constitutional foundation of privacy rights and improving the legal protection of citizens in the era of digital governance.

METHODOLOGY

The research adopts a normative legal research approach. It seeks to comprehensively examine the nature of population data from a human rights perspective and the current legal framework governing its protection in ensuring human rights. The approaches used in this study include the statutory, historical, and conceptual approaches. The statutory approach is conducted by reviewing and assessing the consistency and conformity of legal provisions related to the nature of population data and its regulatory framework. Meanwhile, the conceptual approach analyses doctrines and views of scholars on human rights, the right to data protection, and the right to privacy, in order to formulate the essence of population data in ensuring the fulfilment of human rights. This study uses secondary data sources. The data collection technique employed is document study, which involves gathering information from books, archives, documents, numerical records, and images in the form of reports and supporting materials (Halstead, 2009). The process includes collecting, identifying, and reviewing all legal provisions related to the nature of population data and its legal protection. The analysis is conducted using qualitative methods, combining data processing and analysis through legal interpretation and inductive reasoning, focusing on all legal provisions concerning the nature of population data from a human right perspective and its legal protection framework.

RESEARCH RESULT

On the other hand, recent regulations indicate a shift, where population data is also viewed as an object with economic value through the mechanism of Non Tax State Revenue (PNBP). This has the potential to shift the function of data from individual protection toward a source of state revenue, thereby creating tension between the state's economic interests and the right to privacy (Population Administration Law, 2006).

From a human rights perspective, personal data is inherently attached to the individual and inseparable from their identity and dignity. This principle is affirmed in various international instruments, such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which guarantee the protection of privacy, including personal information (Personal Data Protection, 2022). In Indonesia, this concept is reflected in the regulation of population data and personal data, although different terms are used. Substantively, both remain data derived from an individual's life and must be protected. From a property rights perspective, there is a mismatch, as

population data can't be treated like an object that can be freely transferred or exploited. Although it is inherently attached to individuals, in practice it is often treated as an object with economic value, creating an imbalance between privacy protection and its utilization. This condition shows that population data occupies a unique position, it is neither fully a property right nor entirely a privacy right. Therefore, population data is more appropriately understood as a *sui generis* right, a special type of right that is personal in nature because it is attached to the individual, yet managed by the state and capable of economic utilization.

DISCUSSION

Human rights are fundamental entitlements that every person possesses since birth, which the state is obligated to uphold, safeguard, and ensure their realization. Among these rights, the right to privacy holds a fundamental position, encompassing the protection of one's personal life, family, home, communications, and personal information from arbitrary or unlawful interference. This right has been widely recognized and firmly established in various international human rights instruments (Law Number 39 of 1999 on Human Rights, 1999). In the Universal Declaration of Human Rights, Article 12 affirms that everyone has the right to protection against interference with their privacy, family, home, correspondence, as well as their honour and reputation (Michael, James R, 1994). This provision is further reinforced in the International Covenant on Civil and Political Rights through Article 17, which obliges states not only to protect but also to prevent all forms of privacy violations (Constitutional Court Decision Number 5/PUU-VIII/2021, 2021). In addition, the protection of privacy is also regulated in various regional instrument, such as the European Convention on Human Rights (Rights and Europe, 2018), the American Convention on Human Rights (Rosadi, Sinta Dewi, 2022), the Cairo Declaration on Human Rights in Islam (Banking Law, 1998), and the Asean Human Rights Declaration (Telecommunications Law, 1999). All these instrument essentially affirm that privacy encompasses personal life, family, home, communication, and personal information, and must be protected from unlawful interference.

Substantively, privacy encompasses the protection of personal space, the freedom to make decisions, as well as control over one's data and identity (Consumer Protection Law, 1999). Therefore, the state has two primary obligations: to refrain from interfering with privacy (negative obligation) and to provide effective legal protection against any violations (positive obligation) (Population Administration Law, 2006). Over time, the concept of privacy has evolved beyond the protection of personal life to include the protection of personal data, particularly in response to advances in information technology. In this context individuals have the right to control information about themselves, including determining whether such data may be collected, used, or disclosed. Data protection thus concerns not only confidentiality, but also ensuring that data is processed fairly, has a clear legal basis, and is not used in a discriminatory manner.

