# Cybersecurity Threats: The Impact of Cybercrime on Citizen Data Privacy and the Integrity of Election Processes in the Context of Modern Democracies

**Launa[1], Bambang Mudjiyanto[2], Fit Yanuar[3], Hayu Lusianawati[4]**

[1,3,4]Sahid University, Jl. Prof. Dr. Soepomo No. 84, Tebet Dalam, South Jakarta, 12870, Indonesia
[2]National Research and Innovation Agency, Jl. Gatot Subroto, West Kuningan, South Jakarta, 12710, Indonesia
*Email :* launa@usahid.ac.id

**Article Info**

***Article history:***

Received August 01, 2025
Revised October 10, 2025
Accepted October 23, 2025

***Keywords:***

*Kejahatan Dunia Maya, Perlindungan Data, Implikasi Politik Dan Ekonomi, Integritas Pemilu*

## ABSTRAK

Tindakan kriminal pencurian data pribadi dapat merusak kepercayaan publik terhadap proses dan hasil pemilu. Teknologi pemilu elektronik sesungguhnya memudahkan masyarakat siber dalam melakukan aktivitas politik virtual di era demokrasi digital saat ini. Studi ini berupaya menjelaskan kejahatan siber, lemahnya perlindungan data warga negara, dan implikasinya terhadap integritas hasil pemilu. Studi kualitatif dengan pendekatan studi kasus berbasis tinjauan pustaka ini menemukan fakta bahwa perkembangan teknologi digital akan selalu kompatibel dengan peningkatan kejahatan pencurian data dan implikasinya terhadap integritas hasil pemilu akibat modus kebocoran data yang kerap dimanfaatkan para peretas untuk mendelegitimasi kendali negara atas hasil pemilu yang bermartabat.

**Article Info**

***Article history:***

Received August 01, 2025
Revised October 10, 2025
Accepted October 23, 2025

***Keywords:***

*Cybercrime, Data Protection, Political And Economic Implication, Election Integrity*

## *ABSTRACT*

*Criminal acts of personal data theft can undermine public trust in election processes and results. Electronic election technology actually makes it easier for cyber citizens to engage in virtual political activities in the current era of digital democracy. This study seeks to explain cybercrime, the weak protection of citizen data, and its implications for the integrity of election results. This qualitative study, using a case study approach based on a literature review, found that the development of digital technology will always be compatible with an increase in data theft crimes and its implications for the integrity of election results due to data leaks that are often exploited by hackers to delegitimize state control over dignified election results.*

***Corresponding Author:***

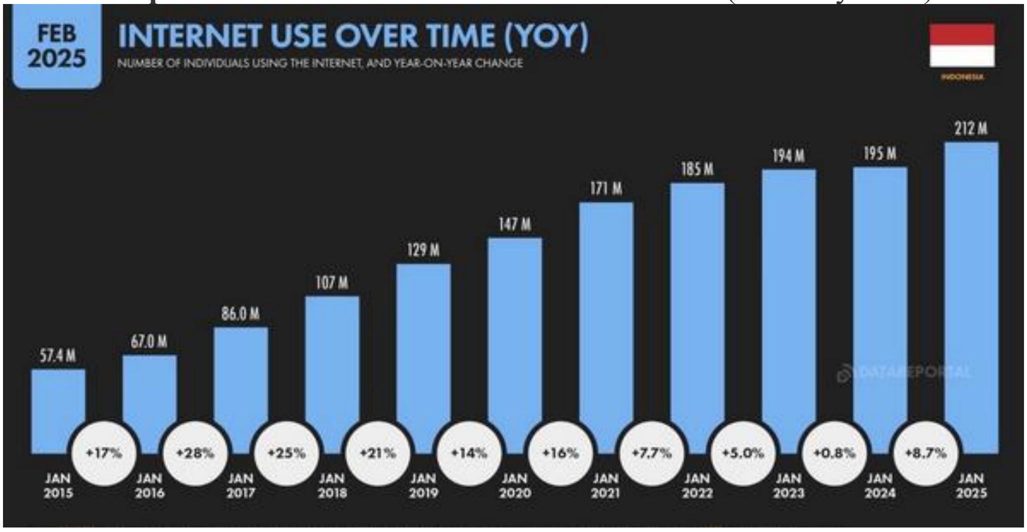
Launa
Universitas Sahid Jakarta
*Email*: launa@usahid.ac.id

## INTRODUCTION

The recurring phenomenon of personal data leaks and cybercrime within public institutions underscores how information security challenges are an integral part of the problems of digital democracy (e-democracy). According to digital democracy theory (Wilhelm, 2000; Barth & Schlegelmilch, 2014), information technology opens up broader and more inclusive political participation, but also carries significant risks, such as data manipulation, disinformation, and cyberattacks that can undermine the legitimacy of the democratic process. This situation aligns with Giddens' (1990) prediction, which views modernity as a force operating in uncertainty and high risk, including in the realm of digital politics. In the Indonesian context, the implementation of the Electronic Information and Transactions Law (UU ITE) represents a form of state control to maintain a balanced digital democracy without compromising citizens' rights and freedoms. However, the challenge of cybercrime continues to grow, creating threats referred to as 'crimes of democracy.' Recent studies (Barth & Schlegelmilch, 2014; Whyte, 2020; V-Dem, 2024) emphasize that in addition to technical risks such as hacking and data leaks, there are also political risks such as polarization and manipulation of public opinion that threaten the integrity of democracy.

On the one hand, e-democracy offers great hope for citizens to actively, effectively, intensively, and massively engage in the democratic process (which appears to be a benign process and offers a variety of effective solutions). However, on the other hand, this facade of e-democracy also harbors (if not conceals) various political risks and democratic uncertainties, such as voter data manipulation, irregularities in political procedures, or the decay of democratic values and practices (Bialik, 2012).

**Graph 1**. Number of Internet Users in Indonesia (February 2025)



Source: Fatoni, 2025

Borrowing the thesis of Daniel Skog et al. (2018), that the world society has now entered an era of full disruption, an era where fundamental transformation has changed the system, order, landscape, and human consciousness to enter into a new value system, including the value system of political life and democracy. According to Skog et al. (2018, p 432), the era of disruption has practically succeeded in organizing political and democratic habitus that is completely dependent on technology. To keep up with the changing social order, digital technology must also move in harmony with the demands of the digital society

in order to give birth to various new ideas and innovations to support the order of cyber society in a digital-based virtual interaction space (cyberspace).

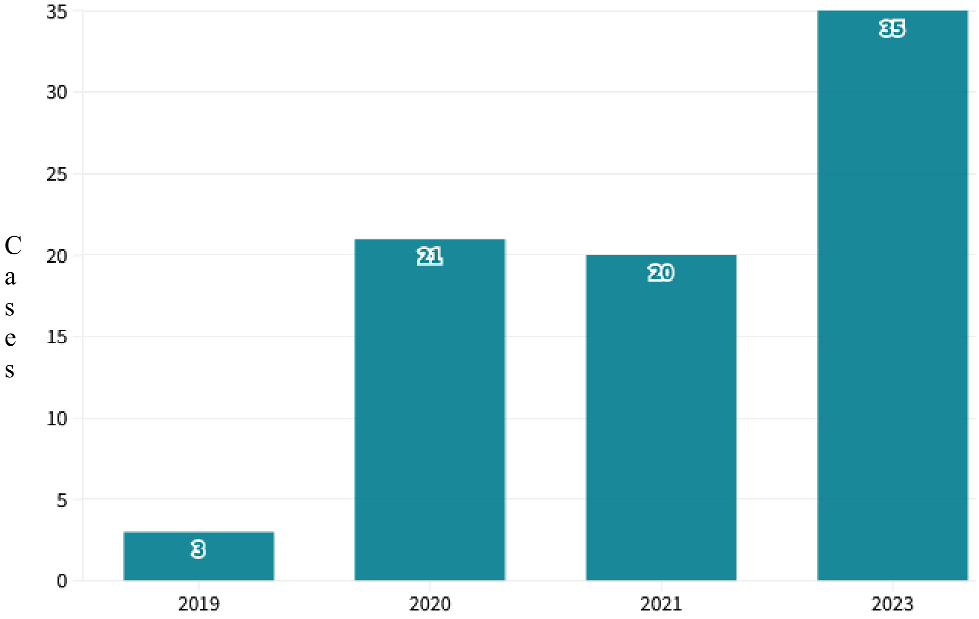
The development of the internet and the massive migration of internet users in the last two decades have triggered an era of disruption. The era of disruption is another term for the era of the industrial revolution based on digital technology. This era is defined as an era of fundamental changes in the field of technology with the aim of processing all human needs easily and practically (such as processing goods that were originally done by humans with high costs and long times, replaced by machines and computers with maximum output and low costs. Meanwhile, the industrial revolution 4.0 is an era where all human activities migrate fully into the digital society order due to technological disruption. The industrial revolution is the trigger for the era of disruption that fundamentally changes the order of people's lives; the impact of revolutionary innovation in the field of digital technology (Skog, et al., 2018, p. 435).

