International Journal of Social Science and Human Research

ISSN (print): 2644-0679, ISSN (online): 2644-0695

Volume 07 Issue 08 August 2024

DOI: 10.47191/ijsshr/v7-i08-52**,** Impact factor- 7.876

Page No: 6244-6251

The Integrity of Elections: Urgency of Personal Data Protection in Modern Democracy

Yanita Kusuma[1], Sabri Yanto[2]

[1,2]Universitas Jambi

ABSTRACT: A fair and transparent election is a crucial foundation of modern democracy. Nowadays, in the digitized era, protecting voters' data is essential to ensure the integrity of the electoral process. This study examines the urgency of personal data protection in the context of elections, identifies the main challenges faced, and evaluates the steps that can be taken to address these issues. It uses conceptual, statutory, and legal philosophical approaches. The theories used are Democratic Justice theory and legal protection. Due to increasing threats to data privacy and security, the protection of voter information prevents data misuse and maintains public trust in electoral systems. By analyzing regulations, technology, and best practices in different countries, this study provides policy recommendations to strengthen personal data protection and ensure that elections are fair and transparent. In conclusion, personal data protection is an essential element in maintaining the fairness and integrity of democracy amidst rapid technological development.

KEYWORDS: Democracy, Elections, Legal Protection, Personal Data

I. INTRODUCTION

The 1945 Constitution of the Republic of Indonesia, as amended by Article 28D, stipulates that everyone has the right to recognition, guarantees, protection, and certainty of a just law and equal treatment before the law. These guarantees include personal data. Personal data is sensitive and urgent for confidentiality because it can result in irresponsible use by criminal elements. Not only that, personal data is essentially a person's privacy, within a fundamental right that is protected under the 1945 Constitution of the Republic of Indonesia, as explained in Article 28G Paragraph (1): "Every person has the right to protection of personal data, family, honor, dignity, and property under his/her control, as well as the right to security and protection from threats of fear to do or not to do something which is a human right." Personal data protection is related to the concept of privacy. The concept of privacy is defined as the idea of maintaining personal integrity and dignity(Wahyudi Djafar and Asep Komarudin 2004).

Personal data protection is linked to the concept of privacy. The concept of privacy is the idea of preserving personal integrity and dignity(Rosadi 2015). According to Waren and Brendeis in Rosadi: "Privacy is the right to enjoy life and inviolability, and this development is inevitable and demands legal recognition"(Rosadi 2015). The collection and dissemination of personal data violates a person's privacy because the right to privacy includes deciding whether to provide personal data. Personal data is an asset or commodity of high economic value (Edmon Makarim 2003). Moreover, there is a correlative relationship between the level of trust and protecting specific data from private life. The legal collection of personal data can be legitimised by legal means, although the potential for hacking certainly exists. Therefore, a stronger legal umbrella is needed, in order to create security. Including electoral data in the name of the constitution. In line with what Indriyani stated that the protection of privacy rights to privacy data is very important. It is necessary because it involves a person's identity and human rights. When the identity is hacked, various other crimes will arise, such as fraud, piracy, manipulation, etc (Indriyani Firdaus 2022).

The presence of personal data is currently significant because, in human life, the need for personal data protection is very close. On the one hand, personal data sometimes must be disclosed as part of necessity. On the other hand, personal data must also be kept confidential. This problem cannot be separated from the constitutionality and conception of Indonesia as a state of law. Moreover, personal data is essentially a person's privacy, which is included as a fundamental right protected under the 1945 Constitution of the Republic of Indonesia, as explained in Article 28G Paragraph (1): “Every person has the right to protection of personal data, family, honor, dignity, and property under his/her control, as well as the right to security and protection from threats of fear to do or not to do something which is a human right.”