In Indonesia, the right to privacy has essentially received constitutional recognition through Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which guarantees protection of personal self, family, honour, dignity, and property (Personal Data Protection Law, 2022). This provision is further reinforced in Law Number 39 of 1999 on Human Rights, which affirms that every person has the right to personal protection (OECD Privacy Guidelines, n.d.). Although it isn't explicitly referred to as the "right to privacy", this provision essentially reflects the protection of individual privacy. This right to privacy includes several important aspects, namely the right to be free from interference in one's personal life, the right to control the use of one's personal data by others. In this context, individuals aren't merely objects of data, but also subjects who have control over their own data (Council of Europe Convention 108, n.d.). In addition, the Constitutional Court has affirmed that the protection of personal data is part of the right to privacy, which is included within human rights. This protection covers various aspects, such as personal information, family, home, communication, honour, and reputation. This indicates that personal data protection isn't merely an administrative matter, but also an integral part of human rights protection (European Union Data Protection Directive, n.d.).

In international legal instruments, personal data is understood as information relating to an identified or identifiable individual, including professional activities as well as information about their public life. This means that such information is connected to a person whose identity is either clearly established or can be determined through additional information (GDPR, n.d.). In international legal instruments, personal data is understood as information relating to an identified or identifiable individual, including professional activities as well as information about their public life. This means that such information is connected to a person whose identity is either clearly established or can be determined through additional information (Personal Data Protection Act Singapore, n.d.). Thus, the identification process requires elements that can describe a person so that they can be distinguished from others and recognized as an individual. For example, a phone number written on a piece of paper without any additional information is merely ordinary data. However, if the same paper includes the phone number along with the name of its owner, it becomes personal data. A phone number on its own can't be considered personal data because it can't be used to identify its owner. In contrast, when a phone number is accompanied by the owner's name, the information can directly identify the individual concerned. Therefore, the combination of a phone number and its owner is categorized as personal data (Personal Data Protection Act No, 2010). As another example, a person's name isn't always unique, therefore, identifying an individual often requires additional attributes to avoid confusion with others who have similar names. In some cases, both direct and indirect attributes need to be combined to ensure accurate identification of an individual as the subject of the information. Date and place of birth are commonly used for this purpose. In addition, many countries implement personal identification

numbers to distinguish each citizen more accurately in various administrative processes (Personal Information Protection Act, n.d.).

In Indonesia, the regulation of personal data initially developed in a sectoral manner and lacked a clear definition. Several laws, such as those in the banking (Types and Affairs, 2023), telecommunications (UDHR, n.d.), and consumer protection sectors (Dukcapil, 2013), only regulated information confidentiality in a limited way without providing a comprehensive concept of personal data. In practice, this situation created the potential for data misuse, for example, the use of consumer data for promotional purposes without consent. This indicates that personal data, such as phone numbers and addresses, is part of privacy that should be protected. More explicit regulation began to emerge with Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 on Population Administration, which defines personal data as certain individual data that must be kept confidential, including sensitive data such as biometrics and personal conditions (safeguard, and realization, n.d.). However, this regulation remains limited to the population administration sector. The diversity of these sectoral regulations shows that Indonesian didn't yet have an integrated legal framework for personal data protection. Therefore, Law Number 27 of 2022 on Personal Data Protection was enacted as an overarching framework to provide more comprehensive protection and legal certainty for the public (Constitution, 1945).

Law Number 27 of 2022 on Personal Data Protection describes personal data as any information relating to an individual whose identity can be determined, whether directly or indirectly, including when such information is combined with other data (manner and definition, 2013). This definition aligns with various international standards that broadly view personal data as any information that can lead to the identification of a person. Such alignment can be seen in several international instruments, including the OECD Privacy Guidelines (Personal Data Protection Law, 2022), Council of Europe Convention 108 (Personal Data Protection, 2022), European Union Data Protection Directive (individual et al., n.d.), and the General Data Protection Regulation (GDPR) (Law Number 39 of 1999 on Human Rights, 1999). Similar regulations are also found in the Personal Data Protection Act *Singapura* (Population Administration Law, 2013), Personal Data Protection Act No. 709 of 2010 (Personal Data Protection, 2010), and the Personal Information Protection Act (61), all of which essentially affirm that personal data includes any information relating to an individual, whether directly or indirectly identifiable, including through digital identity characteristics. These regulations also emphasize that personal data doesn't have to be factually accurate, as long as it can lead to the identification of an individual. Even data that doesn't directly identify a person or has been processed, such as pseudonymized data, remains classified as personal data if it can still be linked back to a specific individual.

