Al-Zayn: Jurnal Ilmu Sosial & Hukum e-ISSN 3026-2917
https://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZyn p-ISSN 3026-2925
Volume 3 Number 5, 2025
DOI: https://doi.org/10.61104/alz.v3i5.2445

Recognition of Digital Identity as a Legal Subject in the Era of Digital Transformation

Bagus Gede Ari Rama
Faculty Of Law, Universitas Pendidikan Nasional[1]
Email Korespondensi : arirama@undiknas.ac.id

Article received: 15 September 2025, Review process: 25 September 2025
Article Accepted: 10 Oktober 2025, Article published: 18 November 2025

ABSTRACT
The development of digital technology has transformed the way individuals are identified and recognized in modern legal systems through the emergence of digital identities. This study formulates two main issues: the legal status of digital identities in the Indonesian legal system and the form of legal protection provided to digital identity holders against potential misuse of personal data. This study uses a normative legal research method with a statutory and conceptual approach. The primary legal materials used include the 1945 Constitution, Law Number 1 of 2024 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Regulation of the Minister of Home Affairs Number 72 of 2022 concerning Digital Population Identity. The analysis was conducted deductively by examining the theory of legal protection, the principle of legality, and the concept of legal personhood in the digital context. The results of the discussion indicate that digital identities have received normative recognition as part of an individual's legal status. However, the effectiveness of legal protection remains weak due to the suboptimal implementation of the principles of transparency, accountability, and data security by electronic system administrators.
Keywords: *Digital Identity, Legal Protection, Personal Data, Privacy Rights*

ABSTRAK
Perkembangan teknologi digital telah mengubah cara individu diidentifikasi dan diakui dalam sistem hukum modern melalui hadirnya identitas digital. Penelitian ini merumuskan dua masalah utama, yaitu kedudukan hukum identitas digital dalam sistem hukum Indonesia dan bentuk perlindungan hukum yang diberikan kepada pemilik identitas digital terhadap potensi penyalahgunaan data pribadi. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan konseptual. Bahan hukum primer yang digunakan antara lain Undang-Undang Dasar 1945, Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dan Permendagri Nomor 72 Tahun 2022 tentang Identitas Kependudukan Digital. Analisis dilakukan secara deduktif dengan menelaah teori perlindungan hukum, asas legalitas, dan konsep kepersonaan hukum dalam konteks digital. Hasil pembahasan menunjukkan bahwa identitas digital telah memperoleh pengakuan normatif sebagai bagian dari status hukum individu. Namun, efektivitas perlindungan hukum masih lemah karena penerapan prinsip transparansi, akuntabilitas, dan keamanan data oleh penyelenggara sistem elektronik belum optimal.
Kata Kunci: *Identitas Digital, Perlindungan Hukum, Data Pribadi, Hak Privasi*

INTRODUCTION

The development of information technology has brought about major changes in the way humans interact, work, and carry out their legal activities. The shift of human activities to the digital space demands a new form of identity that can replace the role of conventional identity. Digital identity is now an important element in various online activities such as electronic transactions, public services, and administrative activities that require the validity and authentication of individual identities. The existence of digital identity is not just a technical tool, but a legal representation of a person in cyberspace that has implications for legal rights, obligations, and responsibilities.(Utomo et al., 2025) This phenomenon signifies a paradigm shift in the concept of legal personality which has only been recognized in physical form, towards the recognition of a person's digital existence.

In the context of national law, the regulation regarding the existence of digital identities is not yet fully comprehensive. Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 (ITE Law) provides a legal basis for the validity of electronic information and electronic signatures. Article 5 paragraph (1) of the ITE Law states that electronic information and/or electronic documents are valid legal evidence, while Article 11 provides recognition of electronic signatures as a means of authentication and identity verification. This provision shows that Indonesian law has provided recognition of the digital aspect of legal relations, but this recognition is still limited to proof and has not touched on the aspect of the legal status of the digital identity itself. Furthermore, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) affirms the obligations of the state and business actors in protecting individual personal data. Article 2 of the PDP Law emphasizes the principle of legitimacy and accountability in the processing of personal data, which implicitly contains protection against forms of digital identity. (Roselin & Putra, 2025). However, there is no norm that explicitly establishes digital identity as a legal subject that has its own legal rights and responsibilities.