There are many forms of personal data privacy violation, such as hacking personal data or theft of personal data used for election fraud, which can affect and change the results of vote recapitulation. In such cases, it has an impact on democracy without

integrity. However, Article 1 paragraph (2) of the 1945 Constitution of the Republic of Indonesia stipulates that sovereignty is in the hands of the people and is exercised according to the Constitution. It emphasizes that Indonesia is a constitutional democracy. To implement the principle of popular sovereignty led by wisdom in deliberation and representation, "it is necessary to establish Consultative Institutions and People's Representative Institutions whose members are elected through general elections conducted democratically and transparently as one of the main requirements of democracy."

According to the background of the above problems, and to avoid widespread discussion and not deviate from the actual situation, in this study, the author limits the problem with a problem formulation that focuses on how the protection of voters' data can affect the integrity and fairness of the electoral process, and what are the main threats to voters' data in the digital era and its impact on democracy according to the state institutions of the Republic of Indonesia. This study uses a doctrinal research method with a non-native juridical type through a conceptual approach, a legislative approach, and a legal philosophy approach.

II. FINDING AND DISCUSSION

The progression of the internet and information technology happens very fast, where the ability of every human being or user as a general audience to understand it is not as fast as the development of information technology itself. Hence, it is not uncommon for users to be unaware that they have shared sensitive personal data on the internet, which can then be misused by users and others who want to misuse it. The law's role is to protect personal data for information and communication technology users through legislation. In regards to Article 26 paragraph (1) of Law Number 11 Year 2008 on Electronic Information and Transactions as amended by Law Number 19 Year 2016 (ITE Law), it is stipulated as follows: "Unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's data must be carried out with the consent of the person concerned."

Referring to the description of Article 26 paragraph (1) of the ITE Law above, the protection of personal data is one part of privacy rights, which implies the following:

1. The right to privacy is the right to enjoy a private life and to be free from all kinds of interference;
2. The right to privacy is the right to be able to communicate with others without spying and
3. The right to privacy is the right to control access to information about one's private life and data.

The data protection concept implies that individuals have the right to determine whether or not to share or exchange their data. Individuals also have the right to choose the conditions for personal data transfer. Furthermore, data protection also relates to the concept of the right to privacy. The right to privacy has evolved so that it can be used to formulate the right to protect personal data (Anon 1988).

The right to privacy through data protection is crucial for individual freedom and dignity. Data protection enables the realization of political, spiritual, religious, and even sexual liberties. The right to self-determination, freedom of expression, and privacy are essential to making us human.

The collection and dissemination of personal data violates a person's privacy because the right to privacy includes deciding whether to provide personal data(Anon 1988). Personal data is an asset or commodity of high economic value (Edmon Makarim 2003). In the same way, there is a correlative relationship between the level of trust and the protection of specific data from private life.

In the context of personal data protection regulated in various laws and regulations, the government has not been able to implement personal data protection regulations effectively and optimally because the implementing rules of Law Number 27 Year 2022 on Personal Data Protection have not yet been drafted and there is no special institution that handles disputes in personal data protection.

In the implementation of direct elections, disputes are likely to arise, one of which is a dispute over the results of direct elections. The dispute over the results of the direct elections must be resolved in a manner that is by the law (due process of law), including the authorized institution. Several rules and regulations are related to this matter, and different legal policies exist (Suhartono and Slamet 2016). It can even lead to disputes over election results that must be accounted for. Even disputes related to election data have become complicated.

The election dispute is one of several problems in implementing elections. In 2019, the Constitutional Court ('Constitutional Court') received 470 disputed cases of Application for General Election Results (after this abbreviated as PHPU) in the 2019 General Election. In detail, 215 PHPU applications were filed at the Regency / City DPRD Legislative Election (Pileg) level, 110 at the Provincial DPRD level, 71 at the DPR level, 11 at the DPD level, and one at the Presidential Election level. 62 PHPU requests were not identified at the election level (Dimas Jarot Bayu 2019). The election disputes will be resolved by an institution called the Election Supervisory Agency (Bawaslu). In his article entitled "Transformation of Bawaslu into a Special Court" in 2018, Ruslan Husein provides an alternative view of Bawaslu's duties as a special court. According to Ruslan Husein, in his article titled "Transformation of Bawaslu into a Special Court" in 2018, he provided alternative views on Bawaslu's duties as a special court: (1) a Special Election Court Agency under the Supreme Court; (2) a Special Election Court Agency as an autonomous body; and (3) a Special Election Court that is semi-court in nature (Ruslan Husen 2018).