The era of technological disruption in the cyber society has not only given birth to revolutionary ideas and innovations, but also brought about negative side effects such as the proliferation of cybercrime. Cybercrime is a criminal act or a type of illegal activity that utilizes technological intelligence to harm the interests or seize the rights of others, such as theft, hacking, fraud, spreading viruses, and other types of digital crimes. Steven Furnell (2001) divides cybercrime into the following areas: (1) crimes that damage devices (devices of software), such as hacking or spreading viruses; (2) material crimes, such as payment fraud or consumer fraud; and (3) victimizing someone (the person of the victim), such as sending threats or carrying out online stalking. Meanwhile, the impacts caused by cybercrime from a victimological perspective can be in the form of material losses (financial loss), psychological loss (psychological loss), physical loss (physical loss), and social loss (social loss). The worst psychological effects on hacking victims can range from mild to severe stress, and in some cases can even lead to suicide (Leukfeldt et al., 2019).

In Indonesia, the issue of personal data protection (PDP) remains a serious problem. For example, cybercrime is on the rise, as seen in the 2020 data theft of 91 million Tokopedia users' data, which was hacked by hackers and sold on the black market. Another shocking case was the 2022 data breach by a hacker using the pseudonym Bjorka. He claimed to have sold no less than 1.3 billion personal data items hacked through SIM card registrations. Bjorka offered the data on the Breached Forums website. To attract potential buyers, Bjorka even offered 2 million pieces of data as free samples to prospective buyers. On Breached Forums, Bjorka also distributed documents (important letters) claiming to be personal data belonging to the President of the Republic of Indonesia (Hardiansyah, 2022).

Another example is the case of various data leaks experienced by government and private public service institutions, such as the hacking of data belonging to BPJS Ketenagakerjaan users, BPJS Kesehatan, users of the Ministry of Health's e-HAC application, Bank Syariah Indonesia customer data, MyIndiHome user data, BRI Life customer data, data of Indonesian citizens holding passports, and much earlier, in 2014, there was also the theft of 2.3 population data on the Permanent Voter List (DPT) for the Election stored in the KPU database (Tamtomo & Galih, 2022; Widi, 2023). Various cases of leaks of personal data belonging to citizens have certainly caused public unrest and public distrust in the government. Personal data protection (PDP) and a series of other regulations that have been prepared by the government to protect factual personal data have not been able to anticipate the poor data center ecosystem in Indonesia that is effective in protecting citizens' personal data from potential fraud, defamation, online intimidation, and the public's right to control personal data.

**Graph 2**. Data Leak Cases in Indonesia
(January Period 2019 to June 2023)



Source: Kominfo RI

However, in various official statements or clarifications, both from the government and public service institutions that have been hacked, ironically, the public is always the 'blameless' party, even though legally the public's position is the 'victim.' The public is considered "not to understand the importance of protecting personal data in the current era of increasingly massive growth of mobile phones and the internet." In fact, Commission I of the House of Representatives has repeatedly reminded the government to anticipate data leaks that continue to recur and harm the public. The House of Representatives has also asked the government to focus on protecting citizens' personal data and immediately develop a national cybersecurity roadmap. The opaque national cybersecurity roadmap will clearly make it difficult to optimize the protection of citizens' personal data. The House of Representatives also requested that government institutions no longer shift responsibility when data leaks occur, especially in strategic public service institutions (www.dpr.go.id/).

In the context of political integrity and democratic legitimacy, repeated leaks of election voter list (DPT) data will undoubtedly erode the government's political legitimacy and undermine the integrity of the General Elections Commission (KPU) as the election organizing body. Most recently, at the start of the 2024 election campaign, 252 million DPT data items were leaked from the KPU website. The leaked DPT items were allegedly traded on an online forum, uploaded by the anonymous user Jimbo. Similar cases also occurred in 2014 (theft of 2.3 million KPU DPT items) and September 2020 (theft of 105 million KPU DPT items) (Siregar, 2023).

The leak of voter data from the final voter list (DPT) is clearly no trivial matter, especially when it occurs in the lead-up to the 2024 elections, a highly sensitive and heated period. If any hacker could easily breach the General Elections Commission (KPU) website, this would undoubtedly pose a serious threat to the legitimacy of the election results, which will be held simultaneously in mid-February 2024. Furthermore, this is not the first time that alleged hacking has targeted voter data on the KPU website. Prospective voters are understandably concerned that such a method could be exploited by certain parties to alter the vote count recapitulation results. If that were to happen, the democratic process would undoubtedly be undermined. It is even possible that cases of personal data leaks could trigger a wave of protests and national political unrest.

It is no exaggeration to say that the ongoing data leak phenomenon in Indonesia at least confirms the fact that PDP has not yet fully become the focus of attention and the main priority of the government to be immediately followed up through the development of a national cybersecurity system to anticipate hacker attacks, both local, domestic, and global hackers. As recommended by the European Data Protection Supervisory Agency, every country is obliged to strengthen the digital ethics system, control the expansion of artificial intelligence products, and strengthen the personal data protection system to anticipate the negative impacts of the digital technology environment, such as the protection of computer networks, software applications, critical systems, and data protection from potential threats of digital crime (Annual Report: European Data Protection Supervisor, 2019).

The fact that voter personal data leaks due to digital crime have been mapped through academic research by Pippa Norris (2020) and Stephen Dawson (2023). According to these two analysts, cybercrime is not only related to economic or financial crimes, but in the future, it is not impossible that it has the potential to become a trend of political crime that can harm the election process and undermine public trust in election results. Referring to the above arguments, this study seeks to examine the phenomenon of cybercrime and its relationship to the theft of citizen data that often operates in the public sector, especially the theft of politically motivated data (voter list data) that has the potential to damage the integrity of election results. This study will begin with a conceptual description of cybercrime, followed by the economic and political implications of cybercrime and an analysis of various cases of hacking of citizens' personal data in the lead-up to elections and their relationship to the integrity of election results.

## Conceptual Definition and Literature Review

By definition, the Oxford dictionary defines cybercrime as a crime committed by an individual or group via the internet, such as stealing someone's personal data or infecting a computer with a virus (crimes committed using the internet, such as stealing someone's personal data or infecting a computer with a virus) (www.oxfordlearnersdictionaries.com). The Britannica dictionary defines cybercrime as the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in pornography and intellectual property, stealing identities, or violating privacy (www.britannica.com). Meanwhile, the Merriam-Webster dictionary defines cybercrime as criminal activity, such as fraud, theft, or distribution of child pornography committed using computer devices to illegally access, transmit, or manipulate data (www.merriam-webster.com).