This not ideal legal condition is exacerbated by the reality on the ground which shows a high vulnerability to misuse of personal data. The case of large-scale personal data leaks has become a fact that cannot be ignored. Based on reports from various trusted national media, in 2024 there will be a data leak of 4.6 million West Java residents which includes NIK, names, and full addresses. (Puspasari, 2025). A similar case also occurred in prepaid SIM card registration data which reached more than 1.3 billion user data. (Clinten & Wahyudi, 2022). This leak shows the weak protection system for citizens' digital identities that should be guaranteed by the state. Not only that, fraud modes that use the pretext of activating Digital Population Identity (IKD) are also rampant. The perpetrator pretended to be an official officer of the Population and Civil Registration Office (Disdukcapil) to obtain people's personal data through short messages or instant messaging applications. (Mutaqin et al., 2024) These facts show that existing legal policies have not been able to provide effective protection for digital identities as a form of a person's legal existence in cyberspace.

The government's efforts to build a national digital identity system through the Digital Population Identity (IKD) program should be appreciated, because it is the first step towards digital-based public service transformation. The program allows people to access various government services using a mobile-based application without the need for physical documents. In addition, the government through the Ministry of Communication and Information Technology together with GovTech Indonesia and Perum Peruri is preparing a *national Digital ID* system that is integrated with public services through the *single sign-on* platform (INA-Pass). (Zahra et al., 2024). However, the policy is not yet fully accompanied by a strong legal framework regarding legitimacy and responsibility for the use of digital identities. The absence of a firm regulation regarding the legal position of digital identities has the potential to cause legal uncertainty when data misuse, cybercrimes, or disputes involving digital identities occur.

From the perspective of legal theory, the fundamental question arises about whether digital identity can be categorized as a legal subject. In the doctrine of civil law, the subject of law includes the human being as *a natural person* and a legal entity as *rechtspersoon*, both of which have legal rights and obligations. (Robles-Carrillo, 2024). In digital developments, digital identities often act as a representation of individuals in carrying out legal acts such as signing electronic documents, online financial transactions, and submitting public services. (Babel et al., 2025). These representations have legal consequences, because actions taken by digital identities can have real legal consequences. When abuse or infringement occurs, legal accountability becomes blurred because there is no clarity on whether digital identity is treated as a recognized legal tool, evidence, or entity. (Vardanyan, Hamuľák, & Kocharyan, 2024). This ambiguity has implications for the effectiveness of legal protection for individuals whose digital identities are used without permission, as well as raises questions about the position of digital identity in Indonesia's positive legal system.

The gap between technological development and legal adaptation is a serious challenge for the national legal system. Article 28D paragraph (1) and Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia affirm the right of every citizen to personal protection, legal certainty, and security. (Priyantiwi, 2025). Thus, constitutionally the state has an obligation to provide equal protection for the existence of individuals, both in the real and digital worlds. However, until now, there has been no arrangement that gives full legitimacy to a person's digital existence. (Darnela & Rusdiana, n.d.). The absence of clear norms has the potential to result in violations of citizens' rights, especially in the context of personal data protection, electronic transactions, and the legality of legal acts carried out digitally. This emphasizes the importance of discussing the position of digital identity in the national legal system and the urgency of its legal recognition.
Based on this description, the formulation of the problem in this study is focused on two main problems. First, what is the position of digital identity in Indonesia's national legal system in the midst of an ever-growing digital transformation? Second, what is the urgency of recognizing digital identity as a legal subject who

has legal rights and obligations in order to realize certainty and legal protection for citizens in the digital space.

METHODS

This study uses normative legal methods with a focus on the study of legal norms and concepts that govern digital identity in the Indonesian legal system. The approaches used include a legislative approach and a conceptual approach. (Syahputra, 2024). The legislative approach is carried out by examining the provisions in the 1945 Constitution of the Republic of Indonesia, Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 1 of 2024, Law Number 27 of 2022 concerning Personal Data Protection, as well as derivative regulations such as Permendagri Number 95 of 2019 and Permendagri Number 72 of 2022. Meanwhile, a conceptual approach is used to examine the notion of legal subjects, legal personality, and the protection of digital identities according to legal doctrine. The legal materials used include primary, secondary, and tertiary materials, obtained through literature studies and qualitatively analyzed to find clarity on the position of digital identity in the national legal system.

