JOURNAL OF LAW AND ECONOMICS
E-ISSN: 2963-7937, P-ISSN: 2963-9204
Volume 4 Number 2, November 2025, pp 145-152.
DOI: https://doi.org/10.56347/jle.v4i2.330.

Personal Data Security Violations in East Jakarta Regional Elections: Legal Analysis Through Personal Data Protection Legislation

Khairul Alwan Albaldan [a*], Nin Yasmine Lisasih [b]
[a*,b] Universitas Esa Unggul, West Jakarta City, Special Capital Region of Jakarta, Indonesia.

ABSTRACT
This research examines the personal data breach case during the East Jakarta regional elections and analyzes the legal responsibilities of the General Elections Commission (KPU) from the perspective of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). Employing a juridical-normative method, statutory-regulatory approach, and conceptual framework, this study investigates the hacking incident involving the Permanent Voters List (DPT) database by a hacker using the pseudonym "Jimbo," who allegedly accessed data of more than 200 million voters. The case violates the principle of legal protection for citizens' privacy rights, as stipulated in the 1945 Constitution and the PDP Law. Within the framework of Satjipto Rahardjo's legal protection theory, personal data protection transcends mere legal norms and must be implemented substantially to ensure justice and public security. This research concludes that KPU's negligence in ensuring cybersecurity constitutes a legal violation and demands accountability alongside strengthened digital data protection policies within Indonesia's democratic system.

ARTICLE HISTORY
Received 22 August 2025
Accepted 1 October 2025
Published 30 November 2025

KEYWORDS
Personal Data Breach; Regional Elections; KPU Accountability; Cybersecurity; Legal Protection Theory.

ABSTRAK
Penelitian ini membahas kasus kebocoran data pribadi dalam penyelenggaraan Pilkada Jakarta Timur dan meninjau tanggung jawab hukum Komisi Pemilihan Umum (KPU) dalam perspektif Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dengan menerapkan metode yuridis-normatif serta pendekatan perundang-undangan dan konseptual, studi ini mengkaji insiden peretasan data Daftar Pemilih Tetap (DPT) oleh peretas bernama samaran "Jimbo", yang diduga berhasil mengakses lebih dari 200 juta data pemilih. Kasus ini dinilai bertentangan dengan prinsip perlindungan hukum atas hak privasi warga negara, sebagaimana ditegaskan dalam UUD 1945 dan UU PDP. Dalam kerangka teori perlindungan hukum Satjipto Rahardjo, perlindungan terhadap data pribadi tidak hanya sebatas norma hukum, tetapi harus diwujudkan secara substansial untuk menjamin keadilan dan rasa aman bagi masyarakat. Penelitian ini menyimpulkan bahwa kelalaian KPU dalam menjamin keamanan siber merupakan bentuk pelanggaran hukum dan menuntut akuntabilitas serta penguatan kebijakan proteksi data digital dalam sistem demokrasi Indonesia.

KATA KUNCI
Kebocoran Data Pribadi; Pilkada, Akuntabilitas KPU; Keamanan Siber; Teori Perlindungan Hukum.

1. Introduction

Democracy represents one of the most frequently invoked concepts worldwide, particularly in nations where citizens struggle to establish governance that genuinely represents their aspirations. At its core, democracy embodies the empowerment of civil society's political forces (Prasetyo, 2025). Consequently, democratic development must accompany efforts to strengthen civil society capacity, guarantee freedom of expression, and create dialogue spaces between the state and citizens. Such measures prevent elite power domination and ensure that citizens' voices receive genuine accommodation in state policies. Indonesia operates under a democratic governance system where individuals possess the right to participate in selecting national leaders, ensuring popular sovereignty and effective governance that serves public interests.

CONTACT Khairul Alwan Albaldan khairul.alwan20006@gmail.com Universitas Esa Unggul, West Jakarta City, Special Capital Region of Jakarta, Indonesia.

