DOI : https://doi.org/10.33373/jtp.v8i2.6541

JURNAL TRIAS POLITIKA

2024, Vol 8. No.2 : 292 – 305

e-ISSN: 2597-7423 / p-ISSN: 2597-7431

Journal Homepage : https://www.journal.unrika.ac.id/index.php/jurnaltriaspolitika

SECURING DEMOCRACY IN CYBERSPACE: VOTER DATA LEAKS IN INDONESIA'S 2024 ELECTION

I Putu Hadi Pradnyana [1] *, Rhesa Anggara Utama [2], Ni Wayan Ditha Sasmita[3]

[1, 2] Department of Government Studies, Faculty of Social and Political Sciences, Warmadewa University, Indonesia

[3] Department of Public Administration, Faculty of Social and Political Sciences, Warmadewa University, Indonesia

Abstract: : *This research examines the impact of voter data leaks on the essence of democracy, focusing on participation, accountability, and transparency. Using a descriptive qualitative method and secondary data sources, this research analyzes voter data breach incidents in Indonesia's 2024 general election as case studies. The findings reveal that voter data breaches threaten public participation by reducing voters' sense of security and trust. Additionally, government accountability is undermined due to the failure to protect citizens' personal data, diminishing legitimacy and public trust. The transparency of the electoral process is also negatively affected, hindering the necessary verification and validation for fair and trustworthy election outcomes. The study concludes that proactive measures from the government are essential to enhance cybersecurity, including the development of stringent regulations, investment in advanced security technologies, and increased public awareness. These steps are crucial to protecting voter data, maintaining the integrity of democracy, and ensuring that every vote is counted honestly and transparently. Therefore, the security of voter data is key to preserving public trust and the essence of democracy in the digital age.*

Keywords : *data leaks; 2024 Indonesian election; cyber security; cyberspace; democracy.*

INTRODUCTION

In late November 2023, the Indonesian public was stirred by the issue of a voter data breach hacked by a hacker, affecting 204 million voter records. Reported via CNBC (2023), Head of the Cyber Security Research Institute, The Communication and Information System Security Research Center (CISSReC) said that the KPU data leak was data from the Permanent Voter List (DPT). The anonymous account "Jimbo" claims to have hacked the kpu.go.id site and succeeded in obtaining voter data. The account has shared 500,000 samples on BreachForums, a site commonly used by hackers to sell results data illegally. Reporting from BBC Indonesia (2023), this data contains information on full name, Population Identification Number (NIK), Family Card (KK), Resident Identity Card (KTP), Passport, gender, date of birth, marital status, complete address, as well as codification of Polling Places (TPS).

Responding to this incident, the General Election Commission (KPU) immediately reported it in coordination with the National Cyber and Crypto Agency (BSSN), the Special Criminal Investigation Directorate (Bareskrim), and other related institutions. In an effort to address the problems that have been identified, the KPU conducted a thorough examination of the information systems mentioned by the parties suspected of being the perpetrators of the

* **Corresponding Author**: *hadypradnyana@gmail.com*

Article History :
Received : (18062024)
Revised : (15092024;)
Accepted : (29092024)

threat, in particular the Voter Data Information System (Sidalih). As a precautionary measure, Sidalih user accounts have been disabled (KPU, 2023).

In the connected digital era, data security has become a crucial component in maintaining the essence of democracy. Democracy, whose essence rests on participation, accountability and transparency, relies heavily on the integrity of the information used in the election process. The increasing cases of voter data leaks leading up to elections reveal weaknesses that threaten the foundations of democracy (Bueermann & Dobrygowski, 2023). This background will outline the importance of maintaining data security to ensure free and fair participation, maintain government accountability, and ensure transparency in the democratic process.

Public participation is one of the main pillars of democracy. Elections give citizens the opportunity to voice their opinions through voting. However, effective and inclusive participation requires ensuring that voter information is protected from misuse. Voter data includes sensitive personal information, such as name, address, identification number, and voter preferences. This data leak can intimidate voters and reduce their participation in elections. Threats from malicious parties can result in identity theft, misuse of data for fraud, or even political intimidation. For example, in the United States, cases Cambridge Analytica shows how personal data is used to manipulate voters through targeted social media campaigns (Kanakia et al, 2019).

Public trust in the electoral system is critical to ensuring broad participation. When voter data leaks occur, this trust is shaken. Citizens may feel unsafe providing their information, which can reduce turnout in elections (Browning, 2023). The voter data leak in Indonesia in 2023, which involved millions of personal data being leaked and sold on the internet, shows how incidents like this can erode public trust in the election system. Accountability is a basic principle in democracy that demands transparency and honesty from the government and public institutions. Data security plays an important role in ensuring that governments are held accountable for their actions. To maintain accountability, the public must have access to accurate and transparent information regarding the election process. Data leaks or manipulation of information can hinder effective public oversight. Governments that are unable to protect voter data will face criticism and lose legitimacy. This also impacts the ability of electoral institutions to carry out their duties with integrity. The government has a responsibility to implement and maintain a strong security system to protect voter data from cyber threats. This includes the development of strict regulations and the implementation of advanced technologies such as encryption and intrusion detection systems. Failure to protect voter data not only shows negligence, but can also be considered a violation of citizens' human rights to vote in a safe and secure environment. Transparency in the electoral process is essential to ensure fair and reliable results. Data security is closely related to transparency because secure data enables honest monitoring and verification of the election process.