Law Number 27 of 2022 on Personal Data Protection divides personal data into two main groups, namely specific personal data and general personal data. Specific data refers to sensitive information, including details related to health conditions, biometric identifiers, genetic, financial, and children's data, which

may pose serious risks if misused. Meanwhile, general data includes basic information such as name, gender, and marital status, as well as other that can identify an individual (Telecommunications Law, 1999). In the context of population administration, population data constitutes part of personal data derived from significant life events, such as birth, marriage, and death, which are then recorded in national system. This data consist of various identity elements, including the National Identification Number (NIK), which is unique and attached to an individual for life, enabling accurate identification. Due to its identifying nature, population data serves an important role in various sectors, such as public services, development, and law enforcement. However, this also indicates that population data is essentially personal data directly related to an individual's identity and private life, and therefore must be protected (Consumer Protection Law, 1999).

CONCLUSIONS AND RECOMMENDATIONS

The conclusion of this study is the nature of population data that constitutes part of personal data inherent to the individual, derived from life events, and directly related to identity, privacy, and human dignity. Such data can't be treated as an ordinary object of property, as it can't be transferred and remains attached to the individual. However, in practice, it is managed by the state and utilized for public interests. Therefore, population data possesses a *sui generis* character, it is personal because it is attached to the individual, and at the same time public because it is managed by the state and has utilitarian value. Accordingly, its management must ensure the protection of the right to privacy

Recommendation

The recommendations of this study is necessary to strengthen the legal foundation for the protection of population data by affirming its status as part of human rights, including through reinforcing constitutional norms and harmonizing the Population Administration Law with the Personal Data Protection Law, so that the *sui generis* nature of population data can be consistently recognized and protected.

REFERENCES

- Administrator of the Civil Registration Office of Banyumas. Utilization of Population Data. <https://dindukcapil.banyumaskab.go.id/news/19542/pemanfaatan-data-kependudukan>
- Administrator of the Civil Registration Office of Buleleng. BPJS Kesehatan Optimizes the Use of e-KTP Card Readers. <https://disdukcapil.bulelengkab.go.id>
- Administrator of the Civil Registration Office of Tegal. Banking Services. <https://disdukcapil.tegalkab.go.id>
- Administrator of the Directorate General of Population and Civil Registration. Cooperation between Dukcapil and Bimas Islam. <https://dukcapil.kemendagri.go.id>