RESULTS AND DISCUSSION

The Position of Digital Identity in the Indonesian Legal System

The development of digital technology has brought about fundamental changes in the way the law views human identity. If previously a person's identity was only tied to physical aspects and administrative documents such as ID cards or passports, now this identity has transformed into a digital form consisting of personal data and electronic attributes that represent the existence of individuals in cyberspace. Digital identity includes various elements such as Population Identification Number (NIK), biometric data, email addresses, and online activity traces used in authentication and electronic transactions. (Chanidia & Rahmayani, 2025). Thus, digital identity is not just a product of technology, but a new manifestation of a person's legal existence in the digital world, as it determines the rights, obligations, and responsibilities of individuals in cyberspace. (Demkin, 2024). These changes demand that the national legal system not only recognize the existence of digital identities, but also provide legal legitimacy and protection commensurate with traditional forms of identity.

In a constitutional context, the recognition of digital identity has a strong legal basis. Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees everyone's right to personal protection, honor, and security, while Article 28H paragraph (4) guarantees the right to fair legal recognition and protection. (Mahameru et al., 2023). These two provisions form the constitutional basis for the protection of digital identities as part of human rights that the state must guarantee. Further regulation at the legal level reinforces that recognition. Law Number 11 of 2008 concerning Information and Electronic Transactions, which has been amended last by Law Number 1 of 2024, provides a legal basis for the enactment of electronic information and electronic documents as evidence and legal

means. (Lahangatubun & Muliyono, 2025). Meanwhile, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) stipulates that personal data is part of the constitutionally guaranteed privacy rights and must be protected by the state. (Rahayuana & Octarina, 2025). At the administrative level, Permendagri Number 72 of 2022 concerning Standards and Specifications for Digital Population Identity (IKD) is the government's concrete step in legitimizing digital identity as an official authentication instrument in the population system and public services. (Sihombing et al., 2025). Through these regulations, digital identities get a strong legal basis and gain status as part of national legal instruments.

In the perspective of legal theory, the position of digital identity can be explained through the concepts of legal personality and legal representation. According to Hans Kelsen and H.L.A. Hart, the subject of law is an entity that is given the capacity by the norm system to have rights and obligations. (Romero, 2023). Digital identity does not stand as a new legal subject, but is an extension of the human legal subject represented in the form of data. (Englezos, 2023). This means that the validity of actions carried out through digital identity depends on normative recognition in the legal system. When a digital identity is issued and regulated by the state such as in an IKD system or certified electronic signature it acquires legal legitimacy as an official representation of a person in the digital space. Thus, the existence of digital identities in the Indonesian legal system is derivative, it is legitimate because of the recognition of norms, not because of the existence of technology.

In terms of legal principles, the principle of legality is the main basis that emphasizes that every action or legal status must have a clear legal basis. The recognition and use of digital identity is only valid if it is based on applicable norms and can be legally tested. The implementation of Permendagri Number 72 of 2022 and the PDP Law is a concrete form of applying this principle because both provide a legal framework for the issuance, storage, and use of digital identities by the public. (Sasongko, 2023). However, the principle of legal protection is also an important aspect in assessing the extent to which the state guarantees the security and rights of citizens to their digital identities. Legal protection, as stated by Satjipto Rahardjo, must be realized in the form of a sense of security and real legal certainty for each individual. (Harahap & Tanjung, 2024). In the digital context, such protection includes the security of personal data, supervision of data processing, and the right of individuals to delete or restrict data in accordance with the provisions of Articles 9–16 of the PDP Law. (Rahman, 2025). Unfortunately, the implementation of this principle of legal protection still faces serious obstacles in the field.