Data leaks can open up opportunities for manipulation and fraud in elections. For example, manipulation of voter data can result in results that do not reflect the will of the people. In many countries, free and fair elections are seen as a key indicator of democratic health (Brennen & Perault, 2021). An inability to protect voter data could create the impression that the election was rigged or rigged. Secure voter data enables transparent verification and validation of the voting process. This ensures that every vote is counted accurately and that no fraud occurs. When voter data is leaked, the verification process can be hampered by uncertainty regarding the integrity of the data. This can give rise to election disputes that consume time and resources. Several cases of significant voter data leaks demonstrate the direct impact on democracy and the urgent need to improve data security. The 2016 and 2020 elections in the United States (Manheim & Kaplan, 2019) are important examples of how voter data leaks and foreign interference can affect public trust and election integrity. Allegations that voter data was used for targeted disinformation campaigns highlight weaknesses in voter data security systems. The voter data leak case in Indonesia in 2020, involving millions of personal data, shows the vulnerability of the government's data security system. These leaks not only disrupt the election process but also threaten individual privacy and national security.

Data security is an important foundation in maintaining the essence of democracy. Free and fair participation, government accountability, and transparency in the electoral process all depend on the ability to protect voter data from cyber threats. The government has a responsibility to ensure that election systems are properly protected through strict regulations, advanced security technology, and high public awareness (Bueermann & Dobrygowski, 2023). Only then can democracy function effectively and maintain the public trust that is at its core. So, it is interesting to examine the impact of voter data leak incidents on the essence of democracy, which focuses on accountability, transparency and public participation.

Several prior studies have highlighted vulnerabilities in the data protection systems employed by Indonesia's General Election Commission (KPU), focusing particularly on the challenges that the commission faces in safeguarding voter information. Research by Kusnaldi et al. (2022) identifies three key challenges the KPU encountered prior to the enactment of the Personal Data Protection (PDP) Law. First, personal data was dispersed across various stages of election administration, resulting in weak centralized control over sensitive information. This scattered data posed a significant risk for breaches. The second challenge revolved around the regulatory framework for personal data protection, which, at that time, was insufficiently robust. Despite KPU's efforts to institute safeguards through regulations such as PKPU No. 5 of 2021 concerning the Implementation of the Electronic-Based Government System and PKPU No. 5 of 2021 concerning the Continuous Voter Data Update, these provisions were limited in scope. The issue stems from the fact that these regulations only applied internally within the KPU, lacking the binding legal force of a national law, thus weakening their impact.

Moreover, Kusnaldi et al. (2022) emphasize a third major challenge: the lack of widespread data protection literacy among election officials, voters, and participants. Many stakeholders, including voters and election organizers, were either unaware of or did not fully comprehend the implications of personal data protection. This gap in understanding made it difficult to ensure that personal data was handled securely throughout the election process. The study suggests that without a concerted effort to improve awareness of data protection, vulnerabilities would continue to exist within the electoral system, especially when it comes to voter data management.

Similarly, Hadad (2023) delves into the security measures needed for the 2024 elections, specifically focusing on the identification and mitigation of security threats to voter data. According to this study, a comprehensive risk assessment must be conducted to identify potential threats and assess the sensitivity of the data in question. To address these risks, Hadad (2023) advocates for an integrated solution, including end-to-end encryption, firewall and intrusion detection systems to secure networks, and regular updates to security protocols. Hadad's approach underscores the importance of a dynamic, multi-layered defense system that can adapt to emerging threats, particularly as Indonesia's election system becomes increasingly digitalized.

Another relevant contribution is Umagapi (2023), which examines the real-world impacts of voter data breaches and what election organizers can do to address them. This study highlights that data leaks can severely undermine public trust in election outcomes, which is a cornerstone of democratic legitimacy. Umagapi (2023) calls for the KPU to develop a malware-resistant system that is impenetrable to hackers, stressing the need for continuous collaboration between the KPU and other relevant agencies, such as BSSN (National Cyber and Crypto Agency), Bareskrim (Criminal Investigation Unit), developers, and related institutions to secure the election infrastructure. The study also advocates for increased support from the

Indonesian parliament, specifically Commission I and Commission II, to help the KPU strengthen its IT systems and protect them from cyber threats.

While these studies provide valuable insights into data security challenges and proposed solutions, none have explicitly explored the broader implications of data breaches on Indonesia's democratic processes. The potential erosion of public trust, the disruption of electoral integrity, and the subsequent impacts on the overall functioning of democracy remain under-researched. This gap is significant because data security issues are not merely technical problems; they have far-reaching consequences for democratic governance, especially in a country as large and diverse as Indonesia.

Thus, this research aims to fill this critical void by examining the impacts of voter data leaks on the integrity of Indonesia's 2024 elections and, more broadly, on democratic resilience. By exploring the intersection of cybersecurity and democratic stability, this study will provide a deeper understanding of how breaches in personal data protection may erode public trust in democratic institutions. In doing so, it will address an essential but under-examined aspect of the election process in Indonesia, offering new perspectives on safeguarding democracy in the digital age.

METHODOLOGY

This research aims to analyze the issue of voter data security and its impact on democracy, as well as highlighting the need for government attention in improving cyber security. To achieve this goal, the research used a qualitative descriptive method by utilizing secondary data sources. This method was chosen because it allows in-depth exploration and comprehensive analysis of complex phenomena by relying on existing data. The qualitative descriptive method aims to provide a clear and detailed picture of a phenomenon or event. In the context of this research, qualitative descriptive methods are used to: 1) Provide an in-depth understanding of data security issues in the context of democracy, including how voter data leaks affect participation, accountability and transparency, 2) Present a detailed analysis of the impact of voter data leaks on public trust , the integrity of the election process, and the legitimacy of the government, 3) Explain the government's responsibilities in maintaining cyber security and the steps that need to be taken to increase the protection of voter data.

Secondary data sources are data that have been collected by other parties and are available for reuse in research. In this research, secondary data will be used to obtain relevant information and facts from various trusted sources. Secondary data sources that will be used include research reports, scientific publications, journal articles, government documents, news articles, Secondary data collection in this research will go through several stages, namely identifying data sources from various relevant and credible sources to obtain the required data. This includes accessing academic databases, government websites, and trusted news portals. The second is to collect relevant documents, such as research reports, government regulations, and journal articles. This data will be stored and organized systematically to facilitate analysis. Third is reviewing and evaluating the data collected to ensure its relevance and accuracy. Irrelevant or inaccurate data will be eliminated from the analysis.

