Vol. 21 No. 2 September 2025 **YURISDIKSI**
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya

ISSN print 2086-6852 and ISSN Online 2598-5892

Responsibility For Personal Data Protection

Niken Arief Rahayuana[1], Nynda Fatmawati Octarina[1]

[1]Faculty of Law, Narotama University, Surabaya, Indonesia

[*]Corresponding Author E-mail: niken.rahayuana@narotama.ac.id

Article History: Received: March 19, 2025; Accepted: May 22, 2025

ABSTRACT

This study examines the Indonesian government's legal responsibilities in protecting citizens' personal data, focusing on constitutional, administrative, and criminal aspects. Using normative legal research methods, the analysis incorporates provisions from the 1945 Constitution, the Personal Data Protection Law (UU PDP), and related regulations to evaluate the state's obligations in preventing and addressing data breaches. The findings reveal that personal data protection is a constitutional right under Article 28G(1) of the 1945 Constitution, reinforced by the UU PDP. As data controllers, government institutions bear layered responsibilities including preventive measures, administrative compliance, victim compensation, and constitutional accountability. However, criminal liability only applies to individual officials rather than government institutions as legal entities. Despite existing safeguards, regulatory gaps remain particularly concerning administrative sanctions, compensation mechanisms, and the establishment of an independent oversight body as mandated by the UU PDP. To strengthen data protection, this study recommends: (1) refining implementing regulations; (2) enhancing oversight mechanisms; (3) improving government officials' capacity; (4) increasing public awareness; and (5) fostering international cooperation to address cross-border data violations. These measures are crucial for ensuring effective personal data protection and safeguarding citizens' constitutional rights in the digital age.

Keywords: data protection, government liability, PDP Law, constitutional rights, regulatory framework

1. INTRODUCTION

The digital era has ushered in unprecedented reliance on information technology, where the exchange and processing of personal data have become ubiquitous across social, economic, and governmental spheres (Zuboff, 2019). In Indonesia, the rapid expansion of digital transactions has exponentially increased the volume of personal data collected, processed, and stored by both public and private entities (Prasetyo et al., 2023). This surge underscores the critical need for robust personal data protection—a multidimensional issue intersecting security, human rights, economic stability, and national sovereignty (World Economic Forum, 2023).

Constitutionally, the Indonesian government is obligated to safeguard citizens' privacy rights under Article 28G(1) of the 1945 Constitution, reinforced by the Personal Data Protection Law (UU PDP No. 27/2022). Globally, frameworks like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) emphasize state and corporate accountability in data security (Hoofnagle et al., 2019). However, Indonesia faces systemic challenges: the country ranks among the top 10 globally for data breaches (Surfshark, 2024), with incidents like the BPJS Health (2021) and General Election Commission (2018) leaks

ISSN print 2086-6852 and ISSN Online 2598-5892

exposing institutional vulnerabilities in public and private sectors. Such breaches incur staggering economic costs—averaging $4.35 million per incident (IBM, 2023)—and erode public trust in digital governance.

The government's role as regulator, overseer, and enforcer is pivotal. It must (1) establish stringent regulations, (2) monitor compliance across sectors (e.g., health, finance), (3) impose sanctions for violations, and (4) promote public awareness (Solove, 2021). Yet, regulatory gaps persist, particularly in administrative sanctions, victim compensation, and the establishment of an independent supervisory body under the UU PDP. Criminal liability remains limited to individual officials, excluding government institutions as legal entities—a loophole demanding scrutiny (Wahyudi, 2023).

The urgency of this study stems from Indonesia's paradoxical position: while digital adoption accelerates, data protection frameworks lag, risking systemic harm to democracy and human rights (Citron, 2022). Existing literature highlights state responsibility in data governance (Bennett & Raab, 2020) but neglects the enforcement challenges in developing economies. This research addresses that gap by interrogating, What forms of legal responsibility should the government bear for failures in personal data protection?, Can criminal liability be imposed on the government for such failures?

By analyzing constitutional, administrative, and criminal liability frameworks, this study proposes systemic reforms—aligning Indonesia's approach with global standards while addressing local institutional weaknesses.

2. RESEARCH METHOD

This study adopts a normative legal research approach, focusing on the systematic examination of legal documents, regulations, and case studies to analyze the Indonesian government's responsibilities in personal data protection. Conducted from January to June 2024, the research draws upon Indonesia's constitutional provisions, the Personal Data Protection Law (UU PDP), and comparative frameworks such as the EU's GDPR and Singapore's PDPA. The methodology combines four key approaches: (1) a legislative analysis of statutory provisions, (2) a conceptual exploration of privacy theories and legal liability, (3) case studies of significant data breaches in Indonesia (including BPJS Health and election commission incidents), and (4) a comparative assessment of international data protection models.

