

Digital Transformation and the Legal Protection of Personal Data in Indonesia

Nur Khalimatus Sa'diyah¹, Umi Enggarsasi²

^{1,2}Faculty of Law, Wijaya Kusuma University Surabaya, Indonesia

ABSTRACT: The rapid development of digital transformation has fundamentally changed human interaction and data management, while increasing the risk of personal data misuse, which poses serious challenges for law enforcement in Indonesia. This study aims to analyze and develop a comprehensive legal framework for data protection to ensure effective protection for individuals in the digital age. Using an empirical and conceptual legal approach, this study analyzes the existing legal framework, particularly Law No. 27 of 2022 on Personal Data Protection, and identifies gaps in its implementation and enforcement. Findings show that despite formal regulations, there are still significant weaknesses in institutional capacity, law enforcement mechanisms, and victim redress procedures. The proposed model emphasizes three main pillars: institutional reform to strengthen independent supervisory authorities, normative harmonization to eliminate regulatory ambiguity, and victim-oriented mechanisms based on the principle of digital justice. This study highlights the need for an adaptive legal framework that is in tune with the dynamics of technological innovation, ensuring that digital transformation proceeds in balance with the protection of individual rights. This research contributes to the discourse on data protection by proposing an integrative and collaborative legal model that links digital governance with fair legal protection, strengthening Indonesia's readiness to face the increasing complexity of data-related crimes.

KEYWORDS: Digital Transformation; Legal Protection; Personal Data; Indonesia; Justice.

I. INTRODUCTION

The global digital transformation has ushered society into an era where technology profoundly changes the way we live and interact. Amidst this, the concept of Society 5.0 was launched by the Japanese government as a vision for a "Super Smart Society" that integrates artificial intelligence, big data, the Internet of Things, and physical-digital spaces to create a more humane and efficient society [1]. However, behind these great opportunities lie serious challenges related to data security and regulation, particularly in the context of developing countries with suboptimal legal readiness [2]. The shift from the Fourth Industrial Revolution (Industry 4.0) to the emerging Fifth Industrial Revolution (Society 5.0) has ushered in an era marked by massive digital transformation, changing how individuals interact, work, and manage personal data. Digital platforms now dominate essential public and private services, from e-commerce and e-governance to digital health, which require the integration of personal data as a core operational asset. While these innovations offer significant convenience, they also present complex challenges, particularly in terms of personal data protection [3].

In Indonesia, the transition to a digital society has exposed critical vulnerabilities in the management of personal information, resulting in widespread risks of misuse and privacy violations. The 2021 data breach at the Social Security Administration Agency for Health (BPJS Kesehatan), in which over 279 million personal records were allegedly sold on a darknet forum for 0.15 Bitcoin, serves as a stark example of the urgent need for stronger regulatory protections. Such incidents not only cause material losses but also erode public trust in the state's ability to protect its citizens in cyberspace [4].

The personal data economy has grown into a high-value digital commodity in the broader context of the creative and digital economy. However, mechanisms to ensure legal protection are still underdeveloped [5]. Although Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law), the capacity for law enforcement and the effectiveness of its institutions remain questionable (Law of the Republic of Indonesia No. 27 of 2022). According to Article 28H paragraph (4) of the 1945 Constitution, every individual has the right to ownership that cannot be arbitrarily taken away [6]. This constitutional provision implies the recognition of personal data as part of an individual's personal property, and therefore deserving of legal protection (1945 Constitution, Article 28H (4)). However, the existing legal framework struggles to provide adequate compensation for victims of data breaches. Many victims suffer in silence, without access to compensation mechanisms or legal avenues to seek compensation or hold perpetrators accountable [7].

Digital Transformation and the Legal Protection of Personal Data in Indonesia

The misuse of personal data has far-reaching consequences, often involving identity theft, digital fraud, and psychological damage. In this digital environment, the legal system must evolve beyond punitive measures toward a comprehensive model of digital justice. A transformative legal approach is needed, one that not only modernizes the regulatory framework but also integrates principles of human rights and digital equality. Therefore, this study aims to develop a digital transformation model that seeks to ensure legal protection for victims of personal data misuse. The proposed model emphasizes institutional reform, normative clarity, and victim-centered mechanisms based on justice.

This research is relevant and urgent. It focuses on an in-depth analysis of digital transformation and personal data protection law in Indonesia, exploring the effectiveness of the existing regulatory framework in addressing the technological dynamics of Society 5.0, and identifying solutions to strengthen law enforcement and redress mechanisms for victims of data misuse.

II. RESEARCH METHOD

This study uses a normative legal approach (doctrinal legal research) as its main methodological basis, designed to analyze the legal framework for personal data protection in Indonesia in the context of rapid digital transformation. This method focuses on the analysis of legal texts, legal doctrines, and legal principles relevant to data protection issues [8].

