Media Iuris Vol. 7 No. 3, October 2024 p-ISSN: 2721-8384
DOI: 10.20473/mi.v7i3.55931 e-ISSN: 2621-5225
Article history: Submitted 12 March 2024; Accepted 25 September 2024; Available online 18 October 2024.
How to cite: Frendika Suda Utama, Didik Endro Purwoleksono and Taufik Rachman, 'Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection' (2024) 7 Media Iuris.

Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection

Frendika Suda Utama[1], Didik Endro Purwoleksono[2] and Taufik Rachman[3]
[1] Faculty of Law, Universitas Airlangga, Indonesia. E-mail: frendika.suda.utama-2021@fh.unair.ac.id
[2] Faculty of Law, Universitas Airlangga, Indonesia. E-mail: didik.endro@fh.unair.ac.id
[3] Faculty of Law, Universitas Airlangga, Indonesia. E-mail: taufik@fh.unair.ac.id

Keywords:
Data Leaks; Cyber Security; Privacy; Personal Data.

Abstract
Hackers illegally accessed the Indonesian General Elections Commission's (KPU) voter data system to collect voter data to sell to third parties. The regulation requires accountability for voter data leakage to protect people's privacy rights in Indonesia's personal data protection concept. Legal analysis of the modus operandi of personal data sales cases results in patterns of information system vulnerabilities, which can then be used to prevent personal data leakage and improve voter data protection in Indonesian elections. One of the reasons for passing the personal data protection law is the rampant cases of confidential data leakage that occur in government and private institutions in Indonesia. Hackers of voter data systems aim to profit from personal data sold to third parties. The role of the cybersecurity task force team needs to be improved with more concrete arrangements in law enforcement, and mitigating voter data leakage can provide legitimacy for the implementation of credible, reliable, and professional elections in Indonesia. Establishing the task force will optimize the application of voter data systems in conducting general elections in Indonesia and improve personal data protection.

Introduction

Personal Data Protection is closely related to privacy, and this is shown in the relationship between identity, the existence of individuals, communities, corporations managed by government institutions, the public sector, the private sector, and other subjects who collect personal data that are very likely to be connected with other parties.[1] In holding elections in Indonesia, the Indonesian Election Commission (KPU RI) manages voter data and is the election organizing authority in Indonesia. As an election organizer with complete jurisdiction over voter data, the organizer must provide personal data protection on the voter data system application. In this case, data protection concerns all aspects, ranging from collection, processing, research, transmission, and publication to data deletion.[2]

[1] Radi P Romansky and Irina S Noninska, 'Challenges of the Digital Age for Privacy and Personal Data Protection' (2020) 17 Mathematical Biosciences and Engineering 5288.
[2] Helena Toshely Sasmita and others, 'Analisis Faktor Perlindungan Konsumen Dalam Urgensi Pembentukan Undang-Undang Pinjaman Online (Peer To Peer Lending)' (2022) 5 Media Iuris 39.

KPU RI, as an election organizer in Indonesia, must always be independent and transparent about all forms of data regarding the election process and results. The voter data system application was prepared by KPU RI to support the implementation of elections in Indonesia. Support for personal data security and people's need for information are increasing.[3] The information presented by the KPU concerns election result data and ranges from voter, candidate, and political party data to election results data. Technological advances must be aligned with improved cybersecurity in applications used by election administrators in Indonesia.

Voter data collected by the KPU contains personal data of Indonesian residents registered as voters in elections. The identity collected includes full name, ID card or passport identity number, place and date of birth, address, and location of the polling station. Managing the dataset collected from an app for proper use is vital in reducing privacy abuse.[4] The protection of personal data in the voter data system needs to be realized for the legitimacy of elections and the enforcement of proportional personal data protection regulations.

Indonesia does have a PDP Law, but there is still a need for regulations under a PDP Law or technical instructions related to personal data protection to deal with the development of data leakage cases in Indonesia. Today's public relations with internet-based information systems are increasingly inseparable, and even have entered important sectors, namely finance, education, population administration, health, business, and government.[5] In the context of elections, the use of the voter data system by the KPU is actually to facilitate organizers in conveying information and increase speed in processing election results data. Harmonization is needed between the role of election organizers and supervisors in managing election data with institutions tasked with overseeing election data systems and information in Indonesia.[6] Besides data

[3] Serhii Yevseiev and others, 'Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks' (2021) 2021 EUREKA, Physics and Engineering 24.

[4] Shi Cho Cha and others, 'Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges' (2019) 6 IEEE Internet of Things Journal 2159.

[5] Moh Hamzah Hisbulloh, 'The Urgency of the Personal Data Protection Bill' (2021) 37 Unissula Law Journal 119.

[6] Gunardi Lie, Dylan Aldianza Ramadhan and Ahmad Redi, 'The Independent Commission on Personal Data Protection: Quasi-Judiciary and Efforts to Create the Right to Be Forgotten in Indonesia' (2023) 15 Judicial Journal 227.

leakage, factors that encourage this regulation include data theft and the rife sale of personal data by third parties that can harm individual data subjects.[7]

The phenomenon of selling voter data by hackers who have illegal access to the KPU RI voter data system proves that the information system and personal data protection in Indonesia are not entirely secure.[8] Hackers usually use ways to manipulate data from a person and corporations to get something illegally.[9] Hackers generally target apps that store a lot of personal data.[10] Illegal access is a common way for hackers to obtain much information, with the main target being mostly confirmed data. However, not all data collected from the system are necessarily valid.