It can be seen that the electoral dispute resolution mechanism is one of the essential things to ensure that the electoral process does not deviate from democratic values and to protect electoral rights guaranteed in the constitution. However, it can be understood that in a democratic country, the electoral process is measured during the implementation process and judged by how the country resolves electoral issues.

Fairness in the conduct of elections is essential to maintain the continuity of democracy in a country. It involves law enforcement, openness, honesty, and transparency at every stage of the electoral process. In designing and running the electoral process, it must be ensured that every participant and voter has an equal and fair opportunity to participate, thereby producing elections that reflect the people's will. Therefore, the system of fairness in the conduct of elections must be taken seriously and adequately maintained so that there is no abuse of power or injustice in elections. Justice in elections can also be measured by the fairness of using personal data as a reflection of the implementation of democracy according to the Constitution. Data related to the election will be scattered in several stages of the election.

The electoral stages are cyclical, so there is no provision for the beginning or end of the electoral stages. The electoral stages are regulated in General Election Commission Regulation Number 3 of 2022 concerning Stages and Schedules for the Organisation of General Elections in 2024. To achieve democracy with fairness and integrity, the government is obliged to protect the personal data of prospective voters in elections to prevent data leaks that are fatal to each individual.

The regulation on protection of personal data has been regulated in the 1945 Constitution of the Republic of Indonesia, precisely in Chapter XA on Human Rights, which is regulated in Article 28G paragraph (1), which stipulates that "Every person shall have the right to protection of the person, family, honor, dignity, and property under his/her control, and shall have the right to security and protection from threats to do or not to do something which is a human right."

The provision of Article 28G paragraph (1) of the 1945 Constitution mentioned above has affirmed the constitutional recognition of personal protection as an inherent human right for everyone. Although the constitutionally regulated norms do not directly say "personal data" following the characteristics of personal data, which is part of the private identity attached to a person, then according to the author, "protection of personal data" is one of the manifestations of the recognition and regulation of "personal self-protection" inherent to each person. It is, then, firmly stated that the regulation of the protection of personal data attached to each person, according to the author, has gained constitutional legitimacy based on the provisions of Article 28G paragraph (1) of the 1945 Constitution, which gives the characteristics of the protection as a form of recognition and regulation of personal data as an inherent human right of each person.

Furthermore, Article 28I paragraph (4) of the 1945 Constitution states, "The protection, promotion, enforcement, and fulfillment of human rights are the responsibility of the state, especially the government". This arrangement imposes responsibility on the state, especially the Government, to provide protection, promotion, enforcement, and fulfill human rights. In such a position, the recognition and regulation that personal data protection is a form of human rights inherent in every person, then it is the responsibility of the state, especially the Government, to provide protection, promotion, enforcement, and fulfillment of personal data protection inherent in each person. This characteristic ideally becomes a form of responsibility carried out by the Government in following up the constitutional mandate stipulated under Article 28I paragraph (4) of the 1945 Constitution, relating to actions to implement the responsibility for the protection of personal data inherent in each person.

The implementation of the responsibility of the state, especially the Government, to provide protection, promotion, enforcement, and fulfillment of human rights, based on the provisions of Article 28I paragraph (5) of the 1945 Constitution, is provided "To uphold and protect human rights following the principles of a democratic state of law, the implementation of human rights is guaranteed, regulated, and outlined in laws and regulations." With this arrangement, there is a constitutional mandate for the state, especially the Government, to regulate and express the guarantee of protection of human rights, including, in this case, the protection of personal data in the applicable laws and regulations in Indonesia, as a form of enforcement and protection of personal data.