This study adopts several approaches to analyze data comprehensively: Statute Approach: Used to thoroughly examine the substantive legal provisions regulated in Indonesian legislation, particularly the 1945 Constitution of the Republic of Indonesia and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This approach aims to assess the extent to which formal regulations provide strong data protection guarantees. Conceptual Approach: Applied to explore fundamental legal principles such as the right to privacy, digital justice, and state responsibility in digital ecosystem governance. This approach serves to build a theoretical foundation that leads to a deep understanding of the issues under study. Case Approach: Utilizes real-life case studies of data misuse (such as the institutional data breach incident in Indonesia described in the introduction) as secondary data to illustrate the application and challenges of law enforcement in practice.

The sources of data for this study include primary legal materials (binding laws and regulations), secondary legal materials (academic literature, scientific journals, previous research results, policy documents), and tertiary legal materials (legal dictionaries). Data was collected through systematic library research and analyzed using qualitative descriptive methods. This analysis aims to identify regulatory gaps, assess institutional and law enforcement effectiveness, and formulate an adaptive and responsive legal protection model for the complexity of data crime in Indonesia's digital era.

III. RESULTS AND DISCUSSION

A. Mapping Of National Regulations Related To Personal Data Abuse

Before analyzing the challenges and weaknesses in the implementation of personal data protection, it is essential to first map and understand the national legal framework that currently governs the protection and misuse of personal data in Indonesia. This mapping serves as a foundation to identify the normative structure, scope, and consistency of existing laws that regulate personal data both directly and indirectly.

Indonesia's legal protection for personal data has evolved through several legislative instruments that reflect a gradual response to digital transformation and the increasing threat of data misuse. Initially, the protection of personal data was incorporated within broader electronic transaction regulations, particularly through the Electronic Information and Transactions Law (ITE Law). However, as the complexity of digital activities grew, a more specific legal regime the Personal Data Protection Law (Law No. 27 of 2022) was enacted to establish comprehensive principles and obligations regarding data governance.

In addition, the newly enacted Criminal Code (Law No. 1 of 2023), which will take effect in 2026, further integrates cybercrime and personal data abuse as explicit criminal offenses. Together, these three instruments form the backbone of Indonesia's legal architecture for personal data protection. The following section outlines and analyzes each of these laws, their key provisions, and their respective strengths and weaknesses in addressing the issue of personal data misuse.

- 1) Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) in conjunction with Law No. 19 of 2016
 - a. Article 26: The use of personal data in electronic media must be done with the consent of the data owner, Data owners have the right to file a lawsuit in the event of a privacy violation.
 - b. Articles 30, 32, 35: Regulate criminal acts of illegal access, destruction, alteration, or manipulation of personal data.
 - c. Characteristics of the ITE Law: Emphasises criminal aspects (unauthorised access, hacking, manipulation), Victim protection remains limited, only allowing for civil lawsuits.
- 2) Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)

Digital Transformation and the Legal Protection of Personal Data in Indonesia

- a. Definition of Personal Data (Article 1(1)): Data relating to an identified or identifiable individual.
 - b. Data Subject Rights (Articles 5–14): The right to information, the right to access, rectify, erase data, withdraw consent, and the right to object and object to automation.
 - c. Obligations of Data Controllers (Articles 20–25): Must process data lawfully, fairly, transparently, and limited to specific purposes.
 - d. Sanctions (Articles 57–71): Administrative: warnings, temporary suspension, data deletion, fines, Criminal: misuse of personal data may be punishable by up to 6 years' imprisonment and/or a fine of Rp6 billion.
 - e. Weaknesses: The mechanism for victim compensation is not yet clear, The Personal Data Protection Supervisory Agency is still in the process of being established.
- 3) New Criminal Code (Law No. 1 of 2023 concerning the Criminal Code, effective in 2026)
- a. Articles 263–267 (Electronic Identity Fraud): Regulates the falsification, use of false identities, or false electronic documents that may include personal data.
 - b. Articles 351–352 (Misuse of Electronic Information): Prohibits the unauthorised dissemination of personal data.
 - c. Articles 598–601 (Cybercrime/Computer Crime): Affirming the prohibition of illegal access, interception, and interference with electronic systems.
 - d. Characteristics of the new Criminal Code: Provides a general legal basis for the misuse of personal data as a criminal offence, Strengthens the position of personal data as an object of criminal law protection.