Regular power transition mechanisms become necessary (Endah Astuti *et al*., 2024). Therefore, General Elections determine presidents and vice presidents, while Regional Elections (Pilkada) select governors and their deputies, as well as mayors and their deputies, conducted periodically as part of a sustainable democratic system.

Electoral participant data breaches cannot be dismissed lightly. Such incidents significantly damage the reputation and public trust toward the General Elections Commission of the Republic of Indonesia (KPU RI), which society should regard as a reliable institution. When voter personal data becomes available, irresponsible individuals may exploit it for specific interests. The Permanent Voters List (DPT) data breach case during Indonesia's elections demands serious attention, particularly since similar incidents have repeatedly affected KPU RI's systems. The situation generates various suspicions, such as unregistered voters or data collection errors. These assumptions create anxiety among society, especially voters, because their personal data risks misuse. Generally, personal data breaches occur when sensitive individual information—including names, identification numbers, addresses, contacts, medical records, and financial data—becomes exposed or available to unauthorized parties, whether through cyberattacks, negligence, or system abuse.

According to reports from the National Cyber and Crypto Agency of the Republic of Indonesia (BSSN RI), as cited by Nyoman Amie Sandrawati, widespread technology use in Indonesia correlates closely with increased cybercrime, including data hacking (Imran, 2023). Hacking constitutes cybercrime (Sihombing Alfies, 2025) that causes personal data breaches for citizens in the digital era. Such situations represent crimes against democracy, occurring extensively alongside technological development in Indonesia.

During the 2023 data breach incident, KPU RI as election organizer again became a cybercrime target (Michael & Rasji, 2024). The public was shocked by news that approximately 240 million DPT records allegedly leaked from KPU RI's official website. The hacking was allegedly perpetrated by an individual using the pseudonym "Jimbo." Responding to the incident, DPT data and personal information should be protected with strict security systems to prevent hacking attempts, misuse, and personal information sales by irresponsible parties. Article 28G paragraph (1) of the 1945 Constitution, which upholds everyone's right to self-defense, guarantees personal data protection. Furthermore, Article 1 paragraph (1) of the Personal Data Protection Law (PDP Law) of 2022 clarifies that personal data contains information about someone that can reveal their identity, either directly or indirectly, through electronic or non-electronic systems.

Personal data breaches in regional elections carry substantial consequences and can generate various serious repercussions, both directly and indirectly. The most significant impact involves diminished public trust toward election organizing institutions like regional KPUs. When data breaches occur, society tends to doubt the institution's ability to protect personal information security and confidentiality. Moreover, exposed data—such as population identification numbers, home addresses, or full names—risks misuse by careless individuals for violations including fraud, identity falsification, and duplicate voter registration practices in elections.

KPU RI (General Elections Commission of the Republic of Indonesia) plays a role in organizing elections in Indonesia; therefore, the institution holds significant responsibility regarding personal data breaches from the permanent voters list. Consequently, KPU RI must enhance its readiness in organizing elections so data breach problems do not become sources of public concern. Legal protection for personal data becomes extremely necessary to provide security for citizens. Based on the permanent voters' data breach problems, researchers are interested in examining further: "Personal data breaches in East Jakarta regional elections related to the personal data protection law and KPU RI's accountability form in guaranteeing public personal data protection as

election participants in Indonesia?". Research Questions:

1) How are personal data breaches in regional elections analyzed under the Personal Data Protection Law?
2) How are personal data breach problems in East Jakarta regional elections analyzed through legal protection theory?.

2. Methodology

This study employs a juridical-normative method, focusing on the analysis of relevant laws, regulations, and legal standards. Juridical-normative research is conducted by examining regulatory materials related to personal information protection and regional election implementation, which are then analyzed systematically (Tersiana Andra, 2021).

2.1 Research Approach

Two primary methodologies are utilized in this investigation:

1) Statutory Approach is applied to examine various relevant regulations, particularly:
   a) Law Number 27 of 2022 concerning Personal Data Protection
   b) Law Number 10 of 2016 concerning the Election of Governors, Regents, and Mayors
   c) General Elections Commission Regulations (PKPU)
   d) Election Supervisory Body Regulations (Perbawaslu)
2) Conceptual Approach aims to understand the fundamental concepts of personal data protection, privacy rights principles, and the state's obligation to enforce digital information security, specifically within the framework of democracy and regional election administration.