ISSN print 2086-6852 and ISSN Online 2598-5892

3. RESULTS AND DISCUSSION

Urgency of Personal Data Protection in a Rule of Law State

Personal data encompasses information directly or indirectly linked to an individual's identity, including names, national identification numbers, addresses, health records, financial data, and biometrics. The protection of personal data is an integral aspect of modern human rights, particularly the right to privacy, which has evolved into a fundamental right in both international and domestic legal systems due to advancements in information technology (Bloustein). In Indonesia, the constitutional legitimacy of data protection is affirmed under Article 28G(1) of the 1945 Constitution, which guarantees the right to personal, familial, and property protection.

In the digital era, personal data has become a valuable asset ("new oil" or "new currency"), making it highly susceptible to misuse by governments, private entities (financial institutions, tech companies), and cybercriminals (hackers, illegal data traders). The rise of big data management by public and private sectors—covering population, financial, health, and digital activity data—increases risks of cybercrime, identity theft, and economic exploitation. Consequently, the state must establish adaptive legal frameworks to address digital threats, ensuring data security, confidentiality, and integrity (UU PDP No. 27/2022).

Government Accountability in Personal Data Protection

Government accountability in administrative law refers to the liability of state bodies or officials for unlawful actions causing public harm (Van Dunné). In public administration, state liability arises from: 1)Unlawful acts by government agencies or officials. 2)Administrative actions resulting in individual losses. From a human rights perspective, state obligations include : **Obligation to Respect**: The state must refrain from arbitrary interference with privacy rights. **Obligation to Protect**: The state must safeguard individuals from third-party privacy violations. **Obligation to Fulfill**: The state must enact legislative, administrative, and judicial measures to ensure privacy protection. **Legal Foundations of Government Accountability in Indonesia** Indonesian law provides a robust framework for personal data protection: **1945 Constitution (Article 28G(1))**: Guarantees the right to personal and property protection. **Law No. 27/2022 on Personal Data Protection (PDP Law)**: Mandates data controllers (including government agencies) to ensure data accuracy, security, and confidentiality (Articles 21, 35, 58). **Government Administration Law (No. 30/2014)**: Requires adherence to good governance principles (accountability, prudence, transparency). **Human Rights Law (No. 39/1999)**: Obligates the state to respect, protect, and fulfill human rights, including data privacy.

Forms of Government Liability for Data Breaches

ISSN print 2086-6852 and ISSN Online 2598-5892

The government bears multiple layers of responsibility in safeguarding personal data, each addressing different aspects of prevention, enforcement, and redress. These responsibilities are structured to ensure comprehensive protection and accountability in cases of data breaches.

Preventive Responsibility entails proactive measures to mitigate risks before breaches occur. The government must strengthen national cybersecurity infrastructure to defend against unauthorized access and cyber threats. Regular audits of data management systems are essential to identify vulnerabilities and ensure compliance with security protocols. Additionally, training programs for government personnel on data protection best practices must be implemented to enhance institutional competence. Public awareness campaigns are equally crucial to educate citizens about their privacy rights and the importance of data security.

Administrative Responsibility focuses on regulatory oversight and corrective actions within government operations. This includes enforcing compliance with data protection laws through internal monitoring mechanisms. Under Article 57 of Indonesia's Personal Data Protection (PDP) Law, administrative sanctions such as warnings, temporary processing bans, or data deletion may be imposed on agencies that fail to meet security standards. Compensation mechanisms for negligence must also be established to address harm caused by administrative lapses.

Curative Responsibility comes into play after a breach has occurred, emphasizing remedial actions to restore trust and security. Effective complaint resolution mechanisms, facilitated by institutions like the Personal Data Protection Authority or the Ombudsman, ensure that affected individuals can seek redress. Article 58 of the PDP Law mandates compensation for both material and immaterial losses suffered due to data misuse. Furthermore, system recovery efforts—such as patching security flaws and enhancing protective measures—are critical to preventing future incidents.

Criminal Liability addresses deliberate or negligent violations by individuals within the government. While the state as an institution is generally immune from criminal prosecution, individual officials may face legal consequences under the PDP Law (Articles 67–71) for unlawful data collection, processing, or disclosure. The Indonesian Penal Code (KUHP) also provides sanctions for cybercrimes and abuse of authority, ensuring personal accountability for misconduct.

Civil Liability allows affected individuals to seek legal recourse against the government for damages resulting from data breaches. Claims can be filed under Article 1365 of the Civil Code, which holds parties liable for unlawful acts causing harm, or under Article 58 of the PDP

ISSN print 2086-6852 and ISSN Online 2598-5892

Law, which specifically governs compensation for data misuse. This form of liability reinforces the principle that the state must answer for its failures in protecting citizens' data.