The qualitative descriptive method with secondary data sources was chosen because it allows researchers to collect and analyze extensive and varied data regarding the issue of voter data security and its impact on democracy. By using various credible secondary data sources, this research is expected to provide in-depth insights and relevant recommendations to improve cyber security and maintain the essence of democracy.

The analysis process involved several key stages. First, each data source was meticulously reviewed to assess its relevance to the central themes of the study, particularly focusing on data security, democratic participation, and the governmental response to cyber threats. Data from these sources were then categorized based on specific themes, such as the technical aspects of data protection, the legal framework surrounding voter data security, and the societal impact of data breaches. This thematic categorization allowed for a structured analysis, where connections between voter data security and democratic outcomes could be clearly drawn.

The next step in the methodology was the synthesis of theoretical observations. This involved comparing the findings from secondary data with existing theoretical frameworks related to cybersecurity, democracy, and governance. By integrating theoretical perspectives, the research aimed to provide a more nuanced analysis of how voter data leaks can influence trust in democratic institutions and the overall legitimacy of electoral processes. The theoretical observation phase also helped identify gaps in current policies and highlighted areas where further government intervention is needed to secure electoral integrity.

The final stage of the analysis focused on triangulating the data. This process involved cross-referencing findings from different sources to ensure consistency and accuracy. Any conflicting data points were examined closely, with efforts made to reconcile differences through additional theoretical interpretation. By applying this multi-stage analysis, the research was able to construct a detailed and reliable narrative around the critical issue of voter data security and its impact on the democratic process in Indonesia.

RESULTS AND DISCUSSION

Data Privacy and Information Security

Between 2020 and 2024, Indonesia has witnessed a significant surge in data breaches, underscoring the country’s vulnerability to cyberattacks and the urgent need for stronger data protection mechanisms. According to the National Cyber and Crypto Agency (BSSN), there were over 979 million cyberattacks in Indonesia in 2020, encompassing phishing attempts, malware attacks, and data breaches aimed at both private and public sector entities. One of the most alarming incidents involved the leak of 230,000 voter records in May 2020, when hackers managed to access personal data, including identification numbers and voting districts, from the General Election Commission (KPU) (BSSN, 2021).

By 2021, data breaches in Indonesia increased in frequency and severity. In August 2021, personal information from 1.3 million citizens, including names and ID numbers, was leaked from the Health Ministry's PeduliLindungi COVID-19 contact tracing application. Additionally, in September 2021, a hacker identified as "Bjorka" released 105 million records from the General Directorate of Civil Registration (Dukcapil), exposing critical personal data to potential misuse (Kompas, 2021; Jakarta Post, 2021).

The pattern of breaches continued throughout 2022 and 2023. In September 2022, Bjorka resurfaced, leaking sensitive government documents along with 26 million records from the state-owned utility firm PLN. This incident sparked renewed concerns about the government's ability to protect critical infrastructure from cyber threats. Moreover, the leak of 1.3 billion SIM card registration data in November 2022, including phone numbers and national identity numbers, represented one of the most damaging breaches in recent years, affecting millions of Indonesians (Tempo, 2022; CNN Indonesia, 2022).

Concerns remained high in 2023 as attempts were made to breach KPU’s voter databases in anticipation of the 2024 elections. Despite the passage of the Personal Data Protection Law (UU PDP) in October 2022, cyberattacks continued to occur at an alarming rate. This highlights the ongoing challenges faced by Indonesia in enforcing its data protection regulations and strengthening its cybersecurity infrastructure (Kominfo, 2022; BSSN, 2023). Statistical data from BSSN and independent cybersecurity firms suggest that between 2020 and 2024, over 3 billion data records have been compromised in various incidents, positioning Indonesia as one of the most affected nations by data breaches in Southeast Asia. This demonstrates the critical need for stronger regulatory frameworks, enhanced cybersecurity practices, and greater public awareness regarding personal data protection (Kaspersky, 2023; Reuters, 2023).

Bruce Schneier (2015) in the book entitled Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World views privacy as a fundamental human right. He believes that control over personal information is an important aspect of individual dignity and autonomy. In his various writings, Schneier consistently emphasizes that privacy is not just a technical issue, but also a social and political issue. Loss of data privacy has broader impacts on society, including the potential for misuse of data by governments or private companies.

Information security is the foundation of data privacy. Schneier (2015) states that without adequate security, personal data is vulnerable to theft and misuse. Many people are unaware of the extent to which their data is collected, stored and used. This is a serious problem because without adequate awareness, the public cannot make informed decisions about how and when they should share their personal information. Schneier (2015) openly criticizes government surveillance practices, especially those that are widespread. Unrestricted surveillance mechanisms only violate privacy, but can also undermine trust between society and government. This trust is important for maintaining social balance and a healthy democracy. Data security and privacy have significant implications on social and political aspects. believes that the way data is collected, used, and secured has a direct impact on the power structures in society. Control over data means control over individual freedom, and thus, privacy and information security become very important issues in the context of civil liberties and human rights.

In this era of digital transformation, one of the fundamental debates is between the need for security and privacy protection. Schneier (2015) discusses how governments often justify surveillance as necessary for national security, but points out that many of these surveillance programs are ineffective and tend to violate civil rights. If this data collection practice is not strictly regulated, it can certainly threaten individual privacy rights. Loss of privacy is not only a personal issue but also has broader social and political implications, including the potential misuse of data for surveillance and social control.

Overall, Bruce Schneier (2015) sees data privacy and information security not just as technical problems, but as issues that have profound consequences for individual freedom, public trust, and power structures in society. Thus, greater action is needed from government, industry and society to protect privacy and ensure information security.