B. Digital Transformation Trends and Data Vulnerability

Digital transformation has become a major driving force in the global social and economic revolution, with the massive adoption of information and communication technology (ICT) in various sectors of life [9]. This digitization process creates enormous opportunities for efficiency, transparency, and connectivity. However, as the integration between personal data and digital systems increases, so does the significant vulnerability to privacy and data security breaches [10]. Individuals and institutions are now more dependent on interconnected digital systems, which increase the attack surface for sensitive information. The presence of cloud computing, artificial intelligence (AI), Internet of Things (IoT), and big data analytics technologies further expands the scope of digital transformation. These technologies enable the collection, storage, and processing of data on a large scale and in real time. However, alongside these advancements come risks of data breaches due to weak security systems, low digital literacy, and insufficient control over third-party use of data [11]. In this context, personal data is no longer merely an individual asset but also an economic commodity traded on a massive scale in the digital marketplace.

Data vulnerability is exacerbated by a digital economy model that is oriented toward data-driven decision making. Many digital companies rely on profiling and behavioral analytics techniques that are heavily dependent on users' personal data. Without strict regulations and effective oversight mechanisms, these practices often violate individuals' privacy rights and create an unequal relationship between digital service providers and consumers [12]. The “data as oil” paradigm creates economic incentives to exploit data to the maximum, even beyond ethical and legal boundaries. In addition, the shift of human activities to the digital realm during and after the COVID-19 pandemic has accelerated the process of digitalization without adequate preparation in terms of data protection. Education, healthcare, banking, and government services have moved to digital platforms that are not yet fully equipped with robust cybersecurity infrastructure [13]. This situation has led to a surge in data breaches, identity theft, and misuse of personal information, highlighting the gap between the speed of technology adoption and the reliability of legal protections.

In developing countries such as Indonesia, this challenge is exacerbated by digital literacy gaps and limited resources for building robust information security systems. Many institutions do not yet have standard data security protocols or transparent data management systems. In addition, the general public still lacks awareness of the importance of protecting the confidentiality of their personal data [14]. This situation opens up opportunities for systemic and repeated violations, especially by entities that have power over digital infrastructure. The vulnerability of personal data in the context of digital transformation is also transnational. This phenomenon requires a global legal framework capable of regulating cross-border data traffic, including cross-border data protection mechanisms [15]. However, to date there has been no adequate harmonization of international law, resulting in asymmetrical legal protection for victims of data breaches, particularly in countries with weak regulatory frameworks [16]. This is a serious concern in the formulation of global cybersecurity and privacy protection policies. Thus, the trend of digital transformation not only brings opportunities for technological and economic progress, but also creates serious challenges in terms of personal data protection. A comprehensive approach is needed that combines technological innovation, responsive legal policies, and increased public awareness of the importance of privacy. If not addressed seriously, data vulnerabilities could become a new crisis in the digital age, one that harms the most vulnerable users—individuals as data subjects [17].

Digital Transformation and the Legal Protection of Personal Data in Indonesia

With the advancement of digital transformation, fundamental changes have occurred in the ways humans interact, transact, and manage information. The fusion of advanced technologies and global connectivity not only drives innovation but also introduces a spectrum of new vulnerabilities related to personal data protection [18]. This dynamic is reinforced by the interconnected nature of technology, large-scale data utilization, and the growing reliance on digital-based systems across various sectors, ranging from public services, finance, and healthcare to governance. However, every digital innovation inherently carries potential security risks, whether due to design flaws, regulatory gaps, or a lack of user awareness regarding possible privacy and legal implications. To understand these vulnerabilities in a more structured manner, it is necessary to identify the key trends in digital transformation that represent critical points for potential data misuse. This analysis maps out the core technologies shaping the contemporary digital landscape along with the potential threats they pose to individual security and privacy rights.

The Various Digital Transformation Trends and Data Vulnerabilities Are as Follows:

- 1) Internet of Things (IoT): IoT enables connectivity between physical devices through the internet, such as smart homes, wearable devices, and smart cities. However, the majority of IoT devices are designed with minimal security and lack adequate encryption systems, making them highly vulnerable to cyberattacks [19].
- 2) Cloud Computing: Cloud services allow flexible access to data and applications from multiple locations. Although efficient, cloud computing has high security risks, such as server misconfiguration, loss of control over data, and illegal access from third parties [20].
- 3) Artificial Intelligence (AI) & Machine Learning (ML): AI and ML are used for profiling, behavioural prediction, and automated decision-making. However, these systems often use large amounts of personal data without transparency, which can lead to privacy violations and algorithmic discrimination [21].
- 4) Big Data Analytics: The use of big data to analyse consumer behaviour, location and social interactions exposes large volumes of personal data. Although anonymised, the data can still be reconstructed to identify individuals, posing new privacy risks [22].
- 5) Blockchain and Distributed Technology (DLT): Blockchain is considered secure due to its transparent and decentralised nature. However, data that is mistakenly entered into the system cannot be repaired or deleted (immutability), thus potentially storing sensitive information permanently [23].
- 6) Digital Identity & e-KYC (Know Your Customer): Digital identity facilitates verification in public service and financial systems. But in the event of a breach, sensitive information such as biometrics, ID cards, or financial accounts can be misused on a massive scale [24].
- 7) Remote Work & Digital Collaboration: The COVID-19 pandemic has forced the mass adoption of remote working systems that rely on personal connections and online collaborative platforms. Under these conditions, company data and workers' personal data become highly vulnerable to eavesdropping and theft, especially if not supported by strong security policies. That many workers do not receive adequate security training, and embrace new technologies in a hurry-creating high risks such as access through unsecured networks, unchecked surveillance, and increased vectors of cyberattacks on the work environment [25].
- 8) Cross-border Data Flow: Data sent across borders poses new legal challenges due to differences in data protection standards between jurisdictions. This risks exposing citizens' data to countries with weak data protection systems [26]. Cross-border regulation of data exchange varies widely: The European Union applies an extraterritorial approach based on the protection of human rights and privacy values, while other countries need to fulfil an "adequate protection" standard for personal data to be legally transferred from EU territory [27].

