Journal of Law, Society and Living Norms
Publisher: CV. Norma Global
E-ISSN: 3123-2566
Volume 1, Number 3, 2026
E-ISSN: 3123-2566

Legal Protection for PLN in The Disclosure of Customer Data to Law Enforcement Agencies

Riganu Tirta Prastawa[1], Dewi Kartika[2]
[1] Universitas Gadjah Mada
[2] Universitas Pancasila
Correspondence: riganutirtaprastawa@mail.ugm.ac.id[1], dewi_ktk@yahoo.com[2]

Article Info
Article history:
Received Mar 10th, 2026
Revised Apr 10th, 2026
Accepted Apr 13rd, 2026

Keywords:
Personal data protection; law enforcement; legal politics; state-owned enterprises; legal certainty.

ABSTRACT
The interaction between personal data protection and criminal law enforcement created a normative tension within the Indonesian legal system. The enactment of Law Number 27 of 2022 on Personal Data Protection strengthened constitutional guarantees of privacy, while criminal procedural regulations continued to prioritize public interest and effective investigation. PT PLN (Persero), as a state-owned enterprise managing extensive customer data, occupied a legally sensitive position when responding to requests from law enforcement agencies. This research employed a normative juridical approach to examine statutory provisions governing data disclosure and institutional responsibility. The findings indicated that personal data protection was not absolute and could be limited for legitimate investigative purposes based on statutory authority. However, the absence of detailed implementing regulations created interpretative ambiguity and potential institutional vulnerability. Legal certainty could be strengthened through formal written authorization, proportional disclosure standards, and clearer regulatory safeguards ensuring accountability in the disclosure process.

INTRODUCTION

Personal data protection constitutes an essential component of constitutional governance in Indonesia. Article 28G of the 1945 Constitution of the Republic of Indonesia guarantees the right of every individual to personal security and protection of dignity. The enactment of Law Number 27 of 2022 on Personal Data Protection marked a significant development in strengthening these constitutional safeguards within the digital era. As legislation reflects prevailing state policy and political configuration (Mahfud, 2017), the Personal Data Protection Law embodies Indonesia's commitment to balancing individual privacy rights with institutional and technological realities involving large-scale data processing.

Within this regulatory framework, state-owned enterprises managing essential public services occupy a particularly complex legal position. PT PLN (Persero), as the national electricity provider, serves more than 92 million customers across Indonesia (PT PLN, 2024a). In fulfilling its mandate, PLN collects and processes identity numbers, addresses, contact information, electricity consumption records, and other digital interaction data (PT PLN, 2024b). The magnitude of this data management places PLN simultaneously under strict confidentiality obligations and within the operational reach of investigative authorities.

Normative tension arises when law enforcement agencies request access to customer data in the context of criminal investigations conducted under Law Number 8 of 1981 on Criminal Procedure. Criminal procedural law grants investigators authority to obtain information necessary to uncover criminal acts and secure evidence, whereas the Personal Data Protection Law imposes duties to protect data subject rights and prevent unlawful disclosure. Refusal to comply with investigative requests may

potentially be interpreted as obstruction of justice pursuant to Article 221 of the Criminal Code (Jodi, 2024). This dual regulatory environment situates PLN at the intersection of privacy protection and public security objectives.

Recent scholarship has examined data protection compliance and comparative regulatory structures in Southeast Asia (Awwaliyah & Juniarti, 2024). However, existing studies predominantly focus on private-sector compliance or general doctrinal exposition of privacy law. Limited attention has been devoted to the institutional vulnerability of state-owned enterprises managing critical public infrastructure. The intersection between privacy obligations, investigative authority, and potential criminal exposure for obstruction remains underexplored within Indonesian legal discourse.

Accordingly, this article addresses the following research question: how can legal protection for PT PLN (Persero) be ensured when disclosing customer personal data to law enforcement agencies within the framework of Indonesian legal politics? The contribution of this study lies in clarifying the normative boundaries of lawful disclosure while proposing procedural safeguards capable of reconciling constitutional privacy guarantees with criminal justice objectives. By positioning PLN as a public utility entity rather than a private corporation, this research integrates privacy law, criminal procedure, and legal politics into a coherent doctrinal framework that strengthens institutional accountability in the digital governance era.

RESEARCH METHODS

This research employed a normative juridical method to analyze statutory regulations and legal doctrines governing personal data protection and criminal procedural law in Indonesia. Normative juridical research emphasizes the examination of legal norms contained in legislation, authoritative legal interpretations, and doctrinal scholarship in order to assess coherence, hierarchy, and systematic consistency within the legal system (Soekanto, 1986). This method was selected because the issue under examination concerns the interaction between two regulatory regimes and the interpretation of statutory provisions relating to data disclosure for law enforcement purposes.