2.2 Data Types and Sources

This research utilizes various types and sources of data as informational materials, including:

1) Primary Data refers to information obtained directly by researchers from original sources or respondents for specific research purposes (Peraturan Pemerintah RI, 2022):
   a) National legislation related to personal data and regional elections:
      1. Law Number 27 of 2022 concerning Personal Data Protection
      2. Law Number 10 of 2016 concerning the Election of Governors, Regents, and Mayors
   b) Official documents from KPU and Bawaslu
   c) Court decisions and rulings (where relevant)
2) Secondary Data constitutes information obtained from other parties and available prior to research implementation. Such data is acquired through existing sources, including:
   a) Reports (Anggen Suari & Sarjana, 2023)
   b) Academic literature such as books, law journals, and scholarly articles
   c) Reports from non-governmental organizations such as ELSAM and SAFEnet
   d) News or media publications covering data breach cases in East Jakarta regional elections.

2.3 Data Collection Technique

Data and information are gathered through library research from various literary sources, meaning systematic access to legal sources and related literature from libraries, online journals, official government documents, and legal databases (Hartono Jogiyanto, 2018).

2.4 Data Analysis Technique

Analysis is conducted qualitatively, employing description, examination, and interpretation of collected legal materials and data (Firmansyah, 2023). The analysis aims to address research questions through a descriptive-analytical approach, subsequently constructing legal arguments that support the research conclusions and recommendations.

3. Results

3.1 Personal Data Breach in East Jakarta Regional Elections Under the Personal Data Protection Law

The data breach at the General Elections Commission (KPU) contradicts provisions within the newly enacted Personal Data Protection Law (UU PDP). While opinions differ regarding voter data transparency, the PDP Law guarantees protection of personal information, including voter records, against misuse or unauthorized disclosure. KPU holds legal responsibility to ensure the security and confidentiality of such data (Saraya Sitta, 2025) and must implement preventive measures against breaches. Violations of PDP Law provisions carry legal sanctions. The leakage of sensitive information such as National Identity Numbers (NIK) and addresses constitutes a violation of the PDP Law. Such data can be exploited for actions harmful to their owners. Law No. 27 of 2022, Article 39 Paragraph (1) states that personal data controllers must prevent illegal access to personal data, while Article 67 Paragraph (1) stipulates that anyone who intentionally and without authority accesses personal data may face criminal sanctions.

Article 39 Paragraph (1) of the Personal Data Protection Law requires personal data controllers to ensure data security by anticipating unauthorized access, unnecessary data collection, and potential misuse. The provision mandates controllers to implement adequate protective measures to prevent illegal access to personal information. Such protection demands not only strengthened technological infrastructure but also enhanced human resource capacity to maintain data integrity. As the data controller, KPU bears responsibility for protecting voter data under its management. The voter data breach reveals negligence in fulfilling these responsibilities, making KPU subject to sanctions under existing regulations. Meanwhile, Article 67 Paragraph (1) contains violation criteria comprising intentional actions, lack of authorization, and targeting of others' personal data. When all these criteria are met, perpetrators may face imprisonment up to five years and/or a maximum fine of Rp 5 billion.

Weak security systems at KPU in managing personal data can be classified as unlawful acts, particularly when data owners suffer losses—a serious matter. Article 20 of the Personal Data Protection Law emphasizes that personal data controllers must ensure protection of data under their management. When controllers fail to implement preventive measures such as encrypted digital systems or internal access restrictions, such failure constitutes negligence leading to legal violations. Several criteria for unlawful acts must be proven:

1) Unlawful acts or negligence (accessing, distributing, or exploiting voter data without authorization)
2) Fault in the form of malicious intent or negligence
3) Actual harm to other parties (such as identity theft or loss of public trust in KPU)
4) Causality between the act and the harm.