Cyber Attacks and Data Protection

In the current era of digital transformation, elections often involve large-scale data collection and processing, including voters' personal data. This creates cybersecurity risks, such as hacking and the spread of false information, which can influence election results (Morozov, 2013). However, data shows that the trend of cyber attacks in the world is increasing from year to year. If we look more deeply, the most massive type of attack that occurred was Malware and Vulnerabiity. Cyber attacks use malware is one of the most common and damaging forms of digital security threats. Malware is an abbreviation of malicious software, a term for various forms of malicious software designed to damage, disrupt, or allow unauthorized access to a computer system. Meanwhile, cyber attacks that target vulnerabilities or vulnerability, refers to the exploitation of loopholes or weaknesses in security systems, software, or hardware (National Cyber Security Center, 2016). Attackers exploit these vulnerabilities to perform unauthorized access, steal data, or cause damage. Cyber attacks in form malware nor vulnerability can threaten various sectors, including in the context of elections. The most crucial thing in this issue is protecting voter data. The following graphs show trends and types of cyber attacks in 2023:

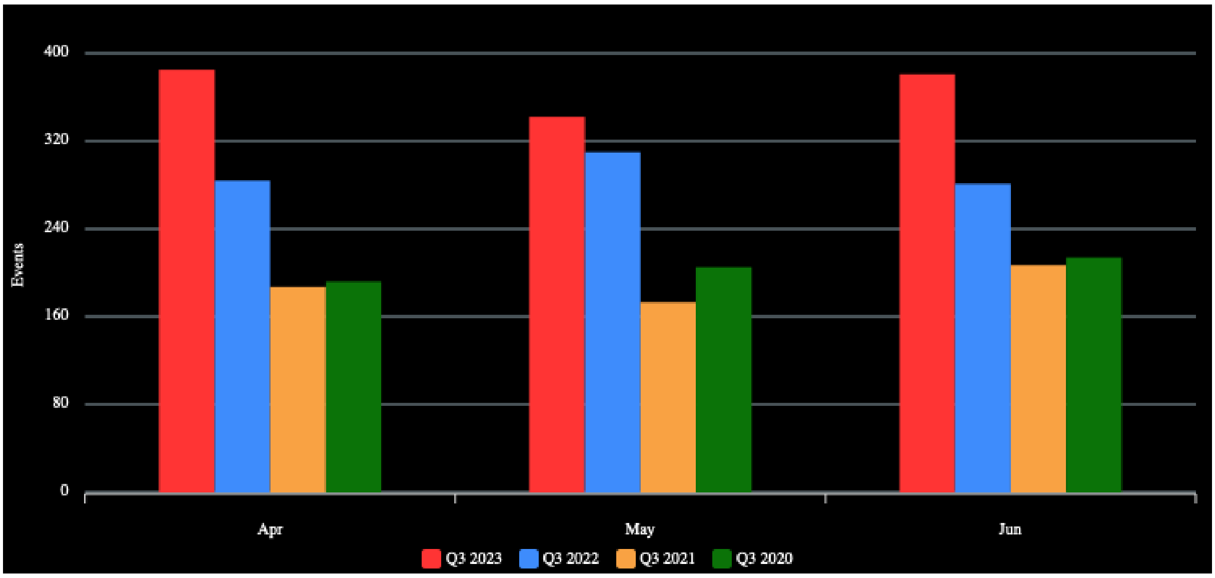

Figure 1. Number of Cyber Attack Incidents in 2020-2023
Source: Hackmageddon, 2023