The primary legal materials consisted of the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 on Personal Data Protection, the Criminal Code, and Law Number 8 of 1981 on Criminal Procedure. These instruments provide the normative foundation for evaluating the rights of personal data subjects, the obligations of data controllers and processors, and the authority of law enforcement agencies. Secondary legal materials included scholarly journal articles published within the last ten years, books on legal politics and constitutional theory, and academic commentaries addressing data protection, proportionality, and obstruction of justice.

A conceptual approach was applied to examine the doctrine of limitation of fundamental rights and the theory of legal politics as an analytical framework for understanding the coexistence of privacy protection and public interest enforcement. In addition, a comparative perspective was utilized to assess the clarity and proportionality of Indonesian regulatory standards by reference to international data protection principles. The analysis was conducted qualitatively through statutory interpretation and systematic examination of legal norms, with particular attention to identifying normative gaps and interpretative ambiguity in the regulation of data disclosure by state-owned enterprises.

RESULTS AND DISCUSSION

The legal position of PT PLN (Persero) within Indonesia's data governance framework must be examined through both quantitative magnitude and normative structure. The scale of customer data under its control directly correlates with the institutional risk associated with disclosure requests from law enforcement authorities. The magnitude of data management is not merely administrative but constitutional in nature, given that any disclosure practice potentially implicates the fundamental rights of a substantial portion of the population. The data demonstrate that household customers constitute the dominant segment, confirming that PLN's data governance responsibilities extend to the majority of Indonesian citizens. Consequently, disclosure practices cannot be treated as routine institutional cooperation but must be assessed within the framework of constitutional proportionality.

Table 1 Classification of PLN Customers in Indonesia (2024)

No	Customer Category	Number of Customers
1	Household	82,465,673
2	Business	5,457,210
3	Industry	308,112
4	Social	1,742,893
5	Government	304,885
6	Public Street Lighting	1,842,519
7	Others	756,000
Total	92,877,292	

Source: PT PLN (Persero), Statistics PLN 2024 (PT PLN, 2024a)

Under the Personal Data Protection Law, data subjects are granted rights including access, rectification, restriction, objection, and withdrawal of consent. These rights reflect recognition of informational self-determination and institutional accountability. However, Article 15 paragraph (1) letter b introduces a limitation mechanism permitting restriction of such rights in the interest of law enforcement. Similarly, Article 50 paragraph (1) letter b provides an exception to confidentiality obligations when disclosure is required for investigative purposes. This normative structure demonstrates that Indonesian data protection law adopts a relative model of privacy protection rather than an absolute one.

Simultaneously, Law Number 8 of 1981 on Criminal Procedure empowers investigators to obtain information necessary to uncover criminal acts and secure evidence. In contemporary investigations, digital and institutional data repositories increasingly serve as evidentiary sources. PLN, as a nationwide utility provider, thus occupies a strategic evidentiary position. The tension that arises does not reflect a contradiction between laws but rather overlapping mandates aimed at protecting different constitutional values: individual privacy and collective security.

The doctrine of limitation of fundamental rights provides the analytical bridge between these mandates. Fundamental rights may be restricted when such limitation is grounded in law, pursues a legitimate aim, and satisfies proportionality. Criminal investigation qualifies as a legitimate aim because it protects public order and the rights of victims. Accordingly, disclosure of customer data for investigative purposes is normatively permissible when it adheres to legality, necessity, and proportionality standards.

However, the primary legal vulnerability lies in interpretative ambiguity regarding scope and procedure. The Personal Data Protection Law does not specify the categories of data that may be disclosed, nor does it establish explicit procedural safeguards such as judicial authorization thresholds or documented necessity tests. In the absence of implementing regulations, institutional discretion becomes the operative mechanism. This regulatory gap generates uncertainty for data controllers and investigative authorities alike.

The potential risk of obstruction of justice further complicates PLN's institutional position. Article 221 of the Criminal Code criminalizes actions that intentionally hinder investigation. Although obstruction traditionally refers to active concealment or interference, expansive interpretation may include refusal to provide requested data. Without clearly defined statutory boundaries, a data controller acting in good faith to protect privacy rights may nonetheless face allegations of obstructing justice. This interpretative elasticity underscores the necessity of regulatory precision (Arfiani et al., 2023). A balanced interpretation requires distinguishing between unlawful obstruction and lawful refusal grounded in proportionality or lack of proper authorization.

Comparative reference to the European regulatory framework highlights the importance of procedural clarity. Article 6 paragraph (1) letters c and e of the General Data Protection Regulation establishes lawful processing where necessary to comply with legal obligations or to perform tasks in the public interest. The European approach emphasizes explicit legal basis and documented authority, thereby reducing discretionary ambiguity (Awwaliyah & Juniarti, 2024). Such structured authorization mechanisms provide stronger institutional protection for data controllers.