Based on the results of the analysis of the provisions of the articles mentioned above, it can be stated that the regulation of personal data protection, constitutionally based on the 1945 Constitution, has the following characteristics:

1. Personal data protection is a form of recognition and protection of human rights;
2. Everyone is guaranteed the right to the protection of personal data;
3. The State, especially the Government, has the responsibility to protect, promote, enforce, and fulfill the right to personal data protection;
4. The form of personal data enforcement and protection is guaranteed, regulated, and outlined in laws and regulations.

According to the author, the characteristics of the constitutional protection of personal data according to the 1945 Constitution mentioned above should be used as a basis for further regulation of personal data protection in Indonesia.

In this study, the researchers argue that personal data protection must be based on the principle of balance of interests, where the law is seen as an instrument to achieve social justice by balancing various conflicting interests in society. This concept views law as ensuring that the needs and rights of individuals, groups, and society are accommodated and respected. Roscoe Pound, one of the figures known for this theory, underlined the importance of adapting the law to social change and evolving values and

paying attention to the social implications of legal decisions. With this approach, the law is expected to provide certainty and create substantial justice by considering the various interests in society. Guided by the principle of balance of interests, the author hopes that there is a classification that explicitly limits what is transparent and private to create legal certainty and the government's efforts to realize justice.

B. Identifying Personal Data Breaches on Election Results and Democratic Legitimacy

According to the Government Models of Electoral Management, *the election organization* adopted the Government Models of Electoral Management. The government has a central role, and the implementation structure involves various levels, including the Minister of Home Affairs, Governor or Regional Head Level I, Regent/Mayor or Regional Head Level II, Sub-District Head or District Head, to Lurah/Regional Head at the level of the Village following their respective positions. All of them are an integral part of the process of organizing elections.

There is a criticism of elections in Indonesia that they are only held to fulfill the requirements of formal democracy as the entire process and stages of implementation are controlled by the government. This has been the practice for 32 years in Indonesia, where the government has always regulated democracy at various levels. In every election period in Indonesia, there are always changes regarding the technicalities of elections. In this digital era, elections in Indonesia are based on digital data. Digital data is prepared in an integrated manner that can be used for any purpose by the state. This can reduce the privacy rights of citizens.

Warren and Brandeis, William L. Prosser (1960) tried to detail the scope of one's right to privacy by referring to at least four forms of interference with one's private self (William L and Prosser 1960), namely:

a. Interference with one's isolation or solitude or interference with personal relationships;
b. Public disclosure of embarrassing personal facts;
c. Publicity that misrepresents a person to the public;
d. Unauthorized appropriation of a person's likeness for the benefit of others.

Alan Westin defines the right to privacy as the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others. The broad scope of privacy usually makes the number of privacy regulations in a country, both in type and level (A. F. Westin 1967). This is similar to the concept presented by Arthur Miller, who emphasizes the idea of privacy as the ability of individuals to exercise control over the dissemination of information related to themselves.

Furthermore, Julie Innes defines privacy as a condition in which a person has control over their private decision domain, which includes decisions on private access, private information, and private actions. Meanwhile, she describes privacy as a product of love, fondness, and care for others(Julie C. Inness 1992). This is in line with Solove's explanation that the context of privacy includes family, body, gender, home, communication, and one's personal information (Daniel J. Solove 2008). Meanwhile, Gavison sees privacy as a 'complex' concept consisting of 'three independent and reducible elements: confidentiality, anonymity, and solitude.' Each element is independent, as 'loss or violation may result from the intrusion of any of the three elements'.

Privacy has also been identified as a measure of an individual's control over several elements of their private life, which include:

a. Information regarding their self;
b. Confidentiality of their identity or
c. Parties who have sensory access to persons (Ferdinand D. Schoeman (ed) 1984).

The elements above become the basis for the emergence of Personal Data, a form of individual privacy rights that must be kept confidential. The existing development then shows that the law of personal data protection is developing along with the development of technology itself, especially information and communication technology.