C. Classification Of Personal Data Abuse in The Digital Age

Advances in digital technology have driven a paradigm shift in the management, distribution and utilisation of personal data. Data is now a high-value commodity, which is not only used to support technology-based services, but also the foundation for strategic decision-making in the economic, political and security sectors. However, behind this potential comes the serious risk of misuse of personal data that can harm individuals and society at large. This risk is increasingly complex because it is cross-border, involves perpetrators with various motives, and is often difficult to uncover due to confidentiality and anonymity in cyberspace [28]. In the digital era, misuse of personal data can take many forms, from commercial practices that violate privacy rights, to criminal acts that exploit information system security gaps. Technological developments such as artificial intelligence (AI), Internet of Things (IoT) and big data analytics have expanded the scale and speed of data processing, but also opened up new opportunities for malicious actors. This situation is exacerbated by users' lack of awareness of digital risks and the gap between technological innovation and the regulations that govern it [29].

The misuse of personal data is not only limited to illegal acts committed by private parties or individuals, but can also be committed by state institutions or large digital platforms that have broad access to user information. In addition, there are also

Digital Transformation and the Legal Protection of Personal Data in Indonesia

cases where the breach occurs not due to malicious intent, but rather due to negligence or lack of system safeguards. Therefore, understanding the classification of personal data abuse is an important first step to building an effective and equitable legal protection framework in the digital era [30].

The Following Are the Classifications of Personal Data Abuse in The Digital Age:

- 1) Economic Exploitation: Perpetrators use personal data for financial gain, such as:
 - a. Use of data for marketing without consent (spamming, targeted ads).
 - b. Data trading on digital black markets (data brokering).
 - c. Theft of credit card or account data for illegal transactions [31].
- 2) Cybercrime-Related Misuse: Data is used as a means or object of a criminal offence, for example:
 - a. Phishing: using data to defraud and gain account access.
 - b. Identity theft: falsifying identities for criminal activity or online lending [32].
 - c. Deepfake: manipulation of visual/audio data for the purpose of fraud or defamation.
- 3) Platform-Based Misuse: Tech companies or digital service providers access, store or share data without the user's explicit consent, such as:
 - a. Cross-platform tracking of user behaviour.
 - b. Algorithmic profiling and data-based discrimination.
 - c. Violation of the principles of *purpose limitation* and *data minimisation* in data processing [33].
- 4) State-Driven Data Abuse: The government or state institutions misuse personal data for:
 - a. Mass surveillance without a legitimate legal basis.
 - b. Repression of certain groups by utilising population data.
 - c. Violation of the right to privacy and freedom of expression [34].
- 5) Misuse due to Negligent Exposure: Not due to malicious intent, but the digital system is not secure enough:
 - a. Data leakage due to server misconfiguration.
 - b. Loss of control over data due to migration to a third party (cloud service).
 - c. Unauthorised access by internal staff due to weak security protocols [35].
- 6) Abuse in Personal Relationships (Personal Abuse): Occurs in interpersonal or domestic relationships:
 - a. Doxing: spreading personal data (address, mobile phone number) to embarrass the victim.
 - b. Monitoring a partner's digital location or activities (digital stalking) [36].

D. Legal Status of Victims in Data Abuse Cases

In the ever-evolving global digital landscape, the misuse of personal data has become one of the most threatening forms of cybercrime to individual rights. However, in many legal systems, the legal status of victims in these cases is still not as strong and explicit as victims in conventional crimes. This situation creates an imbalance in legal protection and restoration of rights that should be guaranteed by the state. In general, victims of personal data misuse face a double challenge: first, the absence or weakness of regulations related to the recognition and legal definition of data crime victims, and second, the lack of remedial mechanisms capable of restoring integrity, digital identity, and material losses due to data breaches. Many jurisdictions still place the issue of data breaches within the framework of administrative or civil law alone, without providing adequate criminal or human rights-based protection space for victims [37].