**Table 1**. Conceptual Differences Between Cyber Security and Cybercrime

| Item | Cyber Security | Cybercrime |
|---|---|---|
| Type of Crime | *Computer crime*: attacks on computer programs or networks, both software and hardware, such as ordinary viruses (soft viruses), worm viruses that spread automatically (worm viruses), dangerous viruses that attack through the file system (ransomware), virus attacks through the use of code (SQL injection), and distributed denial of service attacks. | *Human crimes*: attacks on individual personal data, such as romance fraud, cyberbullying, hate speech, sexting, child pornography, human trafficking, trolling, body shaming, and so on. |
| Victim | Government organs, corporate organs, and other official public organs. | Communities, families, and individuals. |
| Academic programs | Computer science, computer engineering, information technology, cybersecurity studies, or others. | Law, criminology, sociology, psychology, communications, or others. |
| Focus of study | Oriented towards applied science, network coding and strategies to create network security. | Oriented towards basic science about how or why crimes are committed by humans (hackers). |

Source: Graham, 2017

Next, to avoid simplification, this study attempts to establish the conceptual differences between cybersecurity and cybercrime. According to Graham (2017), cybersecurity and cybercrime have different definitions, orientations, and targets (see table 1). Cybersecurity is a set of guidelines, rules, or official government actions aimed at preventing and protecting computer networks/digital systems used by government-owned public bodies, state institutions, state-owned enterprises, and private companies that serve or store citizen data. The main target or goal is to anticipate hackers from exploiting vulnerabilities in vital state-owned network systems or citizens' personal data. Meanwhile, cybercrime focuses on protecting personal data (of small communities, families, and individuals) as they live their online lives or engage in activities in cyberspace.

Personal data theft can be defined as the theft of personal information without the identity owner's permission. Identity theft or fraud is a term commonly used to refer to all types of cybercrime in which a person or group of people illegally hack into another person's personal data by stealing or manipulating data to gain a certain profit (www.justice.gov). Identity theft can take the form of impersonating names and addresses, ID numbers, credit cards, bank accounts, social security, health insurance accounts, or other personal identification numbers (www.consumer.ftc.gov); or the illegal use of another person's personal information to gain material gain (money or credit) (www.merriam-webster.com).

The literature review used in this study refers to the results of previous studies, such as those by Mahpudin (2019), Norris (2020), Dawson (2022), Lesmana (2022), Sandrawati (2022), Kusnaldi et al. (2022), Setiawan and Najicha (2022), Silalahi and Dameria (2023), and Saputra (2023). The literature mapping can be seen in the following main points.

**Table 2**. Literature Review

| Author/Title of Study | Methodology | Research Findings |
|---|---|---|
| Mahpudin (2019)<br>*Teknologi Pemilu, Trust, dan Post Truth Politics: Polemik Pemanfaatan Situng Pada Pilpres 2019* | Political analysis; qualitative-exploratory approach; descriptive-interpretive analysis method; focus of analysis: implications of using Situng as election technology in the post-truth era | The use of Situng technology in post-truth elections has sparked a heated debate about efficiency and public trust, a consequence of the digitization of elections. The use of election technology (Situng) in Indonesia has become increasingly complex due to the public trust involved in election results, which are vulnerable to public criticism and contamination by the spread of misinformation on social media, a logical consequence of the post-truth era. |
| Pippa Norris (2020)<br>*Electoral Integrity in the 2020 U.S. Elections* | Political analysis; comparative survey approach; descriptive analysis method (FGD results, field observations, and interviews); focus of analysis: changes in the 2014 and 2020 US elections as material for reviewing the integrity of US elections through a comparison of 300 national elections in 166 countries. | The U.S. government must prevent further deterioration of public confidence in election results. Every democratic regime is obligated to address various structural weaknesses through a comprehensive and fundamental electoral reform program to restore public trust in the electoral process, such as expanding voter registration locations and providing safe and sterile polling stations (TPS); increasing the independence and professional standards of election management; strengthening fair and impartial dispute resolution mechanisms; prohibiting elite collusion in campaigns; improving the management of political party financial reports; limiting political advertising monopolies; and strengthening ethical regulations for political campaigns. |
| Stephen Dawson (2022)<br>*Electoral Fraud and the Paradox of Political Competition* | Political analysis; qualitative approach; descriptive analysis method (based on poll data); focus of analysis: the relationship between the level of election competition and election fraud. | In established democracies, intense electoral competition often creates political dilemmas and problems. This is because many political parties and candidates receive incentives from external economic and political forces to manipulate the electoral process in such a way that they profit from the victory of their party or candidate. Political incentives take the form of allotting parliamentary seats or certain strategic positions, while economic incentives involve funding the campaign process. |
| Lesmana, dkk. (2022)<br>*Urgensi UU Perlindungan Data Pribadi dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia* | Legal analysis; juridical-normative approach (statute approach); focus of analysis: the urgency of the PDP Law in guaranteeing the personal data of Indonesian citizens. | In Indonesia, the implementation and enforcement of Personal Data Protection (PDP) laws remain problematic, despite the official enactment of various regulations related to PDP. Even before the PDP Law was enacted, numerous cases of personal data leaks continued to occur. Regulations, institutions, and officials mandated by PDP have not yet fully implemented their mandate to ensure the security of personal data and the protection of citizen privacy. |
| Sandrawati (2022)<br>*Antisipasi Cybercrime dan Kesenjangan Digital Dalam Penerapan TIK di KPU* | Election technology analysis; qualitative approach (literature study); analysis focus: anticipating cybercrime, improving KPU ICT human resources, | The digital gap and human resource competency significantly contribute to the success of the KPU's ICT implementation. The obstacles faced by the KPU are increasing daily: cybercrime, unequal internet access, and inadequate human resource competency. The KPU must address cybercrime and the digital gap through strengthened security, cybersecurity |

| | | |
|---|---|---|
| | and addressing the digital divide in society (voters). | guidelines and audits, improved human resource competency, synergistic collaboration with stakeholders, and regular evaluations. |
| Kusnaldi, dkk. (2022)<br>*Perlindungan Data Pribadi Dalam Penyelenggaraan Pemilu: Tantangan dan Tawaran* | Legal analysis; juridical-normative approach; focus of analysis: challenges of digital era elections. | In the era of digital elections, there are three challenges faced by the KPU regarding the Personal Data Protection Law (PDP): (1) scattered data at every stage of the election process, (2) regulations that are not yet optimal, and (3) PDP literacy is still not fully understood by voters or election officials (especially regional KPU/Bawaslu). |
| Setiawan dan Najicha (2022)<br>*Perlindungan Data Pribadi Warga Negara Indonesia Terkait Kebocoran Data* | Legal analysis; juridical-normative approach; focus of analysis: national legal umbrella to protect citizens' personal data. | Digital developments and openness to online transactions often harm citizens' interests and rights regarding data breaches. The government's lack of focus on accelerating the ratification of the Personal Data Protection Law (PDP) has triggered various on going data breaches in Indonesia. Accelerating the ratification of the PDP Law will benefit data owners, stakeholders, and other countries' recognition of the legality of Indonesian citizens' data. |
| Silalahi & Dameria (2023)<br>*Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cybercrime Sebagai Kejahatan Transnasional* | Legal analysis; juridical-normative approach (statute approach); focus of analysis: personal data leak cases as transnational cybercrimes. | The era of technological globalization has pushed the internet into a new medium for data hacking crimes, operations that transcend national borders. Transnational data theft by hackers (transnational cybercrime) has prompted many countries, including Indonesia, to take various preventative measures to address transnational (global-scale) cybercrime. |
| Saputra (2023)<br>*The Right to Privacy: Tinjauan Terhadap Penyalahgunaan Data Pribadi Dalam Perspektif HAM* | Legal analysis; juridical-normative approach; focus of analysis: violation of privacy (citizens' personal data) as an integral part of human rights violations. | The Indonesian government is considered to be insufficiently serious about implementing the Personal Data Protection Bill (PDP) to protect the privacy and security of citizens' data. The use of citizens' data for registration in various unilaterally regulated applications for external purposes has triggered various forms of personal data abuse by cyber hackers through data theft. Data hacking is a human rights crime that violates citizens' right to privacy. |

Source: Data processed by researchers

## RESEARCH METHOD

This type of research is qualitative research with a case study approach. Qualitative research is a scientific method for capturing natural phenomena that: (1) is based on a positivist philosophical framework (interpretive analysis); (2) the researcher is a key instrument in the research process; (3) data collection techniques are characterized by triangulation or are combinative (observation, interviews, and documentation); (4) data analysis is inductive; (5) data sources are qualitative (relying on literature reviews/document studies, in addition to observation); and (6) research results are elaborated descriptively-taxonomically. Meanwhile, the case study approach is generally used to conduct an in-depth study of a natural event by collecting various sources of information to be processed and analyzed; and the results of the data analysis and processing are then interpreted to understand the phenomenon, draw meaning, and find hypotheses (Priya, 2021).