In Indonesian public discourse, privacy is often considered a Western (European) concept, just like human rights. This justifies the low level of public awareness about privacy, especially concerning protecting one's data. The public in Indonesia quickly tells others where they live, their date of birth, and all their kinship relationships. It is also common practice in Indonesia to hand over one's KTP (identity card) and other personal identities, which include one's data, to third parties. In the current context, social media users in Indonesia generally openly state their original place of residence (home address), date, month, year of birth, telephone number, and relationship with parents or siblings. These examples show the lack of public awareness to protect their data, which is the private property of each individual. This will increase the possibility of fraud from interested parties, such as theft of personal data, which can harm the individual.

In response to the impacts of personal data theft, the researcher managed to dig deeper and obtain information that in Indonesia itself, the legal concept of protecting one's privacy was only present along with the presence of colonial legislation, especially after the enactment of the Civil Code in 1848, and the Criminal Code in 1915, by the Dutch East Indies colonial government. The prohibition can identify this as entering another person's house or yard without permission or the ban to opening a letter without consent from the Chief Court, which is regulated in Postordonnantie 1935 (Staatsblad 1934 No. 720).

Based on Law Number 7 of 2017 concerning General Elections, several election law problems in Indonesia can be categorized into six categories. These are the six violations that researchers classify in the following table:

Table 1. Classification of Election Offences

No.	Types of Election Violations	Classification of Election Issues
1.	Election Administration Violations	Election administration violations are handled by the KPU, Provincial KPU, and Regency / City KPU. Administrative violations can take the form of violations of education requirements or voter age requirements, violations of the installation of campaign attributes, the prohibition of bringing children under 7 years old or the ban on cross-region convoys.
2.	Election Process Dispute	Meanwhile, "election process disputes are disputes that occur between election participants and disputes that arise between participants and election organizers. Bawaslu has the authority to decide on the settlement of election process disputes (between the KPU and election participants, as well as between election participants), whose decisions must be followed up.
3.	State Administrative Dispute	Election Administrative Disputes arise for two reasons, namely 1. the issuance of the KPU Decree on the determination of Political Parties as Election Participants 2. being dropped from the permanent candidate list due to the issuance of the KPU Decree on determining the permanent candidate list. The institutions authorized to receive, examine, and decide on settling such process disputes are the Election Supervisory Agency (Bawaslu) and the State Administrative Court (PTUN).
4.	Election offences	The resolution of electoral offenses involves election supervisors, police, prosecutors, and courts in a system of resolution similar to that of the criminal justice system.
5.	Violations of the Code of Ethics	Violations of the code of ethics of election administrators are violations of the ethics of election administrators resolved by the permanent Election Organiser Honour Council (DKPP).
6.	Election result dispute	Disputes over election results are the domain of the Constitutional Court to resolve based on the constitutional mandate given (Article 24C paragraph [1]) of the Third Amendment to the 1945 Constitution). The dispute over the election results itself is a dispute between the KPU and the Election Participants regarding the determination of the vote acquisition of the election results, in the sense that if it is considered that there is an error in the results of the vote count conducted by the KPU, then the Election participants can submit a request to the Constitutional Court.

Source: *Processed by the Author Based on Legislation*

The personal data breaches discussed earlier often occur within the categorization of administrative violations. The first is the lack of orderly data management. In the electoral administration, voters' data is first collected and stored. Administrative violations, such as the lack of strict procedures in data management, can lead to data leakage or unauthorized use of data. In some cases, administrative breaches, such as the absence or negligent implementation of security protocols to protect voter data, can result in unauthorized access or misuse of personal data in electoral activities. Another factor is fraud in the use of technology. Information technology in elections (such as e-voting or digital registration systems) increases the risk of data breaches if not properly managed. Administrative errors in the configuration or maintenance of these systems can result in data protection breaches.