3.2 Unlawful Acts or Negligence

Jimbo admitted that his hacking successfully obtained DPT data from the official KPU RI website. Through BreachForums, he shared 500,000 sample data records from the breach via a post, along with several screenshots from https://cekdptonline.kpu.go.id/ as proof of the data's authenticity. In his post, (Michael) Jimbo confirmed that his 2023 hacking successfully breached 204,807,203 unique

records equivalent to the total voters in KPU RI's DPT. The data covered 514 districts/cities in Indonesia and 128 representative countries. During his operation, Jimbo obtained various personal data, including polling station (TPS) numbers, district codes, sub-district and village codes, neighborhood associations (RW), community units (RT), complete addresses, marital status, place and date of birth, gender, full names, Identity Card (KTP) numbers, and National Identity Numbers (NIK).

3.3 Fault in the Form of Malicious Intent or Negligence

Jimbo's actions constitute deliberate acts with malicious intent, where he openly claimed to have hacked the official website of the General Elections Commission, namely cekdptonline.kpu.go.id. In his statement, Jimbo revealed that he successfully obtained and disseminated 500,000 personal data records as samples from the breach. The data includes sensitive information, including TPS numbers, administrative area codes (districts, sub-districts, and villages), RT/RW, complete addresses, marital status, place and date of birth, gender, full names, KTP numbers, and NIK. On the other hand, these actions also reflect negligence by KPU in maintaining data security systems and voter privacy. Insufficient protection of personal data shows that KPU has not implemented adequate cybersecurity standards, ultimately opening gaps for privacy violations and risks of data misuse by irresponsible parties. To prevent similar incidents, KPU needs to strengthen its digital security systems and increase literacy and internal awareness regarding the importance of personal data protection for all stakeholders.

3.4 Actual Harm to Other Parties

The General Elections Commission of the Republic of Indonesia (KPU RI) suffered direct harm. Jimbo explicitly stated he successfully breached the cekdptonline.kpu.go.id system and gained access to the entire Permanent Voter List (DPT). On the BreachForums platform, Jimbo published 500,000 voter data records as examples of the breach and included screenshots of the official KPU website as proof of the obtained data's validity. In his statement, Jimbo revealed that his 2023 hacking successfully accessed 204,807,203 unique voter records, matching the total KPU DPT from 514 districts/cities in Indonesia and 128 overseas representative countries. The leaked personal data includes highly sensitive information, including TPS numbers, administrative area codes (districts, sub-districts, and villages), RT/RW, complete addresses, marital status, place and date of birth, gender, full names, KTP numbers, and NIK. This massive personal information breach causes real harm to society. The widely spread information carries high risks of being misused for identity theft, digital fraud (phishing, social engineering), (Astuti *et al*., 2025) illegal bank account openings, and political targeting or social manipulation. In some cases, victims may face legal or financial consequences because their identities are used without permission in certain transactions.

3.5 Causality Between the Act and the Harm

These actions directly impact violations of individuals' personal data recorded in the KPU system and cause real harm to parties whose data was exposed, in the form of:

1) Identity theft, where other criminals can use NIK and other data to open fake accounts, take out loans, or register for services illegally
2) Personal data-based fraud, such as spreading fake messages or phishing targeting victims using their actual data
3) Violations of privacy rights, which are fundamental rights of every citizen as regulated in Article 28G of the 1945 Constitution and strengthened in Law No. 27 of 2022 on Personal Data Protection

The personal data breach of voters in the General Elections Commission (KPU) system, particularly in the East Jakarta regional election context, systematically violates provisions in Law Number 27 of 2022 on Personal Data Protection (UU PDP). The

violation occurred because KPU, as the personal data controller, could not prevent illegal access to voter data classified as sensitive, such as NIK, addresses, and TPS data. The personal data breach in the East Jakarta regional elections violates citizens' privacy rights and legal protection, reflecting structural and normative shortcomings of electoral institutions in fulfilling constitutional mandates and the PDP Law.