Information security related to personal data needs to be improved in services in the public sector. In any changes or improvements in the use of data and information, the service provider must also submit a notice to the public service user.[11] Along with globalization and digitalization in public services, every party must pay attention to information security, which is related to the performance of information systems and the use of personal data. The increasing convenience offered in digital services increases the threat in information security.[12] Indonesia already has several legal rules concerning public sector services, such as Law Number 25 of 2009 concerning Public Services, Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE) and Government Regulation Number 17 of 2019 concerning implementing Electronic Systems and Transactions. However, it still needs to be adjusted to the need for personal data protection.

[7] Ditjen Aptika, 'Pentingnya Perlindungan Data Pribadi di Era Digital' (Ministry of Communication & Information Technology, 2021) <https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/> accessed 10 March 2024.

[8] Leski Rizkinaswara, 'Menkominfo Instruksikan Usut Tuntas Dugaan Kebocoran Data DPT' (*Ministry of Communication & Information Technology*, 2021) <https://aptika.kominfo.go.id/2023/11/ menkominfo-instruksikan-usut-tuntas-dugaan-kebocoran-data-dpt/> accessed 10 March 2024.

[9] Pankaj Pandey and Nishchol Mishra, 'Phish-Sight: A New Approach for Phishing Detection Using Dominant Colors on Web Pages and Machine Learning' [2023] International Journal of Information Security.

[10] Van Linh Nguyen and others, 'Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges' (2021) 23 IEEE Communications Surveys and Tutorials 2384.

[11] Dwi Fidhayanti, 'Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/Informasi Konsumen Financial Technology Pada Sektor Mobile Payment' (2020) 11 Jurisdictie: Jurnal Hukum dan Syariah 16.

[12] Domas Maida Budianto, 'Keamanan Informasi Tanggung Jawab Kita Bersama' (Ministry of Finance, 2021) <https://www.djkn.kemenkeu.go.id/kpknl-singkawang/baca-artikel/13136/Keamanan-Informasi-Tanggung-Jawab-Kita-Bersama.html > accessed 12 August 2024.

The PDP Law has mandated the establishment of such an institution, although the specific agency is not yet established. There needs to be an institution that has specific tasks and, more importantly, is independent in supervising personal data. In addition, the PDP Law has regulated the role of officials or officers who carry out personal data protection functions. Still, there are no regulations under the PDP Law that technically regulate this matter. The data protection officer will provide support in processing personal data and provide responses where a personal data breach is possible.[13] Such a vacuum will cause uncertainty in the implementation and supervision to examine the issue of collecting and using personal data in Indonesia. Although a cybersecurity task force team has been formed in response to voter data leakage incidents, the government must establish an institution with supervisory authority over personal data protection.

The PDP Law is the legal foundation for dealing with threats to personal data protection, which has developed dynamically and quickly. The threats that often occur are related to the crime of illegal access and leakage of personal data on systems owned by government agencies, including those associated with the leakage of voter data of the Indonesian Election Commission. Vulnerability mapping in voter data systems needs to be done to provide a picture of cyber threats and minimize the negative impact of the crime. Ransomware is still the main cyber threat that is often faced by individuals or corporations worldwide.[14] Information system audits carried out on an ongoing basis will provide an overview of the integrity of information systems and will provide evaluation information to reduce negligence and fraudulent activities in information systems.[15] Various types of threats in cyberspace can trick victims or take advantage of someone's negligence to take advantage of their personal data, so technological developments must be followed by the ability to detect every potential cybercrime that can harm its users.[16]

[13] Rik Crutzen, Gjalt Jorn Ygram Peters and Christopher Mondschein, 'Why and How We Should Care about the General Data Protection Regulation' (2019) 34 Psychology and Health 1347.

[14] Mamoona Humayun and others, 'Internet of Things and Ransomware: Evolution, Mitigation and Prevention' (Elsevier BV, 1 March 2021) 105.

[15] Petros Lois and others, 'Internal Audits in the Digital Era: Opportunities Risks and Challenges' (2020) 15 EuroMed Journal of Business 205.

[16] Dwiyani Permatasari, 'Tantangan Cyber Security di Era Revolusi Industri 4.0' (*Ministry of Finance*, 2021)<https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-Era-Reavolusi-Industri-40.html> accessed 10 March2024.

The condition of people who cannot do anything when their personal data has been misused is the weakest part of protecting privacy rights in today's digital era.[17] Problems often arise when there is a massive collection of personal data, but if not balanced with serious efforts in managing information systems it will cause the risk of privacy infringement problems.[18] The information system that collects personal data should be accompanied by an information security risk management system to map the vulnerability of violations of personal data privacy.[19] Therefore, it is essential to research the modus operandi of personal data sales cases to map the threat patterns from illegal access and sale of personal data. This study aims to analyze individual data leakage cases from the point of view of personal data protection law in Indonesia to mitigate cyber incidences proportionally.

Research Method

Legal research for this article uses a statute, case, and conceptual approach to obtain critical, neutral papers as academic needs.[20] The statute approach must be the basis for compiling every argument because the ratio legis contains a philosophy that can be explored in regulation. The case approach becomes essential in looking for the modus operandi and ratio decidendi over the findings of the legal facts that are legal considerations in court decisions. The conceptual approach will complement the author's study when finding legal facts that have not received attention from lawmakers.