Based on the description above, several institutions must resolve election law issues in Indonesia. And how is the relationship between the authority to resolve disputes over election results owned by the Constitutional Court based on Article 24C paragraph (1) of the 1945 Constitution with authority to resolve other electoral legal issues owned by Bawaslu, the District Court, and the High Administrative Court. In this regard, it can be explained that in settlement of disputes over the election results of members of the DPR, DPD, President and Vice President, members of DPRD, and Regional Heads, the Constitutional Court is not only presented with requests for resolution of disputes over results, but also accompanied by arguments related to violations of election administration, election crimes, election administrative disputes, and even violations of the election organizer's code of ethics.

C. The Steps for Resolving Election Disputes in Indonesia

The politics of law is a legal policy or official line (policy) about the law to be enacted, either by making new laws or by replacing old laws to achieve state goals. The politics of law is a choice of laws that will be repealed or not enacted, all intended to achieve state goals as stated in the Preamble of the 1945 Constitution of the Republic of Indonesia (Evi Noviawati 2019).

During the post-independence period, the Indonesian government planned to organize elections. The elections were held to elect people who would later fill the Central Indonesian National Committee (KNIP) institution. KNIP was the first people's representative institution owned by Indonesia. The basis for its formation was Article IV of the Transitional Rules of the 1945 Constitution 186 and Edict Number X 16 October 1945 issued by Moh. Hatta as Vice President of Indonesia. Then, in the following edict, namely the Government Edict dated 3 November 1945, it was stated that the election of members of the people's representative body would be held in January 1946 (Jimly Asshiddiqie 2005).

In general, in an election law dispute, the election issues, as the author has described in the table above, can be divided into six types: (1) election administration violations, (2) election criminal offenses, (3) violations of the election organizer's code of ethics, (4) election process disputes, (5) disputes over election results, and (6) other legal disputes.

Bawaslu's authority in resolving election disputes has increased after the amendment to Law Number 15 of 2011 concerning the implementation of general elections to Law Number 7 of 2017 concerning General Elections, which gives authority to Bawaslu, so that Bawaslu is present not only as a recommendation-giving institution but also as a case decider. This is as stated in Article 461 paragraph (1) of Law Number 7/2017, that Bawaslu, Provincial Bawaslu, Regency, or City Bawaslu receive, examine, review, and decide on election administration violations.

The scope of "administrative violations" faced by Bawaslu is also quite broad. As stated in Article 460 of Law Number 7 of 2017, "administrative violations include violations of procedures, procedures, or mechanisms related to the administration of the election in each stage of the election" Bawaslu, in carrying out its duties, by Law Number 7 of 2017 has the authority to resolve election administration violations which in Article 461 Paragraph (6) states that Bawaslu issues a decision on administrative cases which then in Article 462 states that "KPU, Provincial KPU, and Regency / City KPU are required to follow up on the decisions of Bawaslu, Provincial Bawaslu, and Regency / City Bawaslu no later than 3 (three) working days from the date the decision is read out"

Law 22 of 2007 led to a debate regarding the institution of Bawaslu, which was not mentioned, so some parties filed a judicial review to the Constitutional Court to strengthen the position of Bawaslu. Based on the Constitutional Court Decision Number 11/PUU-VIII/2010 dated 17 March 2010, the Constitutional Court made the general election supervisory institution, in this case, Bawaslu, a unity of the national, permanent, and independent functions of the election administration. The Constitutional Court's decision was also the forerunner of the birth of Law Number 15 of 2011 concerning General Election Organisers.

As technology advances, elections in Indonesia will likely increasingly rely on digital systems for voter registration, voting, and vote counting. Technologies such as blockchain, biometrics, and advanced data security systems could become standardized to ensure transparency and reliability of the electoral process.

In line with the increasing awareness of the importance of personal data protection, it is expected that there will be a strengthening of regulations related to personal data protection in elections. The future of elections in Indonesia concerning digital personal data can be viewed through several essential aspects:

1. Increasing the Use of Technology in the Election Process

Technological advancements will affect various aspects of elections, including voter registration, identity verification, voting, and results counting. Technologies such as biometrics for voter identification, blockchain for data transparency and security, and e-voting systems can be implemented to improve the efficiency and reliability of the electoral process.