Empirical facts show that even though normatively regulated, legal protection of digital identities is still weak. Data from Tempo in 2024 recorded a number of large-scale data leaks in Indonesia, including BPJS Kesehatan data, prepaid SIM registration, and KPU permanent voter data, which were spread on online forums and even traded on the digital black market. (Salam & Prasetya, 2024). Kompas also reported the weak law enforcement mechanism against

personal data protection violations, especially in the private sector which often uses user data without explicit consent. (Saptohutomo, 2024. This phenomenon shows the gap between legal norms and practice in the field, as described by Roscoe Pound in the theory of *law in action*, that the effectiveness of law is not measured by its existence in the text of the law, but by its applicability in society. (Munir, 2023). The state's inability to prevent systemic leakage of personal data also indicates that the principle of *due diligence obligation*, which is the state's obligation to protect its citizens from rights violations arising from the negligence of digital system operators, has not been fulfilled.

The weakness of the legal protection shows that although digital identity has been judicially recognized, its position as a legal instrument is still in the transition stage between normative recognition and substantive effectiveness. According to John Rawls' theory of justice, equality in access and protection is a fundamental principle that must be guaranteed by law. (Kiran, Iqbal, & Jawwad, 2023). If some people do not have access to legal and secure digital identities, then there is digital inequality that has the potential to violate the principle of distributive justice. Meanwhile, from the point of view of progressive legal theory Satjipto Rahardjo, law must be responsive to social and technological dynamics, not solely emphasizing formal certainty. (Hidayat, Suteki, & Mahoro, 2024). Therefore, the regulation of digital identity must not stop at the normative level, but must be accompanied by adaptive legal updates, effective enforcement, and transparent accountability mechanisms. Thus, the existence of digital identity in the Indonesian legal system will only have full legitimacy if it is not only legally recognized, but also protected and enforced in real terms in the practice of people's digital lives.

Legal Protection for Digital Identity Owners against Abuse of Personal Data

Legal protection for digital identity owners is a manifestation of the state's obligation to guarantee citizens' basic rights to privacy, security, and control over their personal data in the digital space. In the context of modern law, personal data is not just a set of information, but a legal representation of an individual's existence in cyberspace. A person's digital identity reflects legal status, preferences, and economic activities, so that when the data is misused, what is actually violated is not only the confidentiality of information, but also the integrity and honor of personal as a subject of law. (Sule et.al, 2021). Therefore, legal protection of digital identities has two dimensions: as a constitutional right of individuals and as a legal obligation of the state to protect its citizens from the threat of data misuse by public and private parties. (Widodo et al., 2024).

Normatively, the recognition of digital identity protection has a strong foundation in the Indonesian legal system. Article 28G paragraph (1) of the 1945 Constitution emphasizes that everyone has the right to the protection of their personal self, family, honor, dignity, and property, and has the right to feel safe from threats. (Judijanto et al., 2025). This constitutional norm is the basis for the birth of various more specific legal instruments, such as Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transaction

Law (ITE Law). The PDP Law explicitly places the subject of personal data as the main holder of rights in the legal relationship of data. In Articles 4 to 16, the law regulates the rights of data subjects, such as the right to be notified, the right to rectify and delete data, and the right to object to unauthorised processing. (Putri, Mahendrawati, & Ujianti, 2024). Meanwhile, Articles 57 to 68 stipulate the obligations of data controllers and sanctions for violations. This provision emphasizes the balance between individual rights and the obligations of electronic system operators as part of the principles of *fairness* and *accountability* in data management.

However, this normative power has not been fully reflected in implementation in the field. Based on *a Tempo* report (2024), there was a large-scale data leak involving public institutions such as BPJS Kesehatan and KPU, where the data of millions of citizens—including NIK, address, and population status—was sold freely on *dark web* forums. (Nurani, 2024). The *Kompas* report (2023) also revealed that most victims did not receive official notification of the leak, even though Article 46 paragraph (2) of the PDP Law requires data controllers to report to data subjects no later than three days after the incident is known. (Purnamasari, 2023). This fact shows the weak application of the principles of *transparency* and *due diligence* which are the basis for legal protection for the public. In other words, citizens' legal rights as owners of digital identities are still often ignored due to weak law enforcement and the absence of an independent supervisory authority that functions effectively.