Case Study on the Modus Operandi of Selling Personal Data

There is urgency of protecting voter data privacy in holding general elections. Privacy is an individual or group of people's resilience in safeguarding their privacy,

[17] Jeeyun (Sophia) Baik, 'Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)' (2020) 52 Telematics and Informatics.

[18] Jay Pil Choi, Doh Shin Jeon and Byung Cheol Kim, 'Privacy and Personal Data Collection with Information Externalities' (2019) 173 Journal of Public Economics 113.

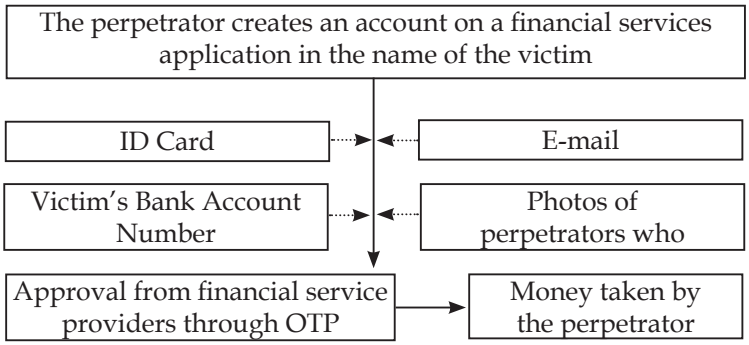
[19] Aggeliki Tsohou and others, 'Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform' (2020) 28 Information and Computer Security 531.

[20] Peter Mahmud Marzuki, *Penelitian Hukum* (Kencana Prenanda Media Group, 2021) 225.

their environment, and every matter related to information about themselves.[21] A privacy disclosure policy should be based on ethical and legal consent in documents, notices, acknowledgments, and consent. The Right to Privacy is a fundamental right equivalent to the right to free expression as a human being. In line with information technology, the right to privacy is directly related to protecting personal data. As a voter data collector, the General Elections Commission is legally obliged to protect the right to privacy and prepare the acting duties requested by the data controller to support compliance with personal data protection in Indonesia.

The mode of operation in leaking personal data can occur not only due to the negligence of the manager who is authorized to collect personal data but also due to the negligence of the data subject. A person's data may be collected by third parties unlawfully, with the intent to gain profit either directly or indirectly. In the first mode, criminals benefit directly from using personal data to take over essential objects or assets of the owner of personal data directly, for example, taking money through access to credit cards, debit cards, fintech, or e-money data. One of the cases that can be discussed in this study is Decision Number 270/Pid.Sus/2023/PN.Btl at the Bantul District Court. In this case, the perpetrator used the victim's data to make online loans and manipulating them so that it seemed as if the perpetrator was a victim; the personal data were then used to activate the application and get OTP from the application service.[22] In this case, the victim immediately experienced material losses, namely, the victim was collected for the loan made by the perpetrator.

Figure 1. Direct Mode of Taking Advantage of the Victim's Personal Data

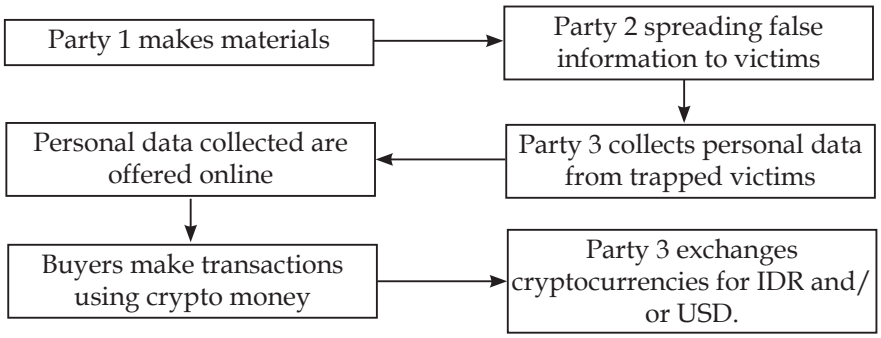


Source: Author's Analysis

[21] Romansky and Noninska (n 1).
[22] Decision Number 270/Pid.Sus/2023/PN.Btl dated October 23, 2023.

In the second mode, criminals get indirect benefits from collecting personal data. One example is a case of a criminal perpetrator spreading false information to his target victims. Then, the deceived victim submits personal data through a link the perpetrator has prepared. When perpetrators have collected personal data from many victims, then they sell that personal data to other parties through illegal data sales community sites. For example, in the case of selling credit card customer data and the case of selling personal data of bank customers, one example is the case analysis study in Decision Number 2575/Pid.Sus/2022/PN.Sby at Surabaya District Court. In this case, the perpetrator is more than one person and then creates a group, with each perpetrator getting a pre-agreed task and role. Some play a role in providing tools and fake formulas that will be distributed to target victims. Then, there is the role of collecting the personal data of victims who have been caught up with false information. Some play a role in selling personal data collected on illegal personal data sales community sites, taking money from transactions to sell personal data.[23] In this case, the victim does not immediately feel the impact of the sale of personal data carried out by the perpetrator because the perpetrator sells the personal data to other parties. Even so, victims are still harmed because their data still have the potential to be misused by parties who buy personal data unlawfully.