The legal status of victims should contain three important elements: recognition, access to justice, and the right to remedy. However, in cases of data misuse, there is often no formal recognition that a person is a "victim" in the legal sense who is entitled to restitution, compensation or rehabilitation [38]. In addition, the criminal justice system tends to focus primarily on the perpetrator, often ignoring the rights and needs of victims, thus ignoring the principles of victim-oriented justice [39].

At the international level, General Comment No. 16 of the UN Committee on the Rights of the Child has emphasised the importance of personal data protection as part of children's rights, and implicitly recognised that data abuse can have serious psychological and social impacts, especially on vulnerable groups such as children and women [40]. Meanwhile, in the EU context, the General Data Protection Regulation (GDPR) has provided a more progressive framework with the recognition of victims of data breaches, including the right to compensation from unlawful data controllers or processors [41]. However, the implementation of these principles in many developing countries is far from ideal. In Indonesia, for example, despite the passing of Law No. 27 of 2022 on Personal Data Protection, there are no explicit provisions stating who is entitled to be called a "victim" and how their rights are legally realised. Law enforcement tends to be reactive and limited to administrative sanctions, whereas the impact of data misuse can include complex financial, reputational and psychological losses [42]. In response to these challenges, a more comprehensive and interdisciplinary legal approach is needed, which not only focuses on technical regulations of data management, but also on ensuring victims' rights, including the right to information, participation in the legal process,

Digital Transformation and the Legal Protection of Personal Data in Indonesia

and guarantees of non-revictimisation in the investigation and court process [43]. Thus, clarifying the legal status of victims in data misuse cases is not only a juridical issue, but also part of the social justice and human rights agenda in the digital era.

One important dimension in discussing the legal status of victims of data misuse is the inequality of access to digital justice. Not all individuals have sufficient capacity or legal literacy to realise that they have become victims of data misuse, let alone to access available legal mechanisms. This phenomenon is prevalent in developing countries, including Indonesia, which faces challenges in building digital equity as a basis for legal protection [44].

The concept of *digital vulnerability* has received increasing academic attention, which is a condition where certain individuals or groups are more vulnerable to data breaches due to social, economic, or technological limitations [45]. In such cases, the misuse of personal data not only causes personal harm, but also deepens existing structural injustices. Therefore, in developing a victim protection framework, the legal approach needs to consider the social vulnerability dimension surrounding the victim.

This is in line with the principles set out in the UN Guidelines on Justice in Matters Involving Child Victims and Witnesses of Crime and the Basic Principles and Guidelines on the Right to a Remedy and Reparation which affirm that victims of crime, including digital crime, have the right to information, participation, protection, and remedy in the form of compensation and rehabilitation [46]. However, the reality in many countries shows that existing legal instruments place more emphasis on data controllers and offenders, while the position of victims remains passive and reactive, without concrete guarantees of remedy. For example, while the GDPR provides data subjects with the right to compensation, implementation often faces obstacles in proving material or psychological harm [47].

In Indonesia, despite the obligation to report data breach incidents and the threat of administrative sanctions, there is no specialised judicial mechanism that actively facilitates victims' claims. Victims' rights often rely on individual initiatives to bring civil suits, which are practically ineffective when compared to the losses suffered. This signals the need for specialised judicial or non-litigation mechanisms that are proactive in providing protection and restoration of the rights of victims of data misuse [48]. In the context of personal data abuse, the restorative justice approach can be a progressive legal policy option to strengthen the legal status of victims. Restorative justice focuses not only on punishment for the perpetrator, but also on restoring the rights and dignity of the victim through mediation, apologies, compensation, and recognition of the losses suffered [49]. This approach is relevant in the realm of digital crime because it adapts to the nature of crimes that are often not physical, but rather target aspects of an individual's identity, reputation and privacy rights. Thus, restorative justice in data crimes will restore the balance of social and legal relations between victims and perpetrators, while strengthening the digital society's sense of justice [50]. Furthermore, the status of victims in data crime must be linked to the principle of digital human rights, which guarantees that every individual has the right to be digitally safe, including the right to privacy, data protection, and the right not to be subjected to manipulation or commercialisation of personal data without consent. Therefore, recognising victims not only as legal victims, but also as subjects of digital human rights is an important step in building a comprehensive legal protection system [51].

E. Proposed Digital Transformation with Legal Guarantees

Digital transformation requires not only technological change, but also comprehensive reform of the legal framework to ensure the security, fairness, and sustainability of digital technology use in society. Digital transformation should not be viewed merely as a technological shift, but as a multidimensional reform that integrates legal, institutional, and ethical aspects to ensure that digitization remains human-centered and rights-based. The law plays a crucial role as a regulator and enabler of digital transformation, ensuring that innovation develops within a framework of fairness, accountability, and data security. The transformation adopts a techno-regulatory approach, which emphasizes that technology design and legal principles must operate in an integrated manner. This approach requires that every digital system embed values such as transparency, accountability, fairness, and respect for privacy from the outset. In Indonesia, this approach is increasingly relevant as the country seeks to balance rapid digital development with the protection of citizens' privacy rights.