4. Discussion

4.1 Personal Data Breach in East Jakarta Regional Elections Examined Through Legal Protection Theory

The personal data breach in the East Jakarta regional elections directly violates privacy rights guaranteed by the constitution and laws. Data such as NIK, home addresses, KTP numbers, and TPS locations leaked to the public through hacking of the official KPU RI website by an irresponsible party identifying himself as "Jimbo." This violates Article 28G paragraph (1) of the 1945 Constitution and Law No. 27 of 2022 on Personal Data Protection (UU PDP), which emphasizes that every individual has the right to protection of their personal information. Under the PDP Law framework, KPU is obligated as a personal data controller to prevent illegal access to citizens' sensitive information. However, weak digital security systems at KPU demonstrate negligence that causes concrete harm to society (Strategic Studies on National Resilience Journal *et al*., 2023), ranging from identity theft to political manipulation. This falls under unlawful acts as described in Article 39 paragraph (1) and Article 67 paragraph (1) of the PDP Law.

According to Satjipto Rahardjo, law is not merely written regulations (legalistic) (Rahardjo Satjipto, 2019) but a tool to realize substantive justice. In this case, legal protection of personal data must be active and responsive. Protection is insufficient by merely listing norms in legislation but must be realized through preventive and repressive mechanisms. KPU should build strong cybersecurity systems and act swiftly in handling violations (Rima *et al*., 2023). This data breach shows KPU's preventive shortcomings in maintaining data integrity and the absence of adequate repressive efforts by the state to restore the rights of harmed citizens. Based on Satjipto's Legal Protection Theory, the state must provide real protection to citizens, not only formally but also substantively. In this regard, Satjipto offers a framework that law must side with the people, especially when they become victims of the system.

A national-scale data breach is not merely an administrative violation but a threat to democracy itself. In regional elections, personal data holds high sensitivity because it relates to voting rights, political identity, and potential election result manipulation. Therefore, legal protection must emerge through strict regulations, institutional accountability, and public participation in overseeing digital electoral systems. In the East Jakarta regional election context, the issue closely relates to digital voter data usage by KPU, Bawaslu, and third parties such as IT vendors. In several incidents, personal data such as NIK, home addresses, and phone numbers were found spread across unofficial channels and illegally traded. This raises serious concerns regarding:

1) Violations of citizen privacy
2) Data manipulation for political interests
3) Minimal legal accountability from organizing institutions
4) Low awareness and legal protection of digital data

In the case of voter personal data breaches in the East Jakarta regional elections, Satjipto's perspective becomes highly relevant. Legal protection that should be provided to voters extends beyond the mere existence of the PDP Law (Law No. 27 of 2022) but must also include:

1) Preventive Measures KPU and related institutions should have strong data security systems so that public personal data is not easily leaked or hacked.

2) Repressive Measures When breaches occur, the state must provide compensation mechanisms, further protection, and law enforcement against perpetrators.

According to Satjipto, when law cannot provide real protection to society, it loses its meaning of justice. Personal data breaches causing harm or anxiety in society reveal gaps between ideal law and field practices. Therefore, legal protection in this regard must truly be realized through state actions and full responsibility from electoral organizing institutions. The problem of personal data breaches in the East Jakarta regional elections needs examination through substantive legal protection, not merely formal. Satjipto Rahardjo's theory offers a foundation for assessing law's role as an instrument of social justice, especially when citizens are harmed by the state's inability to protect their personal data. There must be legal policies that are simultaneously repressive, preventive, and participatory.