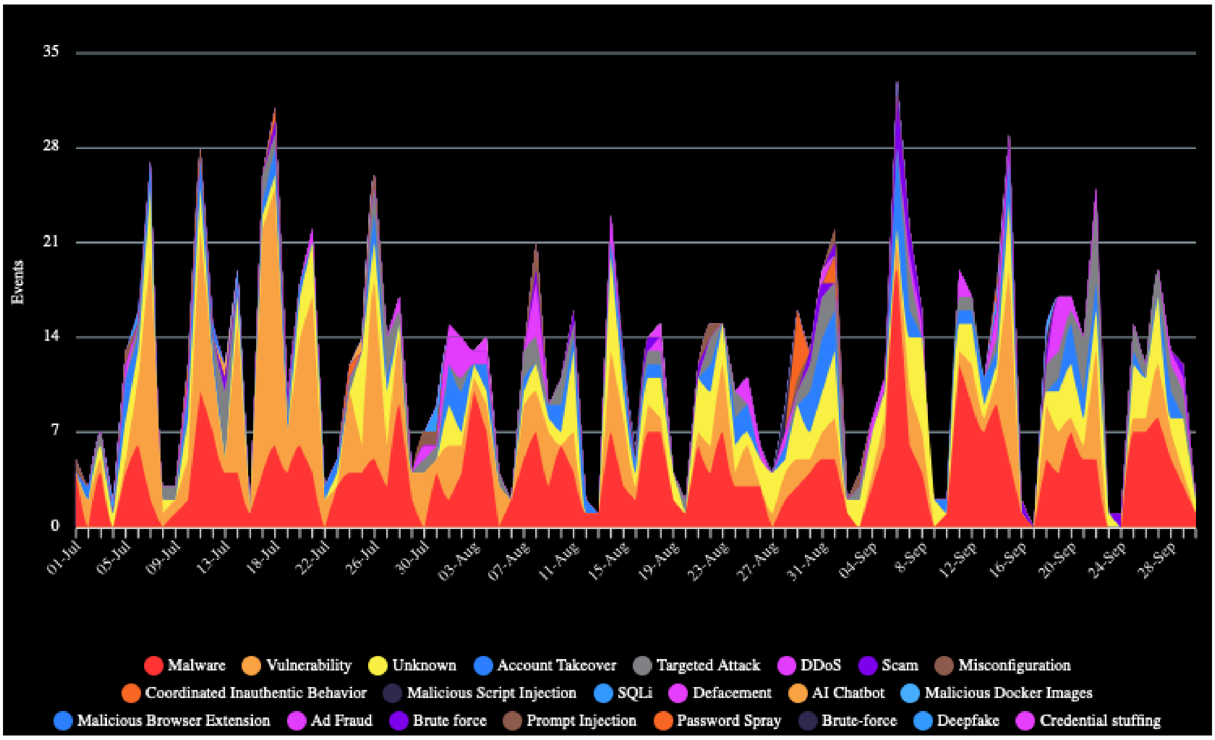

Figure 2. Types of Cyber Attacks 2023
Source: Hackmageddon, 2023

Increasing protection efforts in cyber security and data protection policies is essential, including in the election context. Data security in elections is a multidimensional issue rooted in basic democratic principles such as transparency, accountability, participation, fairness and political stability (Goldman, 2022; Zhang et al, 2022; Manheim & Kaplan, 2019; Browning, 2023). Failure to maintain data security can have far-reaching consequences, not only on the integrity of the electoral process, but also on the trust and effectiveness of democracy as a system of government. In this regard, the public sector and individual data are one of the most massive targets of cyber attacks, as explained in the following graph:

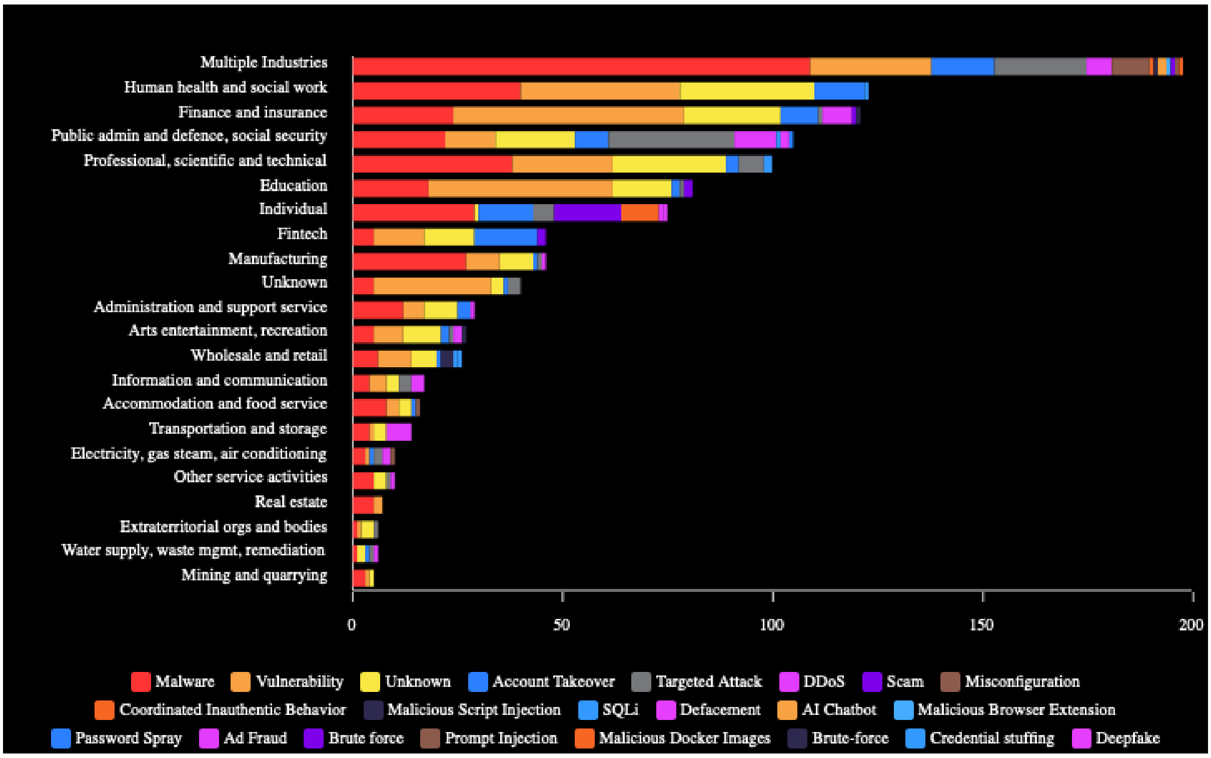

Figure 3. Cyber Attack Targets 2023
Source: Hackmageddon, 2023

Based on the statistical data above, it can be seen how vulnerable public data assets are in the digital space. The high level of cyber threats in the public domain has made data security issues increasingly highlighted. Ideally, various public activities in cyber or digital space should receive proper protection from the government, not only for business, public services, health, education, but also for general elections. The arena of political contestation needs to be reviewed for stakeholders to avoid cyber attack incidents such as theft of voters' personal data, manipulation of election results, spread of fake news or hoax, and so forth. If this is not anticipated effectively, it will have a negative impact on democracy, where democracy must essentially guarantee accountability, transparency and participation.

The Impact of Voter Data Leaks on the Essence of Democracy

Democracy focuses on the process of substantive public participation in general elections (Lessig, 1999; Schneier, 2010; Dahl, 1976). Lawrence Lessig (1999) in The Law of the Horse: What Cyberlaw Might Teach, declared transparency and accountability as the two pillars of democracy. Transparency in elections is achieved when there is certainty that the data used and produced in the election process is accurate and not manipulated. Accountability, on the other hand, is closely related to the ability to track and verify that data. Bruce Schneier (2010) elaborates on the importance of protecting information from unauthorized access, use, disclosure, interference, modification, inspection, recording or destruction. This is very relevant in the context of elections, the integrity and confidentiality of voter data and voting results must be maintained to ensure the legitimacy of the democratic process. Robert Dahl (1971), in his work Polyarchy: Participation and Opposition argued that people's participation in elections is the essence of democracy.