Figure 2. A mode that does not directly take advantage of the victim's data



Source: Author's Analysis

Perpetrators of leaking personal data or buying and selling personal data always use means on the internet and mechanisms that are layered and carried out by several

[23] Decision Number 2575/Pid.Sus/2022/PN. Sby dated February 21, 2023.

groups to cause obscurity so that victims find it difficult to report perpetrators or even victims do not feel victimized. In the case of data leaks known to the victim, they can use legal means that the state has regulated.[24] The challenge in developing cybersecurity services is to know early malware behavior to prevent data leakage and the ability to recover from the incident quickly.[25] Protecting personal data should be based on the balanced use of information, and the right to privacy should also be guided by proportionate supervision.

The leakage of personal data is very threatening to privacy, specifically in holding elections in Indonesia. In 2024, selling voter data will impact the risk of privacy violations. The mode of the voter of sale data starts from the event of illegal access to the voter data information system (Sidalih). In the case study, the perpetrators sold voter data from the KPU RI system (Sidalih). The anonymous account "*Jimbo*" offered about 252,327,304 voter data on the hacker site "*breanchforum.is/user-jimbo*" provided at a value of 24 thousand USD. The hacker also submitted 500,000 voter records as examples on the site. The voter data include full name, ID number, Passport Number for overseas voters, gender, place and date of birth, address, and Polling Station Code (TPS). The KPU, based on checks on the lock firewall, has several known IP addresses that have accessed data between November 26 and November 27, 2023. After a cross-check of 500 thousands of data published by hackers, it turned out to be a match, but some were also false. The KPU RI has reported the incident of data leakage and sale of voter data to the police. The KPU RI does this to mitigate illegal access, data leakage, and voter data sales.[26] The KPU RI submitted the case of the position in the trial of case Number 4-PKE-DKPP/I/2024 of the Honorary Council for the Implementation of Indonesian Elections (DKPP RI) on a complaint from Rico Nufriansyah Ali against the Chairman and Members of the KPU RI.

Quality and trusted public services within the KPU RI are regulated in KPU Regulation Number 5 of 2021 concerning implementing the Electronic-Based Government

[24] Amiliya Handayani, 'Legal Protection for Personal Data Theft in Fintech Lending Services Against Cyber Security Threats in Indonesia', vol 6 (2023) <https://e-journal.unair.ac.id/JD>.

[25] Nguyen and others (n 10).

[26] DKPP, 'DKPP Periksa KPU RI Terkait Kebocoran Data DPT Pemilu 2024' (*Honorary Council for the Implementation of Indonesian Elections, 2024)* <https://dkpp.go.id/dkpp-periksa-kpu-ri-terkait-kebocoran-data-dpt-pemilu-2024/> accessed 10 March2024.

System (SPBE). In this regard, KPU RI, as the organizer of SPBE, has been certified ISO/IEC 2001:2023 for information security management system, with IS Certificate Number 762126 with the scope of the information security management system in the provision of data center services, application development, and infrastructure as of February 10, 2022 to February 9, 2025.[27] However, there are always weaknesses in a system, so nothing is absolutely unhackable. On the other hand, the development of technology and hacker knowledge is also racing with the development of cybersecurity technology. Hackers generally try to infiltrate a system, and then they can send personal data to a location they have prepared.[28] The KPU RI also confirmed the voter data leak case in coordination with the cybersecurity task force team consisting of the Criminal Investigation Agency of the Indonesian Police Headquarters (Bareskrim Mabes Polri), the State Cyber and Encryption Agency (BSSN), the State Intelligence Agency (BIN) of the Republic of Indonesia, and the Ministry of Information and Communication of the Republic of Indonesia (Kominfo) to mitigate the data leak.[29] From the coordination, findings were obtained that there was allegedly illegal access, not using the network through VPN, but internet links. The access is not recorded on the lock firewall, based on the results of analysis related to how hackers were suspected of hacking the KPU RI system or, in this case, on Sidalih, how hackers legitimize changing account status. The perpetrators enter each Sidalih portal of the District/City KPU and take voter data.[30]

Legal Analysis of Voter Data Information System Standardization Reviewed in the Perspective of Personal Data Protection in Indonesia

In the era of digitalization of government administration 5.0, information security and digital trust are essential in optimizing public sector services. The biggest challenge in strengthening information security is the limitation of professional personnel and the

[27] Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.

[28] Cha and others (n 4).

[29] KPU, 'Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU' (*Indonesian Elections Commission, 2024*) <https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu> accessed 10 March 2024.

[30] Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.

limited legal basis for cybersecurity.[31] The case of voter data leakage occurred not only in the 2024 election but also in 2020. At that time, a hacker with the username *"Arlins"* then shared 2.3 million voter data from Yogyakarta Province containing names, places, dates of birth, identification numbers (NIK), and addresses.[32] Voter data are a form of information that is not only collected but must also be protected by the KPU RI during elections. The KPU RI is an institution in the public sector that organizes elections and is obliged to strengthen information security on voter data (DPT). Legislation related to information security in public sector services can be found in the following rules:

1. Law Number 14 of 2008 concerning Public Information Disclosure;
2. Law Number 25 of 2009 concerning Public Service;
3. Law Number 11 of 2008 Jo. Law Number 19 of 2016 concerning Information and Electronic Transactions;
4. Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Transaction Systems;
5. Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE);
6. Government Regulation Number 71 of 2019 concerning implementing Electronic Systems and Transactions.