Based on this theoretical framework, the proposed digital transformation consists of three interrelated pillars:

a. Legal Certainty and Data Protection Standards:

Clear, prescriptive, and human rights-based regulations are a key foundation for this digital transformation. Implementing personal data protection principles in the local context, such as validity, data minimization, and purpose limitation, is crucial to prevent the exploitation of personal data. In the Indonesian context, strengthening the institutional capacity of independent data supervisory authorities is also a key element in preventing the monopoly of data power by the state or corporations. This policy is relevant because it ensures fair and reliable law enforcement and maintains a balance between digital development and the protection of individual rights [52].

b. Legally Responsive Technological Infrastructure:

The digitalization of public and private sector services must be built on an architecture that enables legal oversight and compliance from the outset. Information technology systems must be able to record every data processing step, provide

Digital Transformation and the Legal Protection of Personal Data in Indonesia

detailed consent features, and give users access to control over their own data. This emphasizes that digital infrastructure such as reporting systems, encryption, and evidence management must be built in a manner that is responsive to legal norms and regulations. This means that technology is not only used for efficiency but also designed to actively comply with legal principles such as transparency, accountability, and the protection of individual rights. The technological architecture must reflect "technological regulation," namely the application of law from the outset, bridging regulations and software to ensure victims receive effective and adaptive legal protection [53].

c. Digital Literacy and Public Participation:

This digital transformation emphasizes the importance of building public capacity to understand their rights in the digital ecosystem. Digital literacy serves as a preventive protection instrument, which can reduce the information gap between users and data controllers. Without literacy, digital transformation risks creating a "digital underclass" lacking legal awareness [54].

IV. CONCLUSION

Indonesia's transition to a digital society requires not only technological advances, but also a robust and adaptive legal framework to ensure justice, accountability, and the protection of human rights in cyberspace. The increasing interdependence between digital innovation and personal data management has made data protection a central issue in achieving sustainable and equitable digital transformation. However, analysis shows that the current legal system, despite being strengthened by the enactment of the Personal Data Protection Law (Law No. 27 of 2022) and the New Criminal Code (Law No. 1 of 2023), still faces substantial challenges in terms of implementation, institutional readiness, and victim-oriented law enforcement.

First, the regulatory map shows that Indonesia's legal instruments remain fragmented and reactive, focusing more on administrative and punitive aspects than on prevention and restorative justice. Compensation and victim rights restoration mechanisms remain unclear, leaving individuals affected by data misuse without adequate legal recourse. Second, this study identifies that technological vulnerabilities such as weak cybersecurity infrastructure, low digital literacy, and irregular use of artificial intelligence and big data exacerbate the risk of personal data exploitation. This situation is compounded by limited institutional capacity to consistently monitor, supervise, and enforce data protection principles.

To address these issues, a technological-regulatory approach is proposed that integrates technology design with the legal principles of transparency, accountability, and privacy protection. The success of digital transformation depends on three interrelated pillars: Legal Certainty and Data Protection Standards, which ensure clear, rights-based, and enforceable norms in accordance with Indonesia's constitutional guarantees under Article 28H(4) of the 1945 Constitution; Legally Responsive Technology Infrastructure, ensuring that digital systems are designed to comply with legal norms and facilitate traceable, transparent, and auditable data processing; and Digital Literacy and Public Participation, empowering citizens to understand and exercise their digital rights, thereby strengthening preventive protection mechanisms.

Ultimately, this study emphasizes that achieving digital justice requires a paradigm shift from a state- or corporation-centered regulatory model to a victim- and rights-centered framework. Legal reform must go beyond formal compliance toward ensuring substantive justice, redress mechanisms, and equal access to digital justice for all citizens. The realization of a secure, inclusive, and ethical digital ecosystem in Indonesia depends on how effectively laws, institutions, and technology evolve together to uphold the principles of privacy, accountability, and digital rights as the foundation for national digital transformation.