Within the framework of legal theory, this situation can be explained through the theory of *legal protection* from Philipus M. Hadjon which distinguishes between preventive and repressive protection. Preventive legal protection is provided to prevent violations through regulation, *informed consent*, and control mechanisms over data use. (Harahap & Simamora, 2025). Meanwhile, repressive legal protection is provided after the violation occurs, through administrative, civil, and criminal sanction mechanisms. Ideally, the PDP Law would have accommodated both forms of protection. However, in practice, the preventive aspect is still weak because not all data controllers apply the principle of protection from system design (*privacy by design*) as required by Article 35 of the PDP Law. The repressive aspect has not been effective because the law enforcement mechanism has not been supported by independent institutions that have full authority such as *the Data Protection Authority* in Europe. (Buckley, Caulfield, & Becker, 2024). This shows that the existence of norms without substantive supervision mechanisms has the potential to make legal protection for society formalistic.

Further analysis can use *human rights theories* that place the protection of personal data as an integral part of the right to privacy. Within the framework of international law, Article 12 *of the Universal Declaration of Human Rights* and Article 17 *of the International Covenant on Civil and Political Rights* affirm that everyone has the right to protection from arbitrary interference with his or her personal life and data. (Ramakrishnan, 2024). Indonesia, as a state party to the convention, has an

obligation to adopt the principle in national law. Thus, legal protection for digital identities is not only a domestic issue, but also part of a global commitment to respect for human rights in the digital space.

From the perspective of legal principles, legal protection for digital identity owners reflects the application of the principles of legality, the principle of justice, the principle of proportionality, and the principle of responsibility. The principle of legality demands that any data processing must have a legitimate legal basis and the consent of the data subject. The principle of fairness ensures that the rights of data owners should not be sacrificed for the sake of economic or technological efficiency. The principle of proportionality emphasizes the balance between the need for data collection and the potential risk to individual privacy. (Marelli, 2023). Meanwhile, the principle of responsibility requires data controllers to ensure the security of the system and bear the legal consequences of any breach. In this context, electronic system operators, both government and private, are obliged to provide compensation and recovery to aggrieved individuals, as stipulated in Article 58 paragraph (1) of the PDP Law.

Conceptually, digital identity is inseparable from the legal personality of an individual. It is a digital representation of a person's legal status recognized by the state. (Pierucci & Cesaroni, 2023). Therefore, legal protection of digital identity must be interpreted as protection for the legal existence of the individual itself. When personal data is misused, what is injured is not only the privacy aspect, but also the legal integrity of citizens as legal subjects. Within the framework of *the rule of law*, the state is not only tasked with setting norms, but also ensuring the effectiveness of protection through supervision mechanisms, digital audits, and the enforcement of proportionate sanctions against violators.(Fakeyede et al., 2023). The weak application of these principles will reduce the legitimacy of digital law and weaken public trust in state institutions.

Thus, legal protection for digital identity owners is actually a concrete form of the state's constitutional responsibility to its citizens in facing the digital transformation era. Such protection is not enough to be measured by the existence or absence of regulations, but must be judged by how effective legal norms can guarantee an individual's sense of security and control over their existence in the digital world.

CONCLUSION

Based on the results of the analysis of the legal position and protection of digital identity, it can be concluded that the existence of digital identity in the Indonesian legal system has gained normative legitimacy through various positive legal instruments, ranging from the 1945 Constitution, Law Number 1 of 2024 concerning Information and Electronic Transactions, to Law Number 27 of 2022 concerning Personal Data Protection, as well as technical regulations such as Permendagri Number 72 of 2022 concerning Digital Population Identity. The overall regulation shows that digital identity has been recognized as an integral part of an individual's legal status, not just an administrative instrument. Thus, digital identity can be seen as a form of legal representation of a person's existence

in the digital space that has legal consequences for individual rights and obligations.

However, although the normative recognition has been strong enough, its implementation still faces serious challenges in the context of legal protection for digital identity owners. Cases of large-scale personal data leaks reported by national media such as Tempo and Kompas show the gap between legal norms and the reality of their implementation. The weakness of the cybersecurity system, the ineffective supervision mechanism, and the lack of sanctions enforcement show that the legal rights of the community as the owner of personal data have not been substantively protected. From the perspective of legal protection theory, this condition shows that preventive protection is still formal, while repressive protection has not been effective due to the weak authority and responsibility of data controllers, Thus, the legal position of digital identity in Indonesia has been normatively recognized, but the effectiveness of its protection is still a major challenge in the development of a fair and equitable digital legal system. Legal protection of digital identities should not only be interpreted as compliance with administrative regulations, but also as part of respect for human rights and the constitutional responsibility of the state to ensure the security, honor, and legal existence of its citizens in the digital space.