The regulations above have not specifically regulated the protection of personal data. Regarding voter data, the KPU RI has collected data in the category of personal data, so it is appropriate to use more specific legal rules in analyzing cases of voter data leaks in the election of 2024. Therefore, the PDP Law is needed to deal with cases of voter data leaks to get more precise and more systematic regulations related to personal data.

The preparation of the voter list is carried out using a voter data information system (Sidalih) based on KPU RI Decree Number 81 of 2022 concerning the Determination of Continuous Voter Data Information System Applications. Portal Lindungi Hak is a particular application of the KPU RI that is integrated with the population administration information system and other information systems used within the KPU RI as stipulated

[31] Kominfo, 'Pemerintahan Digital Ditopang Keamanan Siber' (*Ministry of Communication & Information Technology*, 2023) <https://www.kominfo.go.id/content/detail/49533/pemerintahan-digital-ditopangkeamanan-siber/0/berita > accessed 12 August 2024.

[32] Laila Alfina Mayasari Rizqi, Syahrico Radya Fahrezi and Tjokorda Istri Diah Candra Permatasari, 'Pengejawantahan EU GDPR Dalam RUU Perlindungan Data Pribadi: Penguatan Perlindungan Data Pemilih Oleh KPU' (2022) 5 Jurist-Diction 2022 <https://rumahpemilu.org/lindungi-data-pribadi-pemilih-kpu-larang-hal-ini/>.

in Article 177 of KPU Regulation Number 7 of 2022. Sidalih is a voter data management system that records and updates voters in the 2024 elections. In addition, for the research agenda and matching voter data, Sidalih uses DP4 data (Election Potential Population Data), which is verified in the field through a *coklit* process. *Coklit* is an activity of the Voter Data Update Officer to update data with their suitability in the field.

Sidalih is an application that has been prepared by the KPU RI as stated in KPU Decree Number 81 of 2022, which is the basis for the rule of law to realize clean, effective, transparent and accountable governance, as well as quality and reliable public services within the KPU RI. In addition, it is also regulated in KPU Regulation Number 5 of 2021 concerning the Implementation of Electronic-Based Government Systems (SPBE). This regulation contains related, among others, SPBE governance, SPBE Management, information and communication technology audits, SPBE implementation, and SPBE monitoring and evaluation.

Application development is regulated explicitly by Article 29 Paragraph 4 of KPU Regulation Number 5 of 2021, which explains that there is an alternative way to make a particular application, namely a work unit that carries out tasks and functions in the field of data and information centers, or in other words from the internal KPU. But it can also be done through the provider. In this case, Sidalih was developed by a team of developers from the Bogor Agricultural University (IPB), who created a particular application for voter data information systems in elections, as conveyed by the KPU RI in the trial of Case Number 4-PKE-DKPP/I/2024 before the DKPP RI assembly.[33] In the 2024 elections, Sidalih's use and development went through the division of labor. KPU is the party that provides the server, VPN access, and access to the virtual machine. Meanwhile, the IPB development team develops applications through coding based on requests from the KPU data and information fields following regulation, updating voter data for the 2024 election with an information system in the form of Sidalih.[34]

If the KPU provides a VPN access server and access to a virtual machine for the development of Sidalih, the server used for the development of the system is the

[33] Ibid (6).
[34] Ibid.

server used during the simultaneous elections in 2019. The physical server is located in the KPU Data Center in the KPU RI office building, Jalan Imam Bonjol number 29, Menteng, Central Jakarta.[35] The person in charge of the control panel is the KPU data and information center (Pusdatin) and the IPB developer team.[36] Then, the KPU IP server architecture is designed for and can only be accessed with the internet network using VPN , as well as SSH Secure Shell.[37] With policies and procedures related to server security, KPU has implemented web application firewall technology, IP reputation and IPS filtering firewalls.[38] Sites and applications created and developed by the IPB developer team for KPU use user groupings of work areas: the central KPU, provincial KPU with 38 websites, city KPU with 514 websites, and KPU abroad with 128 websites.[39]

Regarding application development, voter data are also regulated through Government Regulation Number 71 of 2019 (PP No. 71/2019) concerning the Implementation of Electronic Systems and Transactions. When examined more deeply, PP No. 71/2019 also contains norms related to personal data protection, including in terms of:[40]

1. Definition of personal data (Article 1 (29));
2. Utilization of personal data (Article 2 (5 to 6));
3. Principles of Personal Data Protection (Article 14);
4. Right to erasure of personal data (Article 15 (3)), 16, 17, 18);
5. Obligation to submit information (Article 29 (g));
6. Privacy guarantee for the operator of the electronic agent (Article 37(g)).

In this case, the role of state administrators is to provide information technology and electronic transaction facilities, ensuring security from various kinds of threats due to multiple types of criminal acts or cybercrimes. This regulation is a manifestation of the implementation of existing provisions, namely in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), with the philosophical aim of protecting the right to privacy and freedom of everyone, as well as cybersecurity in technological advances amid a democratic

[35] Ibid.
[36] Ibid.
[37] Ibid (7).
[38] Ibid.
[39] Ibid.
[40] Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

society.[41] Meanwhile, the PDP Law does not yet have implementing rules or government regulations that can be used to tackle crimes against personal data protection.