In the Indonesian context, legal protection for PLN may be strengthened through cumulative procedural safeguards. Disclosure should occur only upon receipt of formal written authorization issued by competent investigative authorities. The request should clearly specify the legal basis, scope of data

required, relevance to the investigation, and identification of authorized officers. Disclosure must remain strictly proportional, limiting information to what is necessary for investigative purposes. These safeguards function not merely as administrative formalities but as legal protection mechanisms demonstrating compliance with both privacy and criminal law frameworks.

This analysis confirms that Indonesian law already provides normative space for lawful disclosure in the interest of law enforcement. The central issue is not permissibility but regulatory clarity. Without precise procedural standards, institutions such as PLN remain positioned between competing liabilities: civil exposure for excessive disclosure and potential criminal exposure for alleged obstruction.

It must be acknowledged that this study is limited to doctrinal and statutory analysis and does not incorporate empirical examination of investigative practice or judicial interpretation. Future research may enrich the discussion by analyzing court decisions or institutional protocols concerning data disclosure requests. Nevertheless, the normative reconstruction offered in this article provides a foundational framework for strengthening legal certainty within Indonesia's evolving data governance regime.

CONCLUSION

The interaction between the Personal Data Protection Law and criminal procedural regulations reflects the dynamic structure of Indonesian legal politics, in which constitutional guarantees of privacy coexist with the imperative of public order and effective law enforcement. The analysis demonstrates that personal data protection under Law Number 27 of 2022 operates within a relative constitutional framework that permits limitation when grounded in statutory authority and justified by legitimate investigative purposes. As a state-owned enterprise managing extensive and sensitive customer data, PT PLN (Persero) occupies a legally sensitive position that requires careful reconciliation between confidentiality obligations and cooperation with law enforcement agencies. Although Articles 15 and 50 of the Personal Data Protection Law provide normative space for disclosure, the absence of detailed implementing regulations generates interpretative ambiguity regarding scope, proportionality, and procedural safeguards. This ambiguity exposes data controllers to dual institutional risk: liability for excessive disclosure and potential criminal exposure for alleged obstruction of justice. Legal certainty can therefore be strengthened through strict adherence to formal written authorization, proportional disclosure standards, and regulatory refinement that clearly defines permissible categories of data disclosure. Such clarification will ensure balanced protection between constitutional privacy rights and the effective administration of criminal justice within Indonesia's evolving digital governance framework.

REFERENCES

Arfiani, A., Syofyan, S., & Delyarahmi, S. (2023). Problematika penegakan hukum delik obstruction of justice dalam Undang-Undang pemberantasan tindak pidana korupsi. *Swara Justisia, 7*(1), 1–15.

Awwaliyah, R. P., & Juniarti, S. (2024). Perbandingan General Data Protection Regulation (GDPR) dengan regulasi perlindungan data di negara-negara Asia Tenggara. *Jurnal Hukum dan Kewarganegaraan, 12*(2), 45–60.

Habib Shulton, A., & Setiawan, A. (2017). Politik hukum perlindungan HAM di Indonesia. *Jurnal Hukum IAIM NU Metro, 5*(2), 33–47.

Jodi, F. F. (2024). Pemberatan pidana bagi pelaku obstruction of justice dalam sistem hukum Indonesia. *Jurnal Litigasi, 15*(1), 88–102.

Law Number 27 of 2022 on Personal Data Protection (Indonesia).

Law Number 8 of 1981 on Criminal Procedure (Indonesia).

Mahfud, M. D. (2017). *Politik hukum di Indonesia*. Rajawali Pers.

PT PLN (Persero). (2024a). *Statistics PLN 2024*. https://web.pln.co.id

PT PLN (Persero). (2024b). *Kebijakan privasi*. https://layanan.pln.co.id

Rasji, R., Chandra, W., & Hamonangan, M. K. (2025). Hukum sebagai alat rekayasa sosial dalam perspektif modern. *Lex Generalis, 9*(1), 1–18.

Salsabila, S., & Wiraguna, S. A. (2025). Legal liability for personal data breaches under Indonesian law. *Jurnal Ilmu Hukum, 14*(1), 55–72.

Santosa, C. H. (2024). Politik hukum undang-undang bidang ekonomi di Indonesia. *Esensi Hukum, 8*(2), 101–120.

Silalahi, J. A. S., Purba, Y. Y., & Nasution, M. F. (2025). Analisis yuridis mekanisme perlindungan data pribadi dalam sistem informasi elektronik. *Minfo Polgan, 10*(1), 20–36.

Soekanto, S. (1986). *Pengantar penelitian hukum*. UI Press.

The 1945 Constitution of the Republic of Indonesia.