5. Conclusion and Recommendations

The personal data breach issue in the East Jakarta regional elections represents a concrete form of unlawful act, both formally under Law Number 27 of 2022 on Personal Data Protection (UU PDP) and materially from a social justice perspective. In this case, the General Elections Commission (KPU) as the data controller holds legal obligations to prevent illegal access to the permanent voter list (DPT). KPU's inability to anticipate and respond to cyberattacks carried out by a perpetrator using the alias "Jimbo" demonstrates institutional negligence that fulfills the criteria of unlawful acts. This data breach produces not only legal impacts but also socio-political consequences in the form of lost public trust in Indonesia's digital democracy system. Therefore, KPU can be held legally accountable in civil, administrative, and criminal domains if proven to violate Articles 39 and 67 of the PDP Law. Referring to Satjipto Rahardjo's Legal Protection Theory, law should not be viewed as frozen text devoid of reality but as a tool to protect and liberate society from injustice. In this regard, legal protection of personal data extends beyond mere compliance with legislation—it embodies the rule of law principle that guarantees the dignity and privacy of every citizen. Satjipto emphasizes that when law fails to protect vulnerable people or victims, the state must assume substantial responsibility, not merely procedural. Therefore, preventive measures such as building cybersecurity systems, data protection education, and independent oversight systems for data management by KPU must be immediately implemented. On the other hand, repressive measures against cybercrime perpetrators and providing compensation mechanisms to victims also become necessary.

KPU needs to conduct a thorough audit of its information technology systems, including regular penetration testing, data encryption, and implementation of multi-layer security systems. The cekdptonline.kpu.go.id system specifically must be equipped with firewall technology and intrusion detection systems to anticipate future hacking attacks. Given that voter data falls under the sensitive data category, KPU needs to limit access only to information relevant for voter verification purposes. Detailed information such as NIK, complete addresses, and TPS should not be displayed openly on public platforms. The government needs to ensure the implementation of criminal and/or administrative sanctions for KPU's negligence. This is vital so that electoral organizing institutions do not neglect their legal responsibilities and to restore public trust. KPU, Bawaslu, and IT vendors need to strengthen digital security systems with high standards and conduct regular independent audits to prevent data breaches. The state must move beyond rhetoric and provide compensation mechanisms for victims while firmly prosecuting negligent parties and hacking perpetrators to maintain public trust in elections. KPU must also assume substantial responsibility through public reports, transparent

investigations, and system improvements. In line with Satjipto Rahardjo's perspective, law must side with the people and be realized in concrete actions, including building participatory oversight mechanisms involving civil society, academics, and independent institutions to ensure transparency and minimize institutional negligence.

References

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Astuti, E., Suherman, A. M., & Setiady, T. (2024). Implikasi hukum pidana penyalahgunaan data pribadi kasus Dharma Pongrekun Pilkada Jakarta berdasarkan teori penegakan hukum. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora*, *2*(1), 81–95. https://doi.org/10.62383/humif.v2i1.997

Firmansyah, A. (2023). Analisis risiko keamanan siber dalam transformasi digital pelayanan publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2), 12–13. https://doi.org/10.7454/jkskn.v6i2.10082

Hartono, J. (2018). *Metoda pengumpulan dan teknik analisis data* (Vol. 1). Andi.

Imran, M. F. (2023). Cyber criminology: An analysis of the Indonesian and the United States police perception. *International Journal of Cyber Criminology*, *17*(2), 250–261. https://doi.org/10.5281/zenodo.4766715

Michael, M., & Rasji, R. (2024). Analisis yuridis peristiwa kebocoran data daftar pemilih tetap dalam penyelenggaraan pemilihan umum tahun 2024. *Jurnal Ilmu Hukum, Humaniora dan Politik*, *4*(4), 958–967. https://doi.org/10.38035/jihhp.v4i4

Prasetyo, B. (2025). Rekonstruksi hukum pidana terhadap kejahatan siber (cyber crime) dalam sistem peradilan pidana Indonesia. *DJH Dame Journal Hukum*, *1*(1). https://doi.org/10.54254/2753-7048/73/2024.BO17965

Rahardjo, S. (2019). *Teori hukum strategi tertib manusia lintas ruang dan generasi*. Genta Publishing.

Sitta, S. (2025). *Hukum telematika: Regulasi, perlindungan data, dan keamanan siber* (S. I. Andar, Ed.).

Sihombing, A. (2025). *Hukum kejahatan siber*. Zifatamau Jawara.

Tersiana, A. (2021). *Metode penelitian*.

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 195. Jakarta: Sekretariat Negara.