The use of technology in electoral processes continues to increase to improve efficiency, transparency and security. Technology can help address the problem of misuse of personal data in various ways; data encryption ensures that stored and transmitted voter personal data is protected from unauthorised access. Only those with the encryption key can read the data. denryption, even if the data is stolen, the information remains inaccessible without the right key.

2. Strengthening Personal Data Protection Regulation

As awareness of the importance of personal data protection grows, the Indonesian government is likely to tighten regulations related to personal data management in the context of elections. The adoption of a Personal Data Protection Law (PDP Law) will provide a clear legal framework to protect voter data from misuse and leakage.

3. Implementation of a Stronger Security System

To prevent cyber threats and protect the integrity of voter data, Indonesia needs to adopt a more sophisticated security system. This includes data encryption, strong firewalls, and other security protocols to ensure voter data is safe from hacking and leaks. Through this activity, stakeholders can continuously monitor in real-time, using a monitoring system that can detect suspicious or anomalous activities and take quick action. Regular data security audits to ensure compliance with security standards and data protection regulations.

4. Improving Transparency and Accountability

Utilizing digital technology can improve the transparency and accountability of the electoral process. For example, blockchain technology allows the entire election process from registration to vote counting, to be transparently tracked and audited, thereby reducing the potential for fraud.

5. Public Education and Awareness

Improving public education and awareness of the importance of personal data protection will be key. Voters need to be provided with sufficient information on how their data is used and protected during the electoral process. Awareness campaigns and training related to data security are also important to increase public trust in the electoral system. Through technology, election organizers and voters can be provided with training and information on the importance of personal data protection and how to secure it. In addition, the use of simulations to train responses to security incidents helps to increase preparedness and awareness of data security risks.

6. Inter-Institutional Collaboration

Collaboration between various government institutions, such as the General Election Commission (KPU), the Election Supervisory Institution (Bawaslu), and the Ministry of Communication and Information Technology, will be key in ensuring the integrity and security of election data. Cooperation with the private sector and international organizations can also help in adopting best practices and the latest technologies. Inter-institution collaboration ensures that regulations related to personal data protection are consistent and uniformly applied across all levels of government and institutions. In addition, the adoption of the same security standards by all institutions involved in the election helps prevent security gaps and ensure better data protection.

Institutions with specialized expertise in data security or information technology can help electoral institutions develop and implement more effective security systems. Sharing resources such as software, hardware and training between institutions can increase efficiency and effectiveness in protecting personal data. Collaboration between institutions enables a rapid and coordinated response to security incidents, such as data leaks or cyberattacks. Together, institutions can develop comprehensive recovery and mitigation plans to minimise the impact of a security incident.

Institutions can work together to educate voters about the importance of personal data protection and the steps they should take to protect their information. Collaboration on providing security training for election officials ensures that they have the necessary knowledge and skills to protect voter data. Furthermore, legal institutions can work with election institutions to ensure that there are strong legal protections against the misuse of personal data and that offences are dealt with robustly. Collaboration with law enforcement institutions ensures that any incidents of personal data misuse are seriously investigated and acted upon.

7. The Development of Digital Infrastructure

The development of adequate digital infrastructure across Indonesia will support the implementation of advanced election technology. This includes equitable internet access, reliable hardware and software, and technical training for election officials. A robust digital infrastructure enables the implementation of more sophisticated security systems, including end-to-end encryption, strong firewalls and intrusion detection. A modern digital infrastructure can provide better protection against cyberattacks such as hacking, malware and phishing that can compromise voters' personal data. In addition, the development of data centres with high security standards ensures that voter data is stored in secure conditions and protected from unauthorised access.

8. Addressing Cyber Risks and Threats

The government needs to be prepared to face and handle various cyber risks and threats that could disrupt the electoral process. It includes developing risk mitigation strategies, conducting cyberattack simulations, and increasing the capacity of cyber emergency response teams. With these measures, Indonesia can move towards a safer, more efficient and reliable electoral future, where voters' personal data is well protected and the integrity of the democratic process is maintained.