This study relies on data sources from observations and literature studies, such as books, journals, documents, and online articles and news. The discussion framework is structured in three parts. The first part examines various cases of personal data leaks that have occurred in Indonesia. The second part analyzes the economic and political implications arising from these various data leaks. The third part links data leaks to election integrity (both process and results) as political impacts that shape negative public perceptions, particularly voter data leaks in the lead-up to the democratic election or presidential election. The final section concludes with a conclusion.

## DISCUSSION

Long before the rise of data theft cases in Indonesia, and indeed in many countries around the world, the concept of privacy was developed by Warren and Brandhuis (1890), William Prosser (1960), Alan Westin (1968), and Arthur Miller (1971). These five analysts agreed that individual privacy is crucial to protect because it is closely related to 'property rights,' which are the domain of individuals (individual property) and a vital part of democracy. Personal data protection practices were first legally implemented in Germany and Sweden in the early 1970s, where privacy protection began to be regulated by law. However, each country has its own terminology (nomenclature) for personal information and personal data. Because both have similar or relatively identical meanings, it is not surprising that the two terms are often used interchangeably. In the United States, Canada, and Australia, for example, the term 'personal information' is preferred. Meanwhile, in European Union countries and Indonesia, the term 'personal data' is more appropriate.

Personal data protection has been a growing legal issue since the early 1970s, when computers began to be used as data storage devices, particularly for population data. During that time, numerous cases of personal data misuse were uncovered, both by the government and the private sector. In Indonesia, rapid technological advancements and the proliferation of applications requiring the registration of a National Identification Number (NIK) have fueled various forms of cybercrime through computers, mobile devices, and the internet.

**Table 3**. 50 Data Breaches from 2004 to 2021

| Rank | Business Entity | Affected Sector | Record Compromised | Years |
|---|---|---|---|---|
| 1 | America Online (AOL) | Web | 92M | 2004 |
| 2 | TJ-Maxx/The TJ Companies Inc. | Retail | 94M | 2007 |
| 3 | Heartland | Finance | 130M | 2009 |
| 4 | Sony Playstasion Network | Gaming | 77M | 2011 |
| 5 | Rambler.ru | Web | 98M | 2012 |
| 6 | Yahoo | Web | 3.0B | 2013 |
| 7 | Court Ventures | Finance | 200M | 2013 |
| 8 | Massive American Business Hack | Finance | 160M | 2013 |

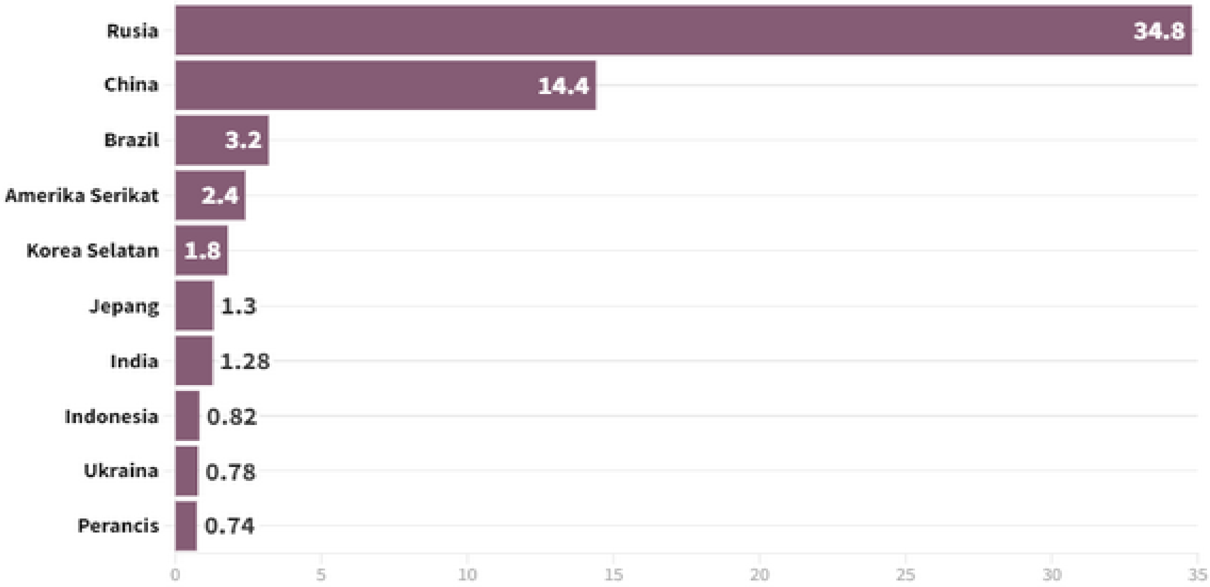
| | | | | |
|---|---|---|---|---|
| 9 | Yahoo | Web | 500M | 2014 |
| 10 | Ebay | Web | 145M | 2014 |
| 11 | Deep Root Analytics | Web | 198M | 2015 |
| 12 | Anthem | Health | 80M | 2015 |
| 13 | Friend Finder Network | Web | 412M | 2016 |
| 14 | V-Kontake (VK) Companies | Web | 171M | 2016 |
| 15 | Linkedin | Web | 117M | 2016 |
| 16 | MySpace | Web | 360M | 2016 |
| 17 | Dailymotion | Web | 85M | 2016 |
| 18 | River City Media | Web | 1.4B | 2017 |
| 19 | Spambot | Web | 771M | 2017 |
| 20 | Equifax | Finance | 163M | 2017 |
| 21 | Aadhaar | Goverment | 1.1B | 2018 |
| 22 | Marriott International | Retail | 500M | 2018 |
| 23 | Exactis | Data | 340M | 2018 |
| 24 | Twitter | Tech | 330M | 2018 |
| 25 | Nametests | App | 120M | 2018 |
| 26 | Apollo | Tech | 200M | 2018 |
| 27 | MyFitnessPal | App | 150M | 2018 |
| 28 | Firebase | App | 100M | 2018 |
| 29 | Quora | Web | 100M | 2018 |
| 30 | MyHeritage | Web | 92M | 2018 |
| 31 | First American Corporation | Finance | 885M | 2019 |
| 32 | Facebook | Web | 419M | 2019 |
| 33 | OxyData | Tech | 380M | 2019 |
| 34 | Airtel | Telecoms | 320M | 2019 |
| 35 | Indian Citizen | Web | 275M | 2019 |
| 36 | Chinese Resume Leak | Web | 202M | 2019 |
| 37 | Zynga | Gaming | 173M | 2019 |
| 38 | Dubsmash | Web | 162M | 2019 |
| 39 | Canva | Web | 139M | 2019 |
| 40 | Microsoft | Web | 250M | 2019 |
| 41 | ElasticSearch | Tech | 108M | 2019 |
| 42 | Capital One | Finance | 106M | 2019 |
| 43 | Wattpad | Web | 270M | 2020 |
| 44 | Tetrad | Finance | 120M | 2020 |
| 45 | Pakistani Mobile Operators | Telecoms | 115M | 2020 |
| 46 | Linkedin | Web | 700M | 2021 |
| 47 | Facebook | Tech | 533M | 2021 |
| 48 | Syniverse | Telcoms | 500M | 2021 |
| 49 | Experian Brazil | Finance | 220M | 2021 |
| 50 | Thailand Visistors | Goverment | 106M | 2021 |

Source: Nwosu, 2022

A data breach is an incident in which sensitive or confidential information is copied, transmitted, or stolen by an unauthorized individual or entity. This typically occurs through malware attacks, payment card fraud, insider leaks, or accidental disclosure. The data targeted for hacking typically includes personally identifiable information (PII) belonging to employees, company data, government agency data, or intellectual property. Perpetrators can be lone hackers, organized cybercrime groups, or even national governments. The stolen information can then be used for other crimes such as identity theft, credit card fraud, or ransom demands (Nwosu, 2022).