REFERENCES

Aryo Putranto Saptohutomo. (2024, September 25). Sanksi kebocoran data di Indonesia belum efektif, apa penyebabnya? *Kompas.* https://nasional.kompas.com/read/2024/09/25/05450041/sanksi-kebocoran-data-di-indonesia-belum-efektif-apa-penyebabnya-

Babel, M., Willburger, L., Lautenschlager, J., Völter, F., Guggenberger, T., Körner, M. F., … & Urbach, N. (2025). Self-sovereign identity and digital wallets. *Electronic Markets, 35*(1), 1–14.

Buckley, G., Caulfield, T., & Becker, I. (2024). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity, 10*(1), tyae017.

Chanidia, A. R. (2025). Consent or coercion? A comparative legal analysis of biometric data practices in digital banking systems. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 5*(1). https://doi.org/10.15294/ipmhi.v5i1.28731

Clinten, B., & Wahyudi, R. (2022, September 1). Data 1,3 miliar nomor HP Indonesia diduga bocor, ada NIK dan nama operator. *Kompas.* https://tekno.kompas.com/read/2022/09/01/12230827/data-13-miliar-nomor-hp-indonesia-diduga-bocor-ada-nik-dan-nama-operator?page=all

Darnela, L., & Rusdiana, E. Public legal awareness and the effectiveness of Indonesia's personal data protection law: Bridging normative framework and privacy paradox. *Supremasi Hukum: Jurnal Kajian Ilmu Hukum, 14*(1).

Demkin, V. O. (2024). Digital identity and digital image of an individual: Legal characteristics and the place in the system of related categories. *RUDN Journal of Law, 28*(3), 512–527.

Englezos, E. (2023). Sign of the times: Legal persons, digitality and the impact on personal autonomy. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique, 36*(2), 441–456.

Fakeyede, O. G., Okeleke, P. A., Hassan, A., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science, 11*(11), 45–58.

Harahap, M. R., & Tanjung, A. S. (2024). Purpose of implementing progressive law against criminal offenders in order to provide legal certainty and legal benefits. *Journal of Progressive Law and Legal Studies, 2*(02), 142–151.

Harahap, P., & Simamora, N. B. (2025). Perlindungan hukum terhadap data pribadi pengguna di platform e-commerce. *Jurnal Hukum Sehasen, 11*(2), 345–352.

Hidayat, M. R., Suteki, S., & Mahoro, J. C. G. (2024). Legal wisdom in Indonesian legal system: Toward progressive law enforcement. *JUSTISI, 10*(3), 518–534.

Judijanto, L., Ahmad, A., Djuhrijjani, D., Furqon, W., & Rohaya, N. (2025). Post-truth law analysis of the protection of privacy rights in cases of digital defamation dissemination in Indonesia. *The Easta Journal Law and Human Rights, 3*(02), 81–88.

Kiran, N., Iqbal, R., & Jawwad, M. (2023). John Rawls on concepts of rights and justice in philosophy of law. *Russian Law Journal, 11*(3), 2067–2079.

Lahangatubun, N., & Muliyono, A. (2025). Public trust and the legal validity of electronic signatures in Indonesia. *Jurnal Ilmu Hukum Kyadiren, 7*(1), 499–516.

Mahameru, D. E., Nurhalizah, A., Badjeber, H., Wildan, A., & Rahmadia, H. (2023). Implementasi UU perlindungan data pribadi terhadap keamanan informasi identitas di Indonesia. *Jurnal Esensi Hukum, 5*(2), 115–131.

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. SSRN 5443854.

Mutaqin, F., Kurniawan, A., Andoyo, S. T., Khumayah, S., & Wulandari, S. (2024). Population activation service through digital civil identification app. *Asian Journal of Social and Humanities, 3*(1), 34–44.

Munir, A. I. (2023). Roscoe Pound's theory of justice & mechanical jurisprudence: A critical evaluation. *Journal of Law & Social Studies (JLSS), 5*(2), 274–280.