The issue of data security in the context of elections and democracy is attracting attention in this era of digital transformation. From a theoretical point of view, data security in elections is not only a technical issue, but also a matter that is closely related to the foundations of democracy itself. This narrative will explain theoretically why data security is an important element in the electoral and democratic process. Finally, data security in elections is not just a technical issue, but is a fundamental element in supporting democratic principles. As various experts have pointed out, data security affects transparency, accountability, participation, trust and fairness in the electoral process. Without adequate data security, the quality of democracy can be threatened and degraded. Various research results have linked the relevance of data security (Morozov, 2013; Schneier, 2010), transparency and accountability (Lessig, 1999), and public trust in the election process (Nye, 2021).

Democracy focuses on aspects of community participation to reach political resources. Participation can only occur in an atmosphere free from fear, one of which is misuse of personal data. Concerns over data security can reduce political participation, which in turn affects the legitimacy of elections and democracy itself. Therefore, data security is not only a technical matter, but also a political and social matter that influences public participation and trust. When linked to the concepts of transparency and accountability from Lessig (1999), data security guarantees these two aspects, ensuring that every vote is counted fairly and that election results authentically reflect the will of the people. Apart from that, the issue of voter data security is crucial to public trust. Joseph S. Nye (2021) in Soft Power: the Evolution of a Concept argue that trust is an important asset in international and domestic relations. In the context of elections, public trust in the election system is highly dependent on their trust in data security. If this trust is damaged, there could be damage to the reputation of democratic institutions and a decline in public trust in government.

Leaks of voter data in elections have a significant impact on the essence of democracy, especially on aspects of participation, accountability and transparency (Goldman, 2022; Zhang et al, 2022; Manheim & Kaplan, 2019). Public participation in elections is one of the main pillars of democracy, where citizens have the right to vote freely and without intimidation. However, voter data leaks that include sensitive personal information such as names, addresses, and identification numbers, can raise concerns and fears among voters. When personal data is exposed and misused, voters may feel threatened and unsafe, ultimately reducing their participation in the electoral process. For example, leaks of voter data in the United States in the 2016 and 2020 elections revealed how the data was used for targeted disinformation campaigns, influencing voter choices and creating distrust of the electoral system (Manheim & Kaplan, 2019).

On the other hand, government accountability is also seriously disrupted due to voter data leaks. Accountability requires governments and public institutions to act transparently and responsibly towards their citizens (Browning, 2023). When data leak incidents occur, governments are deemed to have failed to protect citizens' privacy rights and pointed out weaknesses in their security systems. This can trigger public criticism and reduce the government's legitimacy, which in turn disrupts political stability and public trust in democratic institutions. In Indonesia, for example, a voter data leak in 2020 involving millions of personal data shows how government failure to protect sensitive data can undermine accountability and lead to a crisis of trust.

The transparency aspect is also greatly affected by voter data leaks (Browning, 2023). Transparency in the election process ensures that every step from voter registration to vote counting is carried out honestly and can be monitored by the public. However, when voter data is leaked, the integrity and reliability of the election process is called into question. Data leaks can open up opportunities for manipulation and fraud, undermining public confidence in election results. The verification and validation processes normally undertaken to ensure votes are counted correctly can be hampered by doubts about compromised data. This creates a situation where election results may not reflect the will of the people, and protracted election disputes may result.

The cumulative impact of voter data leaks damages the essence of democracy, namely free and fair participation, government accountability and transparency in the election process. This incident shows how important cybersecurity is in protecting voter data to maintain the integrity of democracy. Without appropriate measures to improve data security, risks to democratic processes will remain high, threatening political stability and citizens' basic rights. Governments must take responsibility for strengthening cybersecurity systems, implementing strict regulations, and ensuring that every citizen can participate in elections safely and confidently that their votes will be counted honestly. In this way, the essence of democracy can be maintained, and public confidence in the electoral system can be restored.

CONCLUSION

This research emphasizes the importance of voter data security as the main foundation in maintaining the essence of democracy. The voter data leak incident that occurred in Indonesia in November 2023 shows how fragile the election system is in this digital era, and how threats to cyber security can have a broad impact on voter participation, government accountability and transparency in the democratic process. Voter participation is one of the main essences of democracy. The freedom and security to vote without fear or intimidation is a fundamental right of every citizen. However, when voter data is leaked and misused, this sense of security is threatened. Voters may become reluctant to participate due to concerns about the consequences of using their personal data. This phenomenon not only reduces participation rates but also disrupts fair and inclusive representation in elections. Voter data leaks that occurred in the United States and Indonesia reveal that threats to privacy can give rise to deep distrust in election systems.

Government accountability is also seriously affected by incidents of voter data leaks. A government that fails to protect the personal data of its citizens shows weaknesses in its governance and responsibilities. This could lead to a serious crisis of trust, where citizens feel that the government is unable to protect their basic rights. This inability reflects injustice and lack of transparency that erodes the government's legitimacy. The data leak case in Indonesia is a clear example of how negligence in protecting voter data can damage reputation and trust in democratic institutions. Additionally, transparency in the electoral process is essential to ensure fairness and honesty. Transparency allows the public and independent monitors to monitor every stage of the election and ensure that there is no manipulation or fraud. However, when voter data is leaked, this process becomes compromised. Public confidence in election results declines, and time- and resource-consuming election disputes can occur. Without trust in the electoral system, democracy itself is in danger.

This research shows that to protect the essence of democracy, governments must take proactive steps to improve cybersecurity. This includes developing strict regulations, investing in advanced security technologies, and increasing public awareness and education regarding the importance of data security. Governments must also work with the international community to develop strong global security standards and ensure that every country has reliable data protection systems. Ultimately, voter data security is key to maintaining the integrity of democracy. Without adequate safeguards, risks to free and fair participation, government accountability, and transparency of the electoral process will remain high. The government has a major responsibility to ensure that voter data is properly protected, so that public trust in the democratic process can be maintained. In this way, democracy can continue to function well, giving every citizen a voice, and ensuring that every vote is counted honestly and transparently. Only with strong data security can the essence of democracy be safeguarded and preserved for future generations.