Citing a report by Shurfshark (a Netherlands-based cybersecurity company), Indonesia is at high risk for personal data breaches. According to Shurfshark, Indonesia ranks among the 10 countries in the world with the highest rate of personal data breaches. Data breaches in the second quarter of 2022 even increased by 143 percent from the first quarter of 2022 (quarter to quarter). Since 2004, the total number of data breaches in Indonesia has reached 120.9 million. Globally, the number of accounts experiencing data breaches in the second quarter of 2022 increased by two percent (quarter to quarter) to 459 accounts per minute, compared to 450 accounts per minute in the first quarter of 2022 (see graph 3).

**Graph 3**. Countries with the Highest Data Breach Rates (Q2/2022)



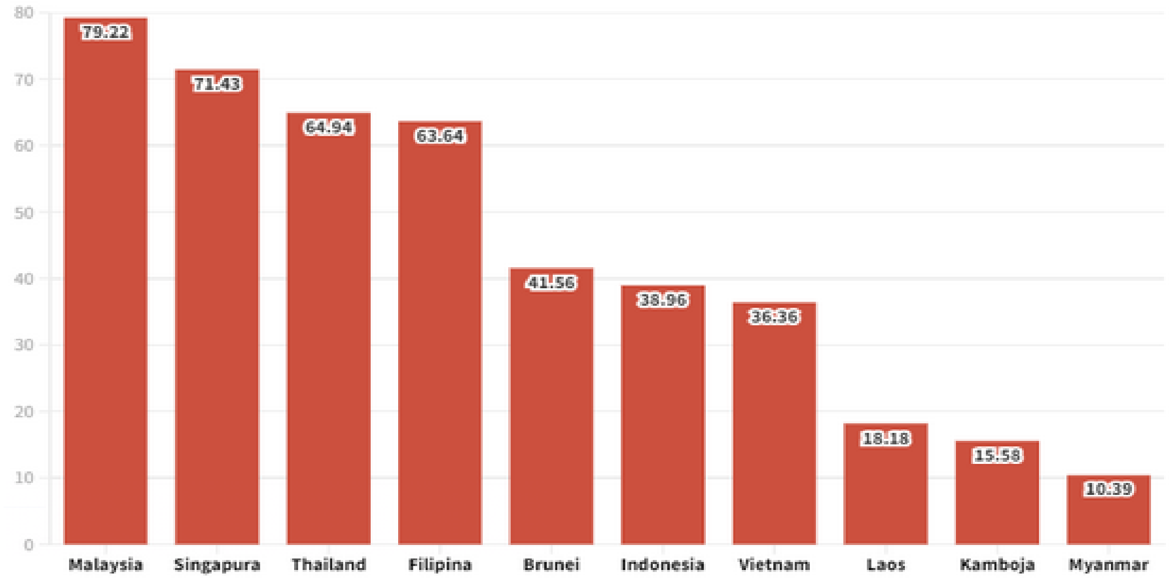
Source: Naurah, 2022

Citing the National Cyber Security Index (NCSI) report, Indonesia's cybersecurity score at the Southeast Asian level ranks sixth in Southeast Asia (out of 11 ASEAN countries) and 83rd out of 160 countries worldwide. Indonesia's cybersecurity score is only 38.96 percent out of 100 percent, as of August 2022. Meanwhile, Malaysia holds the top spot as the country with the best cybersecurity index in Southeast Asia, achieving a score of 79.22, ranking 19th globally (see graph 4).

In Indonesia, according to data from the Indonesian Consumers Foundation (YLKI), the online shopping (e-commerce) industry experienced the highest number of data breach complaints in June 2020, with 54 cases, followed by the telecommunications industry with 31 cases, the electricity industry with 31 cases, and the online lending industry with 28 cases.

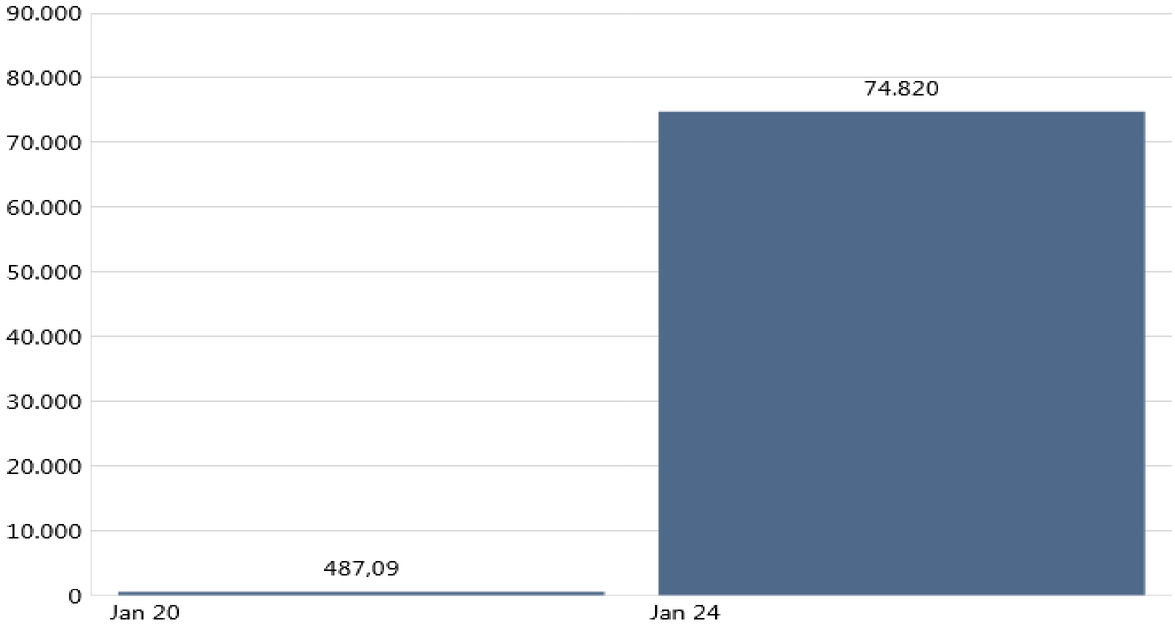
From January to June 2020, the total number of data breaches across various sectors reached 277 (see graph 5).

**Graph 4**. Data Leakage Rates in Five Countries



Source: Naurah, 2022

**Graph 5**. Number of BI Data Capacity Leaks
(Per 24 Januari 2022)

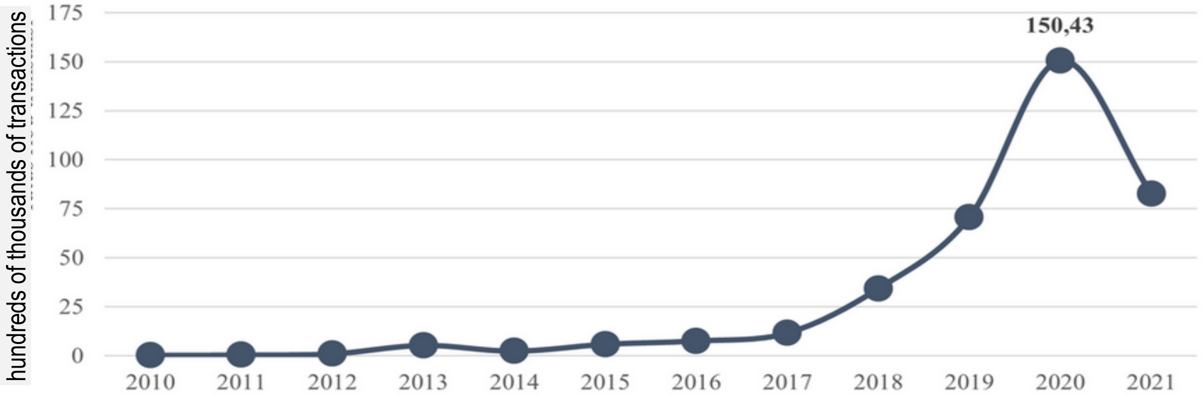


Source: Kusnandar, 2022

Data hacking also occurred in the banking sector. The victim was Bank Indonesia (BI), while the perpetrators were Russian hackers from the Conti Ransomware group.  The alleged leaked BI data went viral on social media after cybersecurity monitoring agency DarkTracer posted its findings on Twitter. DarkTracer revealed that the Conti Ransomware hacker group had hacked 487 MB of data from 16 Personal Computers (PCs) on January 21, 2022. The hack allegedly attacked PCs at the BI branch office in Bengkulu, locking and stealing BI's data system. On January 24, 2020, DarkTracer again posted that the theft of BI data by the

Russian hacker group had increased to 52,767 documents with a data capacity of 74 Gigabytes (GB). The data was hacked from 237 PC units within BI's computer network (Kusnandar, 2022).