CONCLUSIONS

The personal data protection of voters directly affects the integrity and fairness of the electoral process. For example, when voters' data is well protected, public trust in the electoral system increases, which is the main foundation of a healthy democracy. The effective protection prevents data manipulation and electoral fraud, ensuring that every vote is counted fairly and correctly. Without adequate safeguards, the risk of data misuse can undermine public trust, reduce voter turnout, and create unfairness in election results.

In the digital era, voters' data faces various major threats, including cyberattacks, identity theft, and data misuse by third parties. Cyberattacks such as hacking of electoral systems and phishing can result in the leakage of sensitive information. Identity theft can be used for vote manipulation or disinformation. Data misuse by third parties, including technology companies and foreign parties, can influence election results through microtargeting techniques and false information campaigns. These threats' impact on democracy is significant, as they can undermine public trust, compromise the integrity of the electoral process, and create political uncertainty and instability.

The Integrity of Elections: Urgency of Personal Data Protection in Modern Democracy

Protecting voters' data is key to maintaining integrity and fairness in elections. However, without adequate protection, various digital threats can undermine public trust and the integrity of democracy. Therefore, collective efforts from governments, electoral institutions, and communities are needed to address these threats and protect voters' data.

ACKNOWLEDGMENT

The authors express their gratitude to the lecturers who assisted and guided them in writing this article.

REFERENCES

1) F. Westin. 1967. *Privacy and Freedom*. Atheneum, New York .
2) Anon. 1988. *Human Rights Committee General Comment No. 16*.
3) Daniel J. Solove. 2008. *Understanding Privacy, MA, Harvard University Press*. Harvard University Press Cambridge.
4) Dimas Jarot Bayu. 2019. "Jumlah Gugatan Sengketa Pemilu Tahun 2019 Turun 2 Kali Lipat Dibanding 2014 Dalam Https://Katadata.Co.Id/Berita/2019/05/26/Jumlah-Gugatan-Sengketa-Pemilu2019-Turun-2-Kali-Lipat-Dibanding-2014."
5) Edmon Makarim. 2003. *Kompilasi Hukum Telematika*. Jakarta: PT. Raja Grafindo Perkasa.
6) Evi Noviawati. 2019. "Perkembangan Politik Hukum Pemilihan Umum Di Indonesia." *Jurnal Galuh Yustisi,* 7(1).
7) Ferdinand D. Schoeman (ed). 1984. *Philosophical Dimensions of Privacy: An Antology*. Cambridge: Cambridge University Press.
8) Indriyani Firdaus. 2022. "Paya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi Dari Kejahatan Peretasan." *JURNAL RECHTEN: RISET HUKUM DAN HAK ASASI MANUSIA* 4(2):1–30.
9) Jimly Asshiddiqie. 2005. "Implikasi Perubahan UUD 1945 Terhadap Pembangunan Hukum Nasional, Mahkamah Konstitusi Republik Indonesia."
10) Julie C. Inness. 1992. *Privacy, Intimacy, and Isolation, Oxford University Press*. New York: Oxford University Press.
11) Rosadi, SD. 2015. *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional Dan Nasiona*. Jakarta: Refika Aditama.
12) Ruslan Husen. 2018. "Transformasi Bawaslu Menjadi Peradilan Khusus Pemilu," Jurnal Adhyaksa Pemilu 4." 1–5.
13) Suhartono, and Slamet. 2016. "Konstitusionalitas Badan Peradilan Khusus Dan MK Dalam Penyelesaian Sengketa Hasil Pilkada Langsung." *Jurnal Konstitusi* 12(3):503–23.
14) Wahyudi Djafar, and Asep Komarudin. 2004. *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci*. Jakarta: Elsam.
15) William L, and Prosser. 1960. *Privacy: A Legal Analysis*. California Law Review .

There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (https://creativecommons.org/licenses/by-nc/4.0/), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.