Constitutional Liability underscores the government's duty to uphold fundamental rights, including privacy under Article 28G of the 1945 Constitution and human rights protections under Article 28I. If the state neglects these obligations, judicial review by the Constitutional Court can be initiated to challenge systemic failures. This ensures that data protection is not merely a policy issue but a constitutional imperative.

Collectively, these forms of liability create a multi-faceted framework that holds the government accountable at various levels—preventing breaches, enforcing compliance, remedying harm, and upholding constitutional safeguards. This structured approach aligns with global best practices while addressing Indonesia's specific legal and technological challenges in data protection.

Case Study: BPJS Health Data Breach (2021)

The BPJS Health data breach exposed 279 million Indonesians' sensitive data (NIKs, health records, family details). Despite sectoral regulations (e.g., PP No. 71/2019 on Electronic Systems), the breach revealed systemic failures in data security. Legal analyses of data breaches reveal multiple dimensions of government accountability. At the constitutional level, such incidents may violate privacy rights protected under Article 28G of Indonesia's 1945 Constitution, which guarantees personal protection. From an administrative perspective, failures in data protection often constitute negligence under Government Administration Law No. 30/2014, particularly when agencies disregard due diligence requirements in handling sensitive information. Civil law violations emerge when affected parties seek damages through Article 1365 of the Civil Code (KUHPdt), which provides remedies for unlawful acts causing harm. The potential for criminal liability becomes particularly significant under the Personal Data Protection (PDP) Law, where responsible officials could face imprisonment under Articles 67-70 for willful misconduct or gross negligence in data management, had the law been applicable at the time of the breach (UU PDP No. 27/2022).

The question of whether criminal sanctions can apply to the government itself involves complex legal principles. Traditional doctrines of state immunity (par in parem non habet imperium) historically shielded governments from criminal prosecution, preserving sovereign authority. However, contemporary legal developments, particularly in international law through instruments like the ICC Statute, demonstrate a growing trend toward holding states accountable for egregious violations, including systematic human rights abuses. Indonesia's PDP Law reflects a

ISSN print 2086-6852 and ISSN Online 2598-5892

more limited approach, focusing criminal sanctions on individual officials rather than institutional liability (Articles 67-71). This aligns with international practices such as the EU's General Data Protection Regulation (GDPR), which imposes substantial administrative fines on public bodies while reserving criminal charges for individual actors under national laws. The distinction preserves governmental functions while ensuring personal accountability for data protection failures (Van Dunné; GDPR 2016/679).

Academic Analysis

In a rule-of-law state, government accountability for data breaches reflects **state responsibility** and **good governance**. While the PDP Law and revised KUHP (No. 1/2023, Article 118) recognize corporate criminal liability (including public bodies), prosecuting the state institutionally remains contentious. Instead, **personal liability for officials** aligns with the **principle of culpability** in criminal law.

4. CONCLUSIONS

Based on the legal research and analysis conducted, several key conclusions emerge regarding personal data protection in Indonesia. The study confirms that personal data protection constitutes a fundamental human right guaranteed by the constitution. The state, through its government institutions, bears the obligation to protect citizens' privacy rights as stipulated in Article 28G(1) of the 1945 Constitution and reinforced by Law No. 27 of 2022 on Personal Data Protection (PDP Law). As data controllers, government entities assume multifaceted legal responsibilities for data breaches or misuse, encompassing preventive measures (data breach prevention), administrative compliance (legal obligations fulfillment), curative actions (compensation and recovery), and constitutional duties (citizens' rights protection). However, criminal liability applies only to individual officials who demonstrate negligence or willful misconduct under Articles 67-71 of the PDP Law, while government institutions remain subject solely to administrative and civil liabilities. The research further identifies regulatory gaps, particularly regarding detailed administrative sanctions and victim compensation mechanisms in implementing regulations, as well as the crucial need for establishing an independent oversight body to ensure effective state accountability.

To strengthen Indonesia's personal data protection framework, the study proposes several strategic recommendations. First, the government and legislature should expedite comprehensive implementing regulations for the PDP Law, addressing: (1) victim compensation and recovery mechanisms, (2) government information system security standards, (3) public sector data audit

ISSN print 2086-6852 and ISSN Online 2598-5892

protocols, and (4) institutional capacity building for oversight bodies. Second, establishing an independent, professional supervisory institution with broad authority to monitor data processing across both public and private sectors remains imperative. Third, enhancing internal oversight mechanisms within government agencies through capacity building, ethical codes implementation, and robust monitoring systems would minimize administrative and criminal violations. Fourth, comprehensive public legal literacy programs should be developed through collaborations with educational institutions, civil society organizations, and media outlets to raise awareness about data protection rights and remedies. Finally, strengthening international cooperation through extradition treaties, data exchange agreements, and cross-border judicial recognition would better address transnational cybercrimes and global data breaches. These measures collectively aim to establish a comprehensive and effective personal data protection ecosystem in Indonesia.