The incident that occurred in the voter data information system (Sidalih) of the KPU RI, which was accessed by hackers, who then collected voter data in Indonesia then offer the voter data on dark web sites to be sold to third parties to obtain profits from the voter data, clearly violates the provisions in Article 30 Paragraph 2 of Law No. 11 of 2008. This provision has been regulated regarding the prohibition of any person who intentionally and/or without the right to know against the law from accessing computers and/or electronic systems in any way to obtain electronic information and/or documents.[42] In this case, criminal sanctions are also regulated in the form of imprisonment for a maximum of seven years and/or a maximum fine of Rp. 700,000,000.00.

In Indonesia, personal data protection, especially concerning the phenomenon of voter data sales, in the interest of protecting privacy rights, has been regulated by the institution or party that is the controller of personal data responsible for the processing of personal data and shows responsibility in fulfilling obligations to implement personal data protection principles. In the implementation of elections, it is essential to ensure that it can be carried out professionally and proportionately, including:[43]

1. All personal data collected in the implementation of elections must be protected and ensured not to be misused (Protection);
2. In using personal data, election organizers must be based on clear legal rules so that they are recognized by all parties (Legal certainty);
3. In enforcing the law on personal data protection, the KPU RI is obliged to prioritize the interests of the state, defense, and national security (public interest);
4. The implementation of elections must implement personal data protection as a form of contribution to realizing public welfare (Utility);
5. Every election organizer must take into account every risk that has the potential to cause harm in using personal data (Prudence);
6. The aspect of personal data protection in elections must show an equal position between the right to personal data and the rights of the state based on the public interest (Balance);
7. Everyone involved in elections must have a sense of responsibility to ensure that rights and obligations are fulfilled proportionately (Accountability);
8. Personal data in elections must be protected from illegal use (Confidentiality).

[41] Law Number 11 of 2008 concerning Electronic Information and Transactions.
[42] Law Number 11 of 2008 concerning Electronic Information and Transactions.
[43] Law Number 27 of 2022 concerning Personal Data Protection (Article 3).

Specifically related to the data leak in case Number 4-PKE-DKPP/I/2024, the DKPP RI assesses that, regarding the leak of Sidalih voter data, the KPU RI should follow up by guiding the provisions of Article 46 of Law Number 27 of 2022 concerning Personal Data Protection. The KPU RI is required to notify the public as a form of public accountability. As a good election organizer, upholding the principles of honesty, legal certainty, order, openness, and accountability is mandatory. The excuse of the Complainants that the alleged leak of voter data has not been proven because the Bareskrim Polri is still carrying out the investigation stage is not justified according to the ethics of election organizers.[44] Furthermore, the Personal Data Controller must prevent personal data from being unauthorizedly processed, as stipulated in Article 39 Paragraph 1. Suppose there is a failure in personal data protection. In that case, it is mandatory to submit a written notification no later than 3x24 hours, following Article 46 Paragraph 1 of Law Number 27 of 2022. However, regarding the phenomenon of selling voter data, it can be analyzed that hackers who hacked or illegally accessed the KPU voter data information system (Sidalih) have violated the provisions in Article 65 Paragraph 1 and are also regulated regarding criminal sanctions in Article 67 of Law Number 27 of 2022.

Table 1. Comparative Analysis of Regulations in KPU Data Leak Cases

	UU ITE[45]	UU PDP[46]
Subjects	Both of these rules have almost the exact definition of actors, which are limited to individuals and corporations.	
Action	Illegal access to computers, as well as electronic systems, in any way.	Activities that collect personal data from others illegally.
Motif	To obtain electronic information and electronic documents.	This results in the loss of personal data that are subject to benefiting oneself or others.
Legal sanction	Imprisonment for a maximum of seven years and/or a fine of seven hundred million rupiah.	The maximum prison sentence is five years and/or a maximum fine of five hundred million rupiah. Additional penalties include confiscation of profits, assets resulting from the crime, and payment of damages.

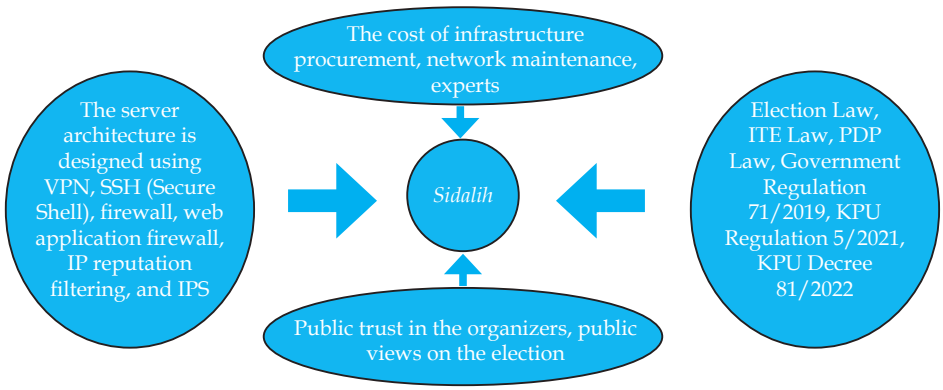
Source: Author's analysis

[44] Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.
[45] Law Number 11 of 2008 concerning Electronic Information and Transactions.
[46] Law Number 27 of 2022 concerning Personal Data Protection.