- Administrator of the Directorate General of Taxes. Integration of Population and Tax Data Towards the Implementation of NIK as NPWP. <https://pajak.go.id/en/node/81216>
- American Convention on Human Rights.
- ASEAN Human Rights Declaration.
- Atmasasmita, R. Rekonstruksi Asas Tiada Pidana Tanpa Kesalahan. Gramedia Pustaka Utama. (2017).
- Beni Ahmad Saebani and others, Metode Penelitian Hukum Pendekatan Yuridis Normatif. (2021).
- Cairo Declaration on Human Rights in Islam.
- Constitutional Court Decision Number 5/PUU-VIII/2021.
- Council of Europe Convention 108.
- Directorate of National Population Data Integration. Evaluation Report on Population Data Utilization. (2025).
- European Convention on Human Rights (ECHR).
- European Union Agency for Fundamental Rights and Council of Europe. Handbook on European Data Protection Law. Publications Office of the European Union. (2018).
- European Union Data Protection Directive.
- Faisal and others, 'Genuine Paradigm of Criminal Justice: Rethinking Penal Reform within Indonesia New Criminal Code', Cogent Social Sciences, 10.1 (2024).
- Fitriyono, R. A. Kebijakan Formulasi Hukum Pidana Dalam Melindungi Transaksi e-Commerce Di Indonesia. Penerbit NEM. (2023).
- General Data Protection Regulation (GDPR).
- Government Regulation Number 10 of 2023 on Types and Tariffs of Non-Tax State Revenue Applicable to the Ministry of Home Affairs.
- Halstead, Peter. Unlocking Human Rights. Routledge. (2009).
- Hartanti, Erni. Aspek Pidana Dalam Tindak Pidana Korporasi. Sinar Grafika. (2023).
- International Covenant on Civil and Political Rights (ICCPR).
- Jeffrey Luther, 'Twenty-First Century Financial Regulation: P2P Lending, Fintech, and the Argument for a Special Purpose Fintech Charter Approach', University of Pennsylvania Law Review, 168.4 (2020), 1013-1059.
- Khakan Najaf, Ravichandran K. Subramaniam, and Osama F. Atayah, 'Understanding the Implications of FinTech Peer-to-Peer (P2P) Lending during the COVID-19 Pandemic', Journal of Sustainable Finance and Investment, 12.1 (2022), 87-102.
- Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 on Banking.
- Law Number 23 of 2006 concerning Population Administration.
- Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 on Population Administration.
- Law Number 27 of 2022 on Personal Data Protection.
- Law Number 36 of 1999 on Telecommunications.

- Law Number 39 of 1999 on Human Rights.
- Law Number 8 of 1999 on Consumer Protection.
- Manik, S. Budi. *Perlindungan Konsumen: Tinjauan Filosofis Dan Sosiologis*. Universitas Airlangga Press. (2021).
- Mawardi, Achmad. *Hukum Siber Dan Perlindungan Konsumen Di Era Digital*. Setara Press. (2021).
- Michael, James R. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*. UNESCO. (1994).
- Mohd, Y. D., Dkk. *Hukum Perlindungan Konsumen*. (2024).
- Nabila Aulia Rahma, Adi Fauzanto, Keri Pranata, *Responsive Law System Of Financial Technology: Upaya Rekonstruksi Konsep Penyelesaian Sengketa Peer-To-Peer Lending*. (2019).
- Nasihuddin, A. A. *Teori Hukum Pancasila*. Elvaretta Buana. (2024).
- OECD Privacy Guidelines.
- Otniel Yustisia Kristian, 'Perlindungan Hukum Pengguna Layanan Fintech P2P Lending Dari Tindak Pidana Ekonomi Dan Terhadap Penyedia Layanan Fintech P2P Lending Illegal', *Majalah Hukum Nasional*, 52.2 (2022), 297–320.
- Personal Data Protection Act No. 709 of 2010.
- Personal Data Protection Act Singapore.
- Personal Information Protection Act.
- Renggong, Ruslan, and Dyah Aulia Rachma Ruslan. *Human Rights in the Perspective of National Law*. Kencana. (2021).
- Romli Atmasasmita. *Sistem Peradilan Pidana: Perspektif Eksistensialisme Dan Abolisionisme*. Mandar Maju. (2020).
- Rosadi, Sinta Dewi. *Privacy Data Aspects under International, Regional, and National Law*. PT Refika Aditama. (2022).
- Ryan Randy Suryono, Indra Budi, and Betty Purwandari, 'Detection of Fintech P2P Lending Issues in Indonesia', *Heliyon*, 7.4 (2021), e06782.
- Sipghotulloh Mujaddidi, 'Constionality of Human Right Limitation on Constitutional Court Decisions', *Jurnal Konstitusi*, 18.3 (2021), 539–607.
- Tempo Administrator. *Continuing Collaboration, BPJS Ketenagakerjaan and Dukcapil Utilize IKD*. <https://www.tempo.co>
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.
- Universal Declaration of Human Rights. (1948).
- Zaenal Arifin and others, 'Peran Otoritas Jasa Keuangan Dalam Pengawasan Jasa Layanan Keuangan Berbasis Financial Technology Peer to Peer Lending', *Jurnal Usm Law Review*, 6.2 (2023), 712–723.
- Zaidan, M. A. *Menuju Pembaruan Hukum Pidana*. Sinar Grafika. (2022).