REFERENCES

Satjipto Rahardjo (2026), Ilmu Hukum, Bandung: Citra Aditya Bakti.

Solove, Daniel J (2008). Understanding Privacy. Harvard University Press.

Wahyudi Djafar dan Elonnai Hickok (2015)., Perlindungan Data Pribadi di Indonesia: Tinjauan terhadap Regulasi dan Praktik, Jakarta: ELSAM.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(203).

United Nations. (1948). Universal Declaration of Human Rights, Art.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Barda Nawawi Arief, Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan, (Bandung: Citra Aditya Bakti, 2001)

Jimly Asshiddiqie, Pengantar Ilmu Hukum Tata Negara, (Jakarta: Konstitusi Press, 2006)

Andi Hamzah (2008)., Pengantar Hukum Pidana Indonesia, Jakarta: Ghalia Indonesia.

Moeljatno (2002)., Asas-Asas Hukum Pidana, Jakarta: Rineka Cipta.

Barda Nawawi Arief (2010). Masalah Penegakan Hukum dan Kebijakan Hukum Pidana, Jakarta: Kencana.

Sudarto, Hukum Pidana I, Bandung: Alumni, 1986, hlm. 143.

Barda Nawawi Arief (2014)., Bunga Rampai Kebijakan Hukum Pidana, Jakarta: Kencana.

ISSN print 2086-6852 and ISSN Online 2598-5892

Andi Hamzah (2005). Delik-Delik Khusus, Jakarta: Sinar Grafika

Barda Nawawi Arief (2015)., Kebijakan Legislasi dalam Penanggulangan Kejahatan, Jakarta: Kencana.

Soerjono Soekanto dan Sri Mamudji, Penelitian Hukum Normatif: Suatu Tinjauan Singkat, (Jakarta: Rajawali Pers, 2015)

Peter Mahmud Marzuki, Penelitian Hukum, (Jakarta: Kencana, 2016)

Philipus M. Hadjon dkk., Pengantar Hukum Administrasi Indonesia, (Yogyakarta: Gadjah Mada University Press, 2005)

Peter Mahmud Marzuki (2010)., Penelitian Hukum, Jakarta: Kencana.

Sudikno Mertokusumo (1993). Penemuan Hukum: Sebuah Pengantar, Yogyakarta: Liberty.

Gustav Radbruch, Legal Philosophy, Translated by Kurt Wilk, New York: The Lawbook Exchange, 2006

Henry J. Steiner & Philip Alston, International Human Rights in Context, Oxford: Oxford University Press, 2000.

Muladi dan Barda Nawawi Arief, Teori-Teori dan Kebijakan Pidana, (Bandung: Alumni, 1998)
Andi Hamzah, Asas-Asas Hukum Pidana, (Jakarta: Rineka Cipta, 1994)

Barda Nawawi Arief, Kebijakan Legislasi dalam Penanggulangan Kejahatan, (Jakarta: Prenada Media, 2013), hlm. 91.

Ian Brownlie, Principles of Public International Law, (Oxford: Oxford University Press, 2008)

Malcolm N. Shaw, International Law, (Cambridge: Cambridge University Press, 2008)

Muladi, Pertanggungjawaban Pidana Korporasi, (Semarang: Badan Penerbit Universitas Diponegoro, 1995)

Jimly Asshiddiqie, Perlindungan Data Pribadi dalam Perspektif Hak Asasi Manusia, Jakarta: Konstitusi Press, 2022

Daniel Moeckli et al., International Human Rights Law, 3rd ed., Oxford University Press, 2018

David Rosenbloom, Administrative Law for Public Managers, Boulder: Westview Press, 2003.

Jimly Asshiddiqie, Perlindungan Data Pribadi dalam Perspektif Hak Konstitusional, Jakarta: Konstitusi Press, 2022

World Economic Forum "The Global Risk Report 2023, 18th Edition" Cologny Geneva Switzerland, January 2023

ISSN print 2086-6852 and ISSN Online 2598-5892

Alifatul Laily Romadloniyah, Dwi Hari Prayitno (2018)., "Pengaruh Persepsi Kemudahan Penggunaan, Persepsi Daya Guna, Persepsi Kepercayaan, Dan Persepsi Manfaat Terhadap Minat Nasabah Dalam Menggunaan E-Money Pada Bank Bri Lamongan." Jurnal Penelitian Ekonomi dan Akuntansi 3.2,

European Parliament and Council. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape Report.

Bloustein, Edward J., Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser, New York University Law Review, Vol. 39, 1964

Van Dunné, Jan M., Administrative Liability in Comparative Perspective, The American Journal of Comparative Law, Vol. 53, 2005

European Union, General Data Protection Regulation (EU) 2016/679, Article

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), Article