This research faces certain limitations, particularly in accessing comprehensive statistical data on voter data breaches in Indonesia. One of the primary challenges is the lack of publicly available and detailed government reports that specifically address data leaks within the electoral system. While general data breaches and cyberattacks in Indonesia have been widely reported, specific cases involving voter data during election periods remain underreported or insufficiently documented. This limitation arises from the sensitive nature of the data, the potential reputational damage to the institutions involved, and the often-classified status of cyberattack investigations. As a result, this research is reliant on fragmented data from various sources such as media reports, third-party cybersecurity firms, and academic studies, which may not provide a fully accurate picture of the scale and impact of voter data leaks in Indonesia.

Additionally, the lack of standardized reporting mechanisms and transparency from relevant government bodies, such as the General Election Commission (KPU) and the National Cyber and Crypto Agency (BSSN), further complicates the process of gathering accurate and comprehensive data. This limitation hinders the ability to conduct a thorough quantitative analysis of the frequency, scope, and specific vulnerabilities in the election systems that have led to these data breaches. As such, the research is primarily qualitative in nature, focusing on theoretical exploration and secondary data analysis rather than statistical modeling or empirical data verification.

For future research, several options could be explored to overcome these limitations. First, there is a need for closer collaboration with government agencies, allowing researchers access to more detailed and confidential reports on electoral cybersecurity issues. Establishing formal partnerships with institutions such as BSSN, KPU, and the Ministry of Communication and Information Technology (Kominfo) would provide access to internal documents and data that are currently unavailable to the public. Second, future research could focus on developing case studies that examine similar incidents of electoral data breaches in other countries, allowing for comparative analysis and the identification of best practices that could be applied in Indonesia. Such comparative studies would help contextualize Indonesia’s cybersecurity challenges in a global framework and highlight areas for improvement.

Another potential direction for future research is the integration of advanced data analytics techniques, such as machine learning and big data analysis, to predict and assess vulnerabilities in the electoral system. By leveraging large datasets and identifying patterns in cyberattack strategies, researchers could contribute to the proactive identification of risks and provide data-driven recommendations to improve the cybersecurity of voter data. Lastly, future research should also include longitudinal studies that monitor the effectiveness of newly implemented policies, such as the Personal Data Protection Law (UU PDP), and evaluate whether these measures successfully mitigate the risks of data breaches in future election cycles.

REFERENCES

Ahuja, V., & Shakeel, M. (2017). Twitter Presence of Jet Airways-Deriving Customer Insights Using Netnography and Wordclouds. Procedia Computer Science, 122, 17–24. https://doi.org/10.1016/j.procs.2017.11.336

Bawaslu. (2023). *Tegaskan Dugaan Kebocoran Data Pemilih Bukan Dari Bawaslu, Bagja Minta KPU Segera Respon Sumber Data*. https://www.bawaslu.go.id/id/berita/tegaskan-dugaan-kebocoran-data-pemilih-bukan-dari-bawaslu-bagja-minta-kpu-segera-respon

BBC Indonesia. (2023). *Ratusan juta data pemilih dari situs KPU diduga diretas, apa akibatnya?*. https://www.bbc.com/indonesia/articles/cgxpk9k3ye5o

Bowler Jr, G. M. (2010). Netnography: A method specifically designed to study cultures and communities online. The Qualitative Report, 15(5), 1270.

Brennen, J. and M. Perault (2021). How to increase transparency for political ads on social media, Brookings, https://www.brookings.edu/articles/how-to-increase-transparency-for-political-ads-on-social-media/.

Browning, Amy I. (2023). A Qualitative Analysis of the Relationship Between Cyberthreats and Democratic Backsliding. *Cybersecurity Undergraduate Research*. 7. https://digitalcommons.odu.edu/covacci-undergraduateresearch/2023spring/projects/7Bueermann, Gretchen & Dobrydowski, Daniel. (2023). *From deepfakes to social engineering, here's what to know about elections, cybersecurity and AI*. https://www.weforum.org/agenda/2023/11/elections-cybersecurity-ai-deep-fakes-social-engineering/

BSSN. (2021). Laporan tahunan ancaman siber di Indonesia 2020. National Cyber and Crypto Agency.

BSSN. (2023). Cybersecurity incidents in Indonesia: 2023 report. National Cyber and Crypto Agency.

CNBC Indonesia. (2023). *204 Juta Data Pemilih KPU Dibobol, Ancam Integritas Pemilu?.* https://www.cnbcindonesia.com/tech/20231201110304-39-493711/204-juta-data-pemilih-kpu-dibobol-ancam-integritas-pemilu

CNN Indonesia. (2022). 1,3 Miliar Data SIM Card Diduga Bocor di Forum Gelap, Kominfo Bantah. https://www.cnnindonesia.com/teknologi/20220901122745-192-841874/13-miliar-data-sim-card-diduga-bocor-di-forum-gelap-kominfo-bantah.

Dahl, Robert A.. (1972). Polyarchy Participation and Opposition. London: Yale University Press.

DPR RI. (2023). *204 Juta DPT Pemilu Bocor, Sukamta Ingatkan KPU Tindaklanjuti Secara Serius*. https://www.dpr.go.id/berita/detail/id/47962/t/204%20Juta%20DPT%20Pemilu%20Bocor,%20Sukamta%20Ingatkan%20KPU%20Tindaklanjuti%20Secara%20Serius

Fidler, David P., "The U.S. Election Hacks, Cybersecurity, and International Law" (2017). Articles by Maurer Faculty. 2607. http://www.repository.law.indiana.edu/facpub/2607

Goldman, E. (2022). The Constitutionality of Mandating Editorial Transparency. *Hastings Law JournalHa*. Vol. 75/5, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=3985&context=hastings_law_journal.Judge, Elizabeth F. and Pal, Michael. (2021). Voter Privacy and Big-Data Elections. *Osgoode Hall Law Journal.* 58(1). 1-55. https://digitalcommons.osgoode.yorku.ca/ohlj/vol58/iss1/1