The norms in Article 65 Paragraph 1 of Law Number 27 of 2022 can be described or elaborated into four main elements.[47] The first element of "everyone" relates to legal subjects, individuals, and corporations. The second element is "unlawfully", actions contrary to the law and the rights of others. So, referring to the legal view of unlawful acts can be interpreted as an act that deprives five rights of other legal subjects, namely life, body, independence, honor, and property.[48] Third, the element "obtaining or collecting personal data that does not belong to him" describes prohibited activities regarding personal data belonging to others collected without the consent of the owner of the personal data. Fourth, the element "to benefit oneself or others that may result in the loss of the personal data subject" concerns the benefits obtained by the perpetrator or third party on personal data that have been misused, which manifestly causes material losses but also indirectly harms the rights of the owner of personal data.

In connection with the rampant leakage of personal data, especially voter data in elections, technology is needed to secure Sidalih as an electronic system. The pathetic dot can provide a theoretical basis for observing the development of digital technology in society. The pathetic dot theory describes four elements that influence the formation of regulations, namely law, social norms, markets, and architecture (technology).[49] Each component has different challenges and functions, but they can support each other and work together.[50] If examined in the case of Sidalih as an electronic system, it has almost similar challenges in the theory.

Figure 3. Challenges faced by Sidalih



Source: Author Using the Pathetic Dot Theory Analogy.[51]

[47] Law Number 27 of 2022 concerning Personal Data Protection.

[48] Didik Endro Purwoleksono, *Perkembangan 3 Pilar Hukum Pidana di Indonesia* (Literasi Nusantara Abadi Group 2023) 75.

[49] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999) 87.

[50] Ibid 88.

[51] Ibid.

The first element is related to the law. Sidalih is regulated and limited by several national legislation rules, namely the Election Law, the ITE Law, the PDP Law, Government Regulation Number 71 of 2019, KPU Regulation Number 5 of 2021, and KPU Decree Number 81 of 2022. Furthermore, there is a social norm, namely Sidalih is a tool that is prepared and used in the implementation of elections, so that if there is a problem in the protection of voter data, it will affect public trust in election organizers, and can even affect public views on the election implementation process. Then there are market challenges, namely the costs related to infrastructure procurement, network maintenance, and human resources, which are experts and skilled in carrying out the Sidalih. The next part is about technology, namely as conveyed by the KPU RI in the examination before the DKPP assembly related to the KPU RI server architecture, which is designed with an internet network using VPN and SSH (Secure Shell) with policies and procedures associated with KPU RI server security applying firewall technology, web application firewall, IP reputation filtering, and IPS.[52] Due to voter data leaks, Sidalih needs to be strengthened by improving information security technology, especially personal data protection. It is necessary to increase the budget to enhance infrastructure and adjust the Election Law to be more accommodating to the development of digital technology, especially regarding personal data protection.

Election law must be adjusted to protect electronic personal data and other developments. The dynamics of the digital era have colored the lives of people around the globe, including Indonesia. The law must be part of welcoming the era of digital transformation to contribute to national development. Law is not only to create order, certainty, and justice but also to become the infrastructure of transformation.[53] Regarding the implementation of elections, the KPU RI and all related institutions need to pay attention to the development of information technology so that legal rules can also be transformed with the development of the cyber world. Adjustments in disclosing events involving technology must be addressed quickly, aligning with digital innovation. The

[52] Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.

[53] Ahmad M Ramli and Tasya Safiranita Ramli, *Hukum sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital* (PT. Refika Aditama 2022) 86.

Election Law accommodates digital transformation, mainly concerning personal data protection. Voter data leaks almost always occur in every election, which shows that it is necessary to make adjustments and anticipate the progress of cybercrime. Law and technology are vital parts of the driving force of national development, and they can reduce the negative impact of global transformation to maintain the sovereignty and identity of the nation.[54] Elections in Indonesia are a big event that most Indonesians attend, so technology should make it easier. Still, it must be aligned with efforts to protect voter data in the era of industrial transformation 5.0.

Conclusion

The modus operandi pattern of selling KPU voter data is closely related to the hackers' motives for profiting from personal data collected through illegal access. Cases of selling personal data target applications or systems that collect large amounts of personal data. The KPU RI voter data system that manages Indonesian voters' data needs to update its security system patterns regularly to obtain information system vulnerability mapping and prevent personal data hacking in the future.

Optimizing the role of the cybersecurity task force team can be an alternative to mitigating data leakage so as not to harm the implementation of elections in Indonesia. Although personal data leakage occurs, information system mitigation must be done quickly and precisely to manage its negative impact and protect other personal data from hacker threats. However, the presence of officers who serve as personal data supervisors in Indonesia will, in principle, further improve the enforcement of personal data protection laws. Lessons that can be learned to enhance personal data protection in the implementation of elections include that the KPU RI needs to synergize with the joint task force on personal data protection, consisting of Polri, BSSN, BIN, Kominfo, and experts or academics. In addition, the government should immediately issue regulations related to data protection officers as mandated by the PDP Law. The Election Law should be able to be adjusted to the development of personal data protection.

[54] Ibid 91.

Acknowledgments

-

Disclosure Statement

No potential conflict of interest was reported by the author.

Funding

No funding was received for this research.

References

Aptika D, 'Pentingnya Perlindungan Data Pribadi di Era Digital' (*Ministry of Communication & Information Technology*, 2021) <https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/> accessed 10 March 2024.