**Graph 6**. Total Electronic Transaction Volume 2010-2021



Source: Bank Indonesia, 2022

Examined from electronic transaction data across all Indonesian banks, BI data shows that the number of electronic transactions continues to increase, from 100,635 transactions (in 2012). Eight years later, in 2020, the number of electronic transactions increased 150-fold, reaching 15,043,475 (with a transaction value reaching 504,956 billion).The significant increase in the number of electronic transactions has the potential to become fertile ground for the rise of electronic crime in the banking sector (see graphs 5 and 6).

**Table 4**. Various Data Leak Cases in Indonesia (2019 – 2023)

| Year | Case | Description |
|---|---|---|
| 2019 | Bukalapak | A Pakistani hacker, "Gnosticplayers" (pseudonym), with the username "Startexmislead," claims to have successfully hacked the data of 13 million Bukalapak users and sold it on the dark web. The data includes email addresses, phone numbers, and birth dates. |
| 2020 | *E-Commerce* Tokopedia | A data breach reportedly affected 15 million users of the e-commerce platform Tokopedia. The leak was uncovered by Under the Breach, an Israeli cybersecurity firm. As a result of the data breach, Tokopedia has been sanctioned by the Indonesian Ministry of Communication and Information Technology. |
| 2020 | Tokopedia | A personal data breach by Gnosticplayes has occurred again on the Tokopedia platform. Gnosticplayes claims to have compromised the data of 91 million Tokopedia app users and 7 million sellers in March 2020. The leaked data included email addresses, phone numbers, dates of birth, and other personal information. |
| 2021 | Aplikasi Npjs-kesehatan. go.id | A Raid Forums user named Kotz is reportedly selling a database containing personal information, such as national ID numbers (NIK), national ID cards (KTP), salaries, mobile phone numbers, addresses, and email addresses, purportedly obtained from a hack of the Npjs-kesehatan.go.id website. The data is being offered for 84.3 million rupiah, or around US$6,000, on the dark web. |
| 2021 | Aplikai e-Hac Kemenkes | The Ministry of Health's Electronic Health Alert (e-HAC) app has leaked data of 1.3 million users. VPN software review site vpnMentor published the discovery of the e-HAC database leak, which was first discovered on July 15, 2021. |

| | | |
|---|---|---|
| 2021 | BPJS Kesehatan | In May 2021, a Twitter post revealed a data leak involving BPJS Kesehatan card users. The hacker, who hacked hundreds of millions of BPJS Kesehatan members, was allegedly planning to sell the data on Raid Forums for around Rp 84 million (approximately US$5,000). The stolen data included information such as National Identity Numbers (NIK), mobile phone numbers, email addresses, addresses, and salaries. |
| 2021 | BRI Life | In July 2021, the data of 2 million BRI Life insurance customers was leaked, allegedly for sale online. The leak was first revealed by the Twitter account @UnderTheBreach on July 27, 2021. The account stated that 463,000 pieces of stolen data were sensitive. The hackers allegedly distributed a 30-minute demonstration video as an introductory advertisement for selling the stolen BRI Life customer data. |
| 2021 | Facebook | Meta, the parent company of Facebook, WhatsApp, and Instagram, was fined 265 million euros (Rp 4.3 trillion) by the Irish Data Protection Commission for the alleged data breach of 500 million Facebook users in 2021. The leaked data included phone numbers and email addresses from 2018 to 2019. |
| 2021 | KPAI | Data belonging to the Indonesian Child Protection Commission (KPAI) has allegedly been leaked and traded on the hacker forum Raid Forums. The data is being offered by an account with the initials C77, codenamed “KPAI Leaked Database.” C77 uploaded the information on October 13, 2021, and provided sample data related to the information being offered. |
| 2023 | Paspor WNI | “Bjorka” is suspected of leaking 34.9 million Indonesian passport data for sale for US$10,000 (Rp150 million). Bjorka is offering 1 million free samples to potential buyers. The leaked data includes passport numbers, full names, expiration dates, dates of birth, and gender. The leaked Indonesian passport data is managed by the National Data Center (PDN) of the Indonesian Ministry of Communication and Information. |
| 2023 | Kartu SIM Ponsel | Hacker “Bjorka” has again hacked 1.3 billion Indonesian mobile phone user numbers, allegedly intended for sale on the online forum Breached Forums. Bjorka claims to have obtained the data from SIM card registrations collected by the Ministry of Communication and Information Technology. Ironically, 2 million of the data will be provided free as samples to potential buyers. |
| 2023 | BPJS Ketenagakerjaan | The data of 19.56 million Indonesian BPJS Ketenagakerjaan (Employment Social Security Agency) card users has allegedly been leaked. This was discovered after a post from the Bjorka account on Breach Forums titled “BPJS Ketenagakerjaan Indonesia 19 Million.” In the post, Bjorka also shared 100,000 sample data containing National Identification Number (NIK), full name, email address, telephone number, address, date of birth, gender, occupation, workplace, and more. Bjorka is selling the data for US$5,000, equivalent to Rp752.65 million. |
| 2023 | MyIndiHome | Another alleged data leak occurred in late June 2023, when Bjorka again hacked 35 million MyIndiHome user data and sold it for US$5,000 (equivalent to Rp752.65 million). Bjorka also displayed 10,050 samples of data containing email addresses, mobile phone numbers, ID numbers, National Identification Numbers (NIK), and internet protocol (IP) addresses. Bjorka also stated that he had sold access to Telkom Indonesia’s internal database servers. |

| | | |
|---|---|---|
| 2023 | Bank Syariah Indonesia/BSI | Lockbit (a Russian ransomware group) successfully stole 1.5 terabytes (TB) of personal data from BSI customers. Lockbit gave BSI a deadline of May 15, 2023, to pay a ransom of US$20 million, equivalent to 297 billion Rupiah. However, BSI refused the request. On May 16, 2023, Lockbit then released BSI customer data, including names, addresses, occupations, telephone numbers, account numbers, account balances, transaction history, and other customer information. |

Source: Data processed by researchers

The various cases of citizen data leaks that have occurred in various public service sectors above demonstrate that technological advancements also bring a dark side that is very dangerous for the confidentiality of citizen data and state secrets. Technological advancements have also led to increasingly sophisticated crime patterns, from conventional crimes (such as pickpocketing, mugging, extortion, and thuggery) to cybercrimes (data hacking, carding, and online fraud).

## Economic and Political Implications

Regarding economic implications, International Business Machines (IBM) reported that the total losses from data breaches globally averaged US$3.86 million in 2020. However, several countries experienced higher losses, such as the United States (US$8.64 million) and the Middle East (US$6.52 million). Furthermore, companies in Canada, Germany, Japan, and France whose data was compromised by hackers (including government, private, and private data) suffered significant losses, amounting to around US$4 million. Similarly, the United Kingdom suffered US$3.9 million in losses. However, several countries recorded lower total losses than the global average, such as Italy and South Korea at around US$3 million, and the ASEAN and Scandinavian regions at around US$2 million. Turkey, Latin America, and Brazil only suffered US$1 million in losses.