Nurani, S. K. (2024, September 22). Sederet kasus kebocoran data terbaru: 6 juta data NPWP diretas Bjorka, siapa tanggung jawab? *Tempo.co.* https://www.tempo.co/hukum/sederet-kebocoran-data-terbaru-6-juta-data-npwp-diretas-bjorka-siapa-tanggung-jawab--7201

Purnamasari, D. D. (2023). BPJS Ketenagakerjaan investigasi klaim Bjorka. *Kompas.id.* https://www.kompas.id/artikel/bpjs-ketenagakerjaan-investigasi-klaim-bjorka

Priyantiwi, R. D. (2025). Ensuring legal protection of personal data in Indonesia's digital identity system. *Justitia Jurnal Hukum, 9*(2).

Putri, N. M. D. G., Mahendrawati, N. L. M., & Ujianti, N. M. P. (2024). Perlindungan hukum terhadap data pribadi warga negara Indonesia berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Preferensi Hukum, 5*(2), 240–245.

Rahman, F. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new Personal Data Protection Act in Indonesia. *UUM Journal of Legal Studies, 16*(1), 1–18.

Ramakrishnan, P. (2024). Preserving the right to privacy in the digital era: A modern-day analysis through the lens of international human rights. SSRN 4960896.

Rahayuana, N. A., & Octarina, N. F. (2025). Responsibility for personal data protection. *YURISDIKSI: Jurnal Wacana Hukum dan Sains, 21*(2), 145–153. https://doi.org/10.55173/yurisdiksi.v21i2.299

Rahmayani, C. A. (2025). Consent or coercion? A comparative legal analysis of biometric data practices in digital banking systems. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, 5*(1). https://doi.org/10.15294/ipmhi.v5i1.28731

Romero, U. D. (2023). An approach to sources: The rule of recognition in Herbert LA Hart's theory. *Estudios de Filosofía, (67)*, 127–147.

Roselin, S., & Putra, M. R. S. (2025). Personal data subject rights protection: A comparative study between Indonesian PDP Law and the UK Data Protection Act. *Jurnal USM Law Review, 8*(2), 825–835.

Salam, R., & Prasetya, W. (2024, September 21). Daftar kebocoran data pribadi di era Jokowi, paling banyak di instansi pemerintah. *Tempo.* https://www.tempo.co/politik/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah--7403

Sasongko, R. W. (2023). Implementasi identitas kependudukan digital di Kabupaten Bandung. *Jurnal Registratie, 5*(1), 69–86.

Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: Issues and trends. *Technology in Society, 67*, 101734.

Utomo, A. P., Ibrohim, N. M., Ramadhani, N., Zidni, N. M., & Wahyuaristy, D. S. (2025). Konsep ideal regulasi identitas digital tunggal dalam konvergensi teknologi sebagai instrumen penguatan perdagangan digital berbasis ekonomi virtual. *Forschungsforum Law Journal, 2*(02), 119–141.

Vardanyan, L., Hamuľák, O., & Kocharyan, H. (2024). Fragmented identities: Legal challenges of digital identity, integrity, and informational self-determination. *European Studies–The Review of European Law, Economics and Politics, 11*(1), 105–121.

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).

Zahra, N., Hapsari, R. A., & Safitri, M. (2024). Perlindungan hukum teknologi identitas digital melalui sistem verifikasi identitas berbasis biometrik.

Supremasi: Jurnal Pemikiran dan Penelitian Ilmu-ilmu Sosial, Hukum, & Pengajarannya, XIX(1).

Robles-Carrillo, M. (2024). Digital identity: An approach to its nature, concept, and functionalities. *International Journal of Law and Information Technology, 32*, eaae019.

Pierucci, F., & Cesaroni, V. (2023). Data subjectivation-self-sovereign identity and digital self-determination. *Digital Society, 2*(2), 21.

Marelli, M. (2023). The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. SSRN 5443854.

Mutaqin, F., Kurniawan, A., Andoyo, S. T., Khumayah, S., & Wulandari, S. (2024). Population activation service through digital civil identification app. *Asian Journal of Social and Humanities, 3*(1), 34–44.