REFERENCES

- 1) Rojas, C. N., Peñafiel, G. A. A., Buitrago, D. F. L., & Romero, C. T. (2021). Society 5.0: A Japanese concept for a superintelligent society. *Sustainability*, 13(12), Article 6567. <https://doi.org/10.3390/su13126567>
- 2) Bhatt, C., & Burman, A. (2024). Data Protection Regulation in the Global South. *Carnegie Endowment for International Peace*. <https://carnegieendowment.org/posts/2024/02/data-protection-regulation-in-the-global-south?lang=en>
- 3) Nasution, V. I. A., Yuliani, I., Akadira, T., & Saleha, E. (2024). Transforming Governance: Indonesia's Digital Leap from Bureaucracy to Big Data in the Era of Society 5.0. In I. P. P. Salmon et al. (Eds.), *Advances in Social Science, Education and Humanities Research*, 894. https://doi.org/10.2991/978-2-38476-340-5_17
- 4) Kusuma Pertiwi, W., & Wahyudi, R. (2021, 22 Mei). Kronologi Kasus Kebocoran Data WNI, Dijual 0,15 Bitcoin hingga Pemanggilan Direksi BPJS. https://tekno.kompas.com/read/2021/05/22/09450057/kronologi-kasus-kebocoran-data-wni-dijual-0-15-bitcoin-hingga-pemanggilan?utm_source
- 5) Wahyuni, W. (2022). Dua jenis data pribadi yang perlu dilindungi menurut UU PDP. *Hukumonline*. accessed from: <https://www.hukumonline.com/berita/a/dua-jenis-data-pribadi-yang-perlu-dilindungi-menurut-uu-pdp-lt6349e2932bd09>

- 6) Sari, Y. N., Nugroho, R., & Khanif, A. (2020). Land acquisition for public interests: A review from the human rights context. *Indonesian Journal of Law and Society*, 1(1), 23–36. <https://ijls.jurnal.unej.ac.id/index.php/IJLS/article/view/16757>, <https://doi.org/10.19184/ijls.v1i1.16757>,
- 7) Rosadi, S. D., & Gumelar Pratama, G. (2018). Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia. *Brawijaya Law Journal*, 5(2), 143–157. <https://doi.org/10.21776/ub.blj.2018.005.01.09>
- 8) Setia Negara, T. A. S. (2023). *Normative Legal Research in Indonesia: Its Origins and Approaches*. *Audito Comparative Law Journal (ACLJ)*, 4(1), 1-9. <https://doi.org/10.22219/aclj.v4i1.24855> – artikel ini menelaah secara komprehensif metode penelitian hukum normatif/doctrinal di Indonesia.
- 9) Sutomo, D. A. (2025). The impact of digital transformation on economic growth in developing countries: A case study of Indonesia. *Innovative: Journal of Social Science Research*, 5(3), 6094–6109. \ <https://doi.org/10.31004/innovative.v5i3.19670>
- 10) D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.-A., & Bourka, A. (2015). Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. *arXiv*. <https://arxiv.org/abs/1512.06000>
- 11) De Donno, M., Kavaja, J., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-Storms come from clouds: Security of Cloud Computing in the IoT Era. *arXiv*. <https://arxiv.org/abs/1902.10071>
- 12) Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, 13(203), 203–218. <https://scholar.law.colorado.edu/ctlj/vol13/iss2/4/>?
- 13) OECD. (2020). Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides. OECD Policy Responses to Coronavirus (COVID-19). <https://img.lalr.co/cms/2020/11/27173400/digital-economy-outlook-covid.pdf>
- 14) Nugroho, A. A., Winanti, A., & Surahmad, S. (2020). Personal data protection in Indonesia: Legal perspective. *International Journal of Multicultural and Multireligious Understanding*, 7(7), 183–189. <https://doi.org/10.18415/ijmmu.v7i7.1773>
- 15) Greenleaf, G. (2014). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, (126), 10–13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418446
- 16) Kuner, C. (2015). *Transborder data flows and data privacy law*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199674619.001.0001>
- 17) Lesmana, D., Afifuddin, M., & Adriyanto, A. (2023). Challenges and cybersecurity threats in digital economic transformation. *International Journal of Humanities Education and Social Sciences*, 2(6). <https://doi.org/10.55227/ijhess.v2i6.515>
- 18) Stefani, E., Costa, I., Gaspar, M. A., Goes, R. de S., Monteiro, R. C., Petrili, B. R., & Pereira, A. de P. (2025). Information security risk framework for digital transformation technologies. *Systems*, 13(1), 37. <https://doi.org/10.3390/systems13010037>
- 19) Mohamad Said, Z., & Zolkipli, M. F. (2022). Internet of Things (IoT): A study of security issues and challenges. *International Journal of Recent Contributions from Engineering, Science & IT (IJES)*, 10(02), 16-31. <https://doi.org/10.3991/ijes.v10i02.29301>
- 20) Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11. <https://doi.org/10.1016/j.jnca.2010.07.006>
- 21) Keswani, V., & Celis, L. E. (2024). Algorithmic fairness from the perspective of legal anti-discrimination principles. *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, 7(1), 724-737. <https://doi.org/10.1609/aies.v7i1.31674>
- 22) Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10, Article 3069. <https://doi.org/10.1038/s41467-019-10933-3>
- 23) Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley.
- 24) Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer. <https://doi.org/10.1007/978-0-387-77326-1>
- 25) Nurse, J. R. C., Williams, N., Collins, E., Panteli, N., Blythe, J., & Koppelman, B. (2021). Pre- and Post-COVID-19 Remote Working: An Analysis of New Threats and Risks to Security and Privacy. In C. Stephanidis, M. Antona, & S. Ntoa (Eds.), *HCI International 2021: Human-Computer Interaction* (pp. [pages]). *Communications in Computer and Information Science*, 1421. Springer. https://doi.org/10.1007/978-3-030-78645-8_74
- 26) Greenleaf, G. (2014). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws & Business International Report*, (126), 10-13.