Jakarta Post. (2021). Concerns raised at slow pace of data breach probe. https://www.thejakartapost.com/paper/2021/05/27/concerns-raised-at-slow-pace-of-data-breach-probe.html

Kanakia, Harshil, Shenoy, Giridhar & Shah, Jimit. (2019). Cambridge analytica a case study. Indian *Journal of Science and Technology*. Vol 12(29), DOI: 10.17485/ijst/2019/v12i29/146977, A

Kaspersky. (2023). Kaspersky experts report more than two critical cyber incidents per day in 2023. https://www.kaspersky.com/about/press-releases/kaspersky-experts-report-more-than-two-critical-cyber-incidents-per-day-in-2023

Kominfo. (2022). RUU PDP Jadi Dasar Pelindungan dan Keamanan Data Pribadi Warga. https://www.kominfo.go.id/content/detail/34654/ruu-pdp-jadi-dasar-pelindungan-dan-keamanan-data-pribadi-warga/0/berita_satker

Kompas. (2021). Kebocoran Data, Aplikasi PeduliLindungi Perlu Diaudit dan Perbaikan. https://www.kompas.com/tren/read/2021/09/05/163000865/kebocoran-data-aplikasi-pedulilindungi-perlu-diaudit-dan-perbaikan?page=all

Kompas. (2023). *Penjelasan KPU Soal Dugaan Kebocoran Data Pemilih Ditunggu Publik*. https://www.kompas.id/baca/polhuk/2023/12/03/penjelasan-kpu-soal-dugaan-kebocoran-data-pemilih-ditunggu-publik

Kozinets, R. V. (2015). Netnography. The International Encyclopedia of Digital Communication and Society. 1–8. https://doi.org/10.1002/9781118767771

KPU. (2023). *Siaran Pers terkait Dugaan Kebocoran Data KPU*. https://www.kpu.go.id/berita/baca/12118/siaran-pers-terkait-informasi-dugaan-kebocoran-data-milik-kpu

Krippendorff, K. (2023). *Content Analysis: An Introduction to Its Methodology*. Sage: Thousand Oaks

Kwak, Jin-ah & Cho, Sung. (2018). Analyzing Public Opinion with Social Media Data during Election Periods: A Selective Literature Review. *Asian Journal for Public Opinion Research*. 5. 285-301. 10.15206/ajpor.2018.5.4.285

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*. 113(2), 501–549. https://doi.org/10.2307/1342331

Manheim, Karl M. and Kaplan, Lyric. (2019). Artificial Intelligence: Risks to Privacy and Democracy (October 25, 2018). *21 Yale Journal of Law and Technology 106*. https://ssrn.com/abstract=3273016

Moleong, Lexy J. (2012). *Metode Penelitian Kualitatif*. Bandung: PT Remaja Rosdakarya.

Morozov, Evgeny. (2013). *To save everything, click here: the folly of technological solutionism.* New York: Public Affairs

National Cyber Security Centre. (2016) *Common Cyber Attacks: Reducing the Impact.* London: GCHQ

Nye, Joseph S. (2021). Soft power: the evolution of a concept. *Journal of Political Power*. 14(1). 196-208. DOI: 10.1080/2158379X.2021.1879572

Perludem. (2023). *Perludem Sayangkan Kebocoran DPT di KPU*. https://perludem.org/2023/12/02/perludem-sayangkan-kebocoran-dpt-di-kpu/

Reuters. (2024). Cyber attack compromised Indonesia data centre, ransom sought. https://www.reuters.com/technology/cybersecurity/cyber-attack-compromised-indonesia-data-centre-ransom-sought-reports-antara-2024-06-24/

Rizal, Muhamad & Yani,Yanyan. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies*. 4(1). 61-78. https://media.neliti.com/media/publications/70606-EN-cybersecurity-policy-and-its-implementat.pdf

Sakti, Rangga Eka & Nainggolan, Bestian. (2023). Understanding the Role of Social Media Toward Satisfaction of Government in Indonesia. *JURNAL KOMUNIKASI INDONESIA*. 12(1). DOI: 10.7454/jkmi.v12i1.1185

Schia, Niels Nagelhus & Gjesvik, Lars. (2020). Hacking democracy: managing influence campaigns and disinformation in the digital age. *Journal of Cyber Policy.* 5(3). 413-428. DOI: 10.1080/23738871.2020.1820060

Schneier, Bruce. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company: New York

Sugiyono. (2011). *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. Bandung: Alfabeta.

Suhaimin, Mohd Suhairi Md, et al. (2023). Social media sentiment analysis and opinion mining in public security: Taxonomy, trend analysis, issues and future directions. *Journal of King Saud University - Computer and Information Sciences*. 35(9). https://doi.org/10.1016/j.jksuci.2023.101776.

Stedmon, Nicholas. (2020). The Impact of Cyber Security Threats on the 2020 US Elections. 10.48550/arXiv.2012.08968.

Tempo. (2022). Cybersecurity Expert Confirms Validity of 105 Mln Leaked Indonesians Data. https://en.tempo.co/read/1631831/cybersecurity-expert-confirms-validity-of-105-mln-leaked-indonesians-data

Zhang, Xichen & Yadollahi, Mohammad Mehdi & Dadkhah, Sajjad & Isah, Haruna & Đức Phong, Lê & Ghorbani, Ali. (2022). Data breach: analysis, countermeasures and challenges. *International Journal of Information and Computer Security*. 19. 402. 10.1504/IJICS.2022.127169.

How to Cite This Article:

Pradnyana, I Putu Hadi., Utama, Rhesa Anggara., & Sasmita, Ni Wayan Ditha. (2024). SECURING DEMOCRACY IN CYBERSPACE: VOTER DATA LEAKS IN INDONESIA'S 2024 ELECTION. JURNAL TRIAS POLITIKA, *8*(2), 292 - 305. doi:https://doi.org/10.33373/jtp.v8i2.6541