Another implication is that the unequal access gap to digital technology is also a problem that requires attention. This is because most urban areas have adopted digital technology at an extraordinary rate, while the majority of rural areas still lag behind in digital technology accessibility. This situation has the potential to create an economic and technological gap between urban and rural areas, which in turn could trigger a "cultural conflict" and slow overall national economic growth.

Unlike WikiLeaks founder Julian Assange, who hacked into classified data and information in the history of the United States and then exposed it to the public for political purposes, Bjorka’s actions were more likely motivated by economic motives. By offering stolen data to buyers, Bjorka’s actions clearly indicated a transaction and the profits to be made. Among hackers, there is a consensus that successful data hacks are merely a ‘testing ground’ for building reputation and inner satisfaction. However, there is also a dominant motive: profiting from businesses, public service agencies, and government institutions (Justice.gov).

The high selling price of illegal personal data allows hackers to reap profits ranging from millions to billions of rupiah. Examined from a political perspective, political data theft also motivates hackers, such as Bjorka’s actions, which successfully stole and disseminated the personal data of several important officials. Bjorka's illegal actions (hacktivism) confirm the weakness of digital data security systems for the public, but also for officials and political elites. The crime of stealing citizens' personal data, at first glance, may be motivated by commercial motives. However, it must be remembered that hackers also have countercultural targets, namely the motive or ambition to delegitimize the state's permanent control over the centralization of digital management. According to Douglas Thomas (2002), in many hacking cases, hacker culture often displays the ambition of hackers (and their networks) to delegitimize the government in the eyes of the national public or downgrade the government's reputation in the eyes of the international community as an 'achievement' or the result of a 'reputation' battle between the state and the hacker community. As data hacking cases spread across many countries, the spread of political crises and the waning public trust in governments and state institutions in guaranteeing data protection for citizens are political facts that are difficult to deny.

## Implications of Election Integrity

In a democracy, individual privacy is crucial, including the protection of citizens' personal data. However, with each election approaching, particularly the simultaneous elections on February 14-15, 2024, cases of voter list (DPT) data leaks have resurfaced. Politically, the DPT is the entry point for maintaining public trust in the election process and results. If the DPT is not safeguarded, the quality of democratic, transparent, and fair elections based on competition and public participation will clearly be difficult to achieve.

**Table 5.** Various Cases of Voter DPT Data Leaks

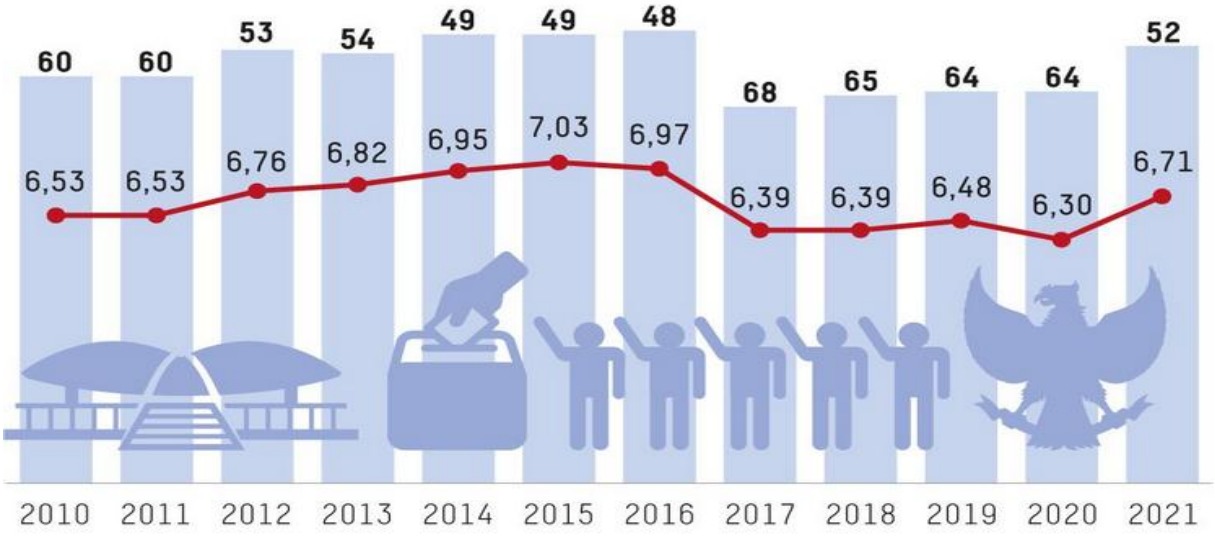
| Month/Year | Case | Description |
|---|---|---|
| September, 2020 | KPU DPT Leak | 105 million KPU election voter list (DPT) data leaked online. This leak was revealed by the account @underthebreach on Thursday, May 21, 2020. The hacked DPT data was shared in the hacker community, which shared an image showing that the hacker had 2.3 million DPT data from the 2014 election. The hacker also claimed to still have 200 million Indonesian citizen data that will be shared in the forum. |
| May, 2022 | KPU DPT Leak | Millions of Indonesian citizens' data from the 2014 Election Voter List (DPT) was leaked online. Although only 2.3 million were leaked, the hacker claimed to have 200 million more to share. The data was shared on the raidxxx.com forum on Wednesday, May 20, 2020, by an account with the initials Arlinst. The 2.3 million DPT data came from the Yogyakarta Special Region (DIY) Province, containing names, place/date of birth, National Identification Number (NIK), and complete address. The data cannot be downloaded for free; it must be exchanged for 8 credits, equivalent to 8 Euros. |
| September, 2022 | KPU DPT Leak | On September 6, 2022, another alleged data leak occurred, with more than 105 million data items being sold by a hacker named Bjorka on the Breached Forums website, allegedly from the General Elections Commission (KPU), under the title "Indonesia Citizenship Database From KPU 105M." Bjorka claimed to hold 105,003,428 million Indonesian citizen data, including details such as National |

| | | |
|---|---|---|
| | | Identity Number (NIK), family card (KK), full name, place and date of birth, gender, age, and more. The personal data was sold for US$5,000, equivalent to Rp7.4 million (US$1 = Rp14,898.20). All of the data was stored in 20GB (uncompressed) or 4GB (compressed) files. |
| November, 2023 | KPU DPT Leak | Alleged data leaks in Indonesia have occurred again at the end of 2023. The 2024 Election Final Voter List (DPT) data managed by the General Elections Commission (KPU) was hacked by the anonymous account Jimbo. The 204 million data hacked from the KPU website will be sold by Jimbo, the DPT from 514 regencies/cities and 128 representative countries for US$74,000 (Rp1.14 billion). The hacked data includes National Identity Number (NIK), Family Card Number (KK), National ID Card (KTP) Number, Passport Number (for overseas voters), full name, gender, date of birth, place of birth, marital status, and residential address (complete with neighborhood unit (RT), neighborhood unit (RW), village, sub-district, and district codes, as well as polling station (TPS) codes). As evidence, Jimbo shared 500 sample data uploaded to the darkweb site Breach Forums. |

Source: Data processed from various sources

Allegations of voter data leaks that have emerged at every stage leading up to the election have raised public doubts about the seriousness of the government and election organizers (KPU) in ensuring what Norris (2020) calls ‘election integrity’; or what Dawson (2022) questions as: how much legal force can protect human rights, amidst the current massive influx of digital technology-based information? The problem is, even though the government has special regulations (lex specialis) related to personal data protection with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) on October 17, 2022, cases of personal data theft continue to occur in many sectors and are increasingly difficult to handle.

**Graph 7**. Indonesian Democracy Index 2010-2021 (from 187 Countries)



Source: Purnamasari, 2023

*Note*: The democracy index is determined based on five variables: (1) election administration and pluralism; (2) government effectiveness (function); (3) political participation; (4) political culture; and (5) civil liberties. The index ranges from 0 to 10. This means that the higher the index score, the better the democracy index.