Baik J (Sophia), 'Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)' (2020) 52 Telematics and Informatics.

Budianto DM, 'Keamanan Informasi Tanggung Jawab Kita Bersama' (*Ministry of Finance, 2021*) <https://www.djkn.kemenkeu.go.id/kpknl-singkawang/baca-artikel/13136/Keamanan-Informasi-Tanggung-Jawab-Kita-Bersama.html > accessed 12 August 2024.

Cha SC and others, 'Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges' (2019) 6 IEEE Internet of Things Journal 2159.

Choi JP, Jeon DS and Kim BC, 'Privacy and Personal Data Collection with Information Externalities' (2019) 173 Journal of Public Economics 113.

Crutzen R, Ygram Peters GJ and Mondschein C, 'Why and How We Should Care about the General Data Protection Regulation' (2019) 34 Psychology and Health 1347.

Decision Number 2575/Pid.Sus/2022/PN. Sby dated February 21, 2023.

Decision Number 270/Pid.Sus/2023/PN.Btl dated October 23, 2023.

Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.

DKPP, 'DKPP Periksa KPU RI Terkait Kebocoran Data DPT Pemilu 2024' (*Honorary Council for the Implementation of Indonesian Elections, 2024*) <https://dkpp. go.id/dkpp-periksa-kpu-ri-terkait-kebocoran-data-dpt-pemilu-2024/> accessed 10

March 2024.

Fidhayanti D, 'Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/ Informasi Konsumen Financial Technology Pada Sektor Mobile Payment' (2020) 11 Jurisdictie: Jurnal Hukum dan Syariah 16.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

Handayani A, 'Perlindungan Hukum Atas Tindakan Pencurian Data Pribadi Pada Layanan Fintech Lending Terhadap Ancaman Cyber Security Di Indonesia', vol 6 (2023) <https://e-journal.unair.ac.id/JD>.

Hisbulloh MH, 'Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi' (2021) 37 Jurnal Hukum Unissula 119.

Humayun M and others, 'Internet of Things and Ransomware: Evolution, Mitigation and Prevention' (Elsevier BV, 1 March 2021) 105.

Kominfo, 'Pemerintahan Digital Ditopang Keamanan Siber' (*Ministry of Communication & Information Technology, 2023*) <https://www.kominfo.go.id/content/detail/ 49533/pemerintahan-digital-ditopangkeamanan-siber/0/berita> accessed 12 August 2024.

KPU, 'Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU' (*Indonesian Elections Commission, 2024*) <https://www.kpu.go.id/berita/baca/12118/ siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu> accessed 10 March 2024.

Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 27 of 2022 concerning Personal Data Protection.

Lessig L., *Code and Other Laws of Cyberspace* (Basic Books 1999).

Lie G, Ramadhan DA and Redi A, 'Komisi Independen Perlindungan Data Pribadi: Quasi Peradilan Dan Upaya Terciptanya Right To Be Forgotten Di Indonesia' (2023) 15 Jurnal Yudisial 227.

Lois P and others, 'Internal Audits in the Digital Era: Opportunities Risks and Challenges' (2020) 15 EuroMed Journal of Business 205.

Marzuki PM, *Penelitian Hukum* (Kencana Prenanda Media Group 2021).

Nguyen VL and others, 'Security and Privacy for 6G: A Survey on Prospective

Technologies and Challenges' (2021) 23 IEEE Communications Surveys and Tutorials 2384.

Pandey P and Mishra N, 'Phish-Sight: A New Approach for Phishing Detection Using Dominant Colors on Web Pages and Machine Learning' [2023] International Journal of Information Security.

Permatasari D, 'Tantangan Cyber Security di Era Revolusi Industri 4.0' (*Ministry of Finance, 2021*) <https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-Era-Reavolusi-Industri-40.html> accessed 10 March 2024.

Purwoleksono Didik Endro, *Perkembangan 3 Pilar Hukum Pidana Di Indonesia* (Literasi Nusantara Abadi Group 2023).

Rizqi LAM, Fahrezi SR and Permatasari TIDC, 'Pengejawantahan EU GDPR Dalam RUU Perlindungan Data Pribadi: Penguatan Perlindungan Data Pemilih Oleh KPU' (2022) 5 Jurist-Diction 2022 <https://rumahpemilu.org/lindungi-data-pribadi-pemilih-kpu-larang-hal-ini/>.

Rizkinaswara L, 'Menkominfo Instruksikan Usut Tuntas Dugaan Kebocoran Data DPT' (*Ministry of Communication & Information Technology*, 2021) <https://aptika.kominfo.go.id/2023/11/ menkominfo-instruksikan-usut-tuntas-dugaan-kebocoran-data-dpt/> accessed 10 March 2024.

Ramli AM and Ramli TS, *Hukum sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital* (PT. Refika Aditama 2022).

Romansky RP and Noninska IS, 'Challenges of the Digital Age for Privacy and Personal Data Protection' (2020) 17 Mathematical Biosciences and Engineering 5288.

Sasmita HT and others, 'Analisis Faktor Perlindungan Konsumen Dalam Urgensi Pembentukan Undang-Undang Pinjaman Online (Peer To Peer Lending)' (2022) 5 Media Iuris 39.

Tsohou A and others, 'Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform' (2020) 28 Information and Computer Security 531.

Yevseiev S and others, 'Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks' (2021) 2021 EUREKA, Physics and Engineering 24.