- 27) Sun, L. (2023). Overview of Regulations on Cross-Border Data Flow. *Academic Journal of Science and Technology*, 8(1), 171-176. <https://doi.org/10.54097/ajst.v8i1.14305>
- 28) Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, 11(5), 239-273. <https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/>
- 29) Solove, D. J. (2021). Privacy harms. *Boston University Law Review*, 102(3), 793-861. <https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf>
- 30) Martin, K., & Shilton, K. (2016). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, 67(8), 1878-1892. <https://doi.org/10.1002/asi.23490>
- 31) Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NYU Press.
- 32) Identity Theft Resource Centre. (2021). Annual Data Breach Report 2021. <https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises>
- 33) Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- 34) Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, 1(2). <https://doi.org/10.1177/2053951714541861>
- 35) Waiganjo, I. N., & Nandjenda, L. S. (2020). Unveiling insider threats: Examining vulnerabilities in an organisational structure: A case study of NamPost. *Open Access Library Journal*, 7, Article e12797. <https://doi.org/10.4236/oalib.1112797>
- 36) Kaspersky. (2021). Digital Stalking in Relationships: What is stalkerware, and do people recognise it? https://media.kasperskydaily.com/wp-content/uploads/sites/86/2021/11/17164103/Kaspersky_Digital-stalking-in-relationships_Report_FINAL.pdf
- 37) Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report*, (145), 10-13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035
- 38) De Hert, P., & Papakonstantinou, V. (2012). The proposed data protection regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, 28(2), 130-142. <https://doi.org/10.1016/j.clsr.2012.01.010>
- 39) Doak, J. (2008). *Victims' Rights, Human Rights and Criminal Justice: Reconceiving the Role of Third Parties*. Oxford: Hart Publishing. ISBN 9781841136035.
- 40) United Nations Committee on the Rights of the Child (2013). General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16.
- 41) Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer. <https://doi.org/10.1007/978-3-319-57959-7>
- 42) Mahendra, G. S. (2024). Legal protection for victims whose passport personal data is spread due to government negligence. *Light: Journal of Social, Political and Legal Studies*, 1(3), 104-111. <https://doi.org/10.62383/terang.v1i3.382>
- 43) UNODC. (2020). Good practices in protecting victims of cybercrime. United Nations Office on Drugs and Crime. <https://www.unodc.org>
- 44) Graham, M., & Dutton, W. H. (2019). *Society and the Internet: How Networks of Information and Communication are Changing Our Lives* (2nd ed.). Oxford University Press.
- 45) Madiega, T. (2021). Digital vulnerability and data protection in the EU. European Parliamentary Research Service. <https://www.europarl.europa.eu>
- 46) United Nations. (2005a). Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime. Economic and Social Council Resolution 2005/20. <https://www.refworld.org/legal/resolution/ecosoc/2005/en/22129>
- 47) Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.
- 48) Siregar, M. (2024). The Absence of Complaint and Redress Mechanisms for Victims of Personal Data Leakage in Indonesia. *Indonesian Journal of Legal Science*, 29(2), 201-220. <https://doi.org/10.24843/JIHI.29.2.2024>
- 49) Zehr, H. (2015). *The Little Book of Restorative Justice*. Good Books.
- 50) Wong, R. Y., & Mulligan, D. K. (2019). Bringing design to the privacy table: Broadening "design" in "privacy by design" through the lens of HCI. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1-23. <https://doi.org/10.1145/3359171>

Digital Transformation and the Legal Protection of Personal Data in Indonesia

- 51) Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 1-14. <https://doi.org/10.1177/2053951717736335>
- 52) Widiatedjaa, I. G. N. P., & Mishra, N. (2022). *Establishing an independent data protection authority in Indonesia: A future-forward perspective*. *International Review of Law, Computers & Technology*, 37(3), 252–273. <https://doi.org/10.1080/13600869.2022.2155793>
- 53) Latifah, E., Bajrektarevic, A. H., & Imanullah, M. N. (2019). Digital Justice in Online Dispute Resolution: The Shifting from Traditional to the New Generation of Dispute Resolution. *Brawijaya Law Journal*, 6(1), 27–37. <https://doi.org/10.21776/ub.blj.2019.006.01.02>
- 54) Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657–670. <https://doi.org/10.1177/1461444816686318>



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0)

(<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.