Examined from a public opinion perspective, public perception regarding the security of personal data protection remains very low. Referring to the results of a survey by the Kurious-Katadata Insight Center (KIC) in July 2023, the majority of respondents (62.5%) stated they were ‘not confident’ about the cybersecurity of the Indonesian government’s data storage centers. Specifically, 19.1% of respondents answered ‘very unsure,’ and 43.4% answered ‘not confident.’ On the other hand, 30% of respondents stated they were confident in the level of cybersecurity in Indonesia, with 22% responding ‘confident’ and 8.1% responding ‘very confident.’ Another 7.4% responded ‘don't know’ (katadata.co.id, 2023).

**Table 6.** Percentage of Respondents’ Confidence in Indonesian Cybersecurity (July 2023)

| Respondent Confidence | Value/Percent (%) | Proportion |
|---|---|---|
| Very unsure | 19,1 | 62,5 |
| Not confident | 43,4 | |
| Certain | 22 | 30 |
| Very confident | 8,1 | |
| Don’t know | 7,4 | 7,4 |

Source: katadata.co.id, 2023

*Description*: The survey conducted by Kurious-KIC involved 633 respondents from various regions in Indonesia, with 55% female respondents and 45% male respondents. The majority of respondents came from Java (64%), namely DKI Jakarta (14.2%), followed by respondents from Sumatra (12.3%). Meanwhile, the proportion of respondents from Kalimantan, Sulawesi, Bali-Nusa Tenggara, and Maluku-Papua ranged from 0.6% to 3.8%.

Referring to table 7 above, it can be seen that the answers ‘very unsure (19.1%) and ‘not sure’ (43.4%) from respondents spread across the country take the highest proportion (62.5%) regarding cybersecurity in Indonesia. The above data is relevant to a study conducted by the Digital Readiness Index (a digital index measurement institute based in Australia) which measures digital readiness in 146 countries based on the following seven major indicators: (1) the level of fulfillment of basic community needs; (2) government and private investment in the technology sector; (3) ease of doing business; (4) quality of human resources; (5) start-up climate; (6) level of adoption (and innovation) of digital technology; (6) condition of digital.

**Table 7**. Southeast Asian Countries Digital Index Score

| Nama Negara | Nilai/Poin<br>(Skala -2,5 – 2,5) | Status |
|---|---|---|
| Singapura | 2,37 | High readiness |
| Malaysia | 0,46 | Ready |
| Thailand | 0,32 | Ready |
| Vietnam | 0,22 | Ready |
| Indonesia | - 0,06 | Not ready |
| Filipina | - 0,25 | Not ready |
| Kamboja | - 0,38 | Not ready |
| Timor Leste | - 0,80 | Not ready |

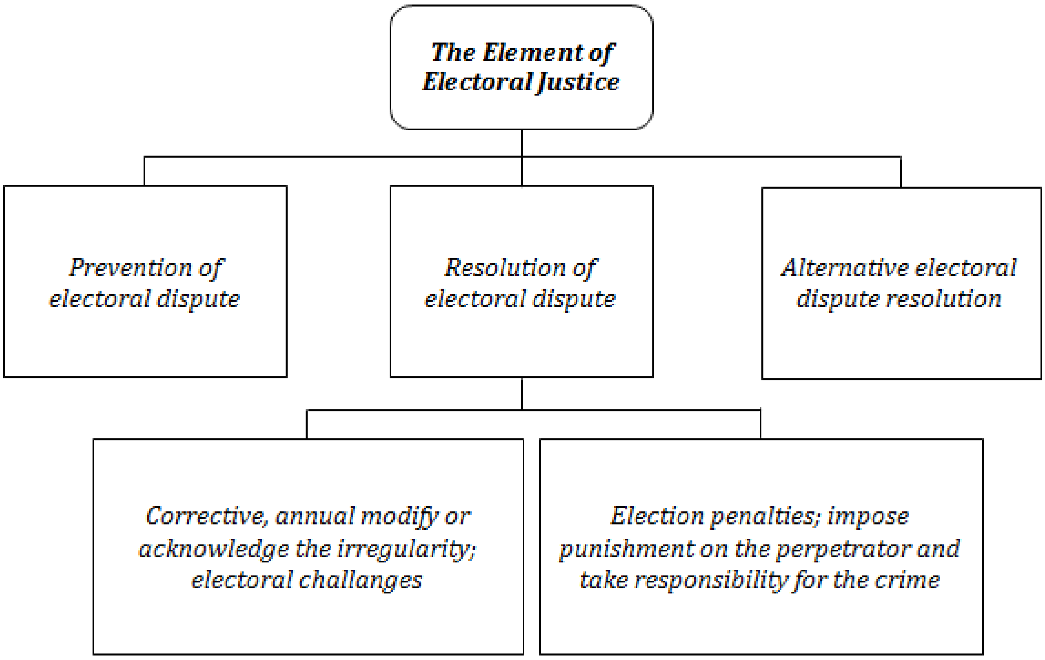
| | | |
|---|---|---|
| Myanmar | - 0,85 | Not ready |
| Laos | - 0,89 | Not ready |

Source: katadata.co.id, 2023

The data above shows that hacking or data theft due to a lack of security preparedness in protecting citizens' personal data (cybersecurity) has a large potential to damage public trust regarding the election process and results.

Regarding election integrity, in Towards an International Statement of Principles of Electoral Justice (2011), the Election Integrity Group refers to election integrity as a series of fair election implementation, including an election process with 10 main principles: (1) high integrity; (2) involving as many citizens as possible; (3) implemented based on the principle of high legal certainty; (4) impartial and fair; (5) professional and independent; (6) transparent; (7) on time according to plan; (8) without violence or free from threats and violence; (9) orderly; (10) election participants receive justice, win or lose (Joseph & McLoughlin, 2019).

**Figure 1**. Elements of Electoral Justice


The Element of Electoral Justice
Prevention of electoral dispute
Resolution of electoral dispute
Alternative electoral dispute resolution
Corrective, annual modify or acknowledge the irregularity; electoral challanges
Election penalties; impose punishment on the perpetrator and take responsibility for the crime

Source: Joseph & McLoughlin, 2019, p. 8

As a democratic country, Indonesia has also established six parameters for democratic elections: (1) direct; (2) general; (3) free; (4) secret; (5) honest, and (6) fair. The principle of democratic election integrity has become the mandate of Article 22E paragraph 1 of the 1945 Constitution. Meanwhile, the Election Law and Election Organizer regulations which are derivatives of the Election Law then added new criteria to ensure the election process and results have integrity, such as transparency, accountability, orderliness, and professionalism. In implementing the six principles of election administration and these additional criteria, Indonesian elections in the early reform era have also made a number of improvements starting from improvements to the electoral system, election governance (electoral process) and law enforcement (due to violations) of elections (electoral law).

However, the meaning of elections with integrity and quality as summarized in the definition of democratic elections above, in the course of subsequent elections experienced various crises, both caused by the authoritarian behavior of rulers, politicians and political elites with anti-democratic characters, causing many parties to lose confidence in the integrity of elections as an arena for testing democracy and a symbol of the people's sovereignty.

## CONCLUSION

The development of the internet and the massive migration of users have shifted the social and political order toward new values in the digital era, particularly in the practice of electronic democracy (e-democracy). Election technology opens up opportunities for broader and virtual political participation, but also poses serious risks such as leaks and theft of personal data in the lead-up to elections, which have the potential to undermine public trust in the integrity of the democratic process. This phenomenon highlights the vulnerability of government cybersecurity as a crucial point in ensuring the legitimacy of digital democracy, where cybercrime is not only economically motivated but can also lead to political delegitimization within the framework of global electoral technology hegemony.

Globally, from 2004 to 2021, more than 5.9 billion personal data items were leaked due to various attack methods, placing Indonesia among the countries with the highest data breach rates. The economic losses caused by hacking amount to billions of dollars, contributing to increased public unrest and eroding trust in digital security systems. Therefore, strengthening public control through multi-sector collaboration, accelerating regulations on personal data protection (such as the implementation of Law Number 27 of 2022 and its implementing regulations), and strengthening digital literacy are strategic steps for improving election governance and effective law enforcement.

However, data sovereignty and election integrity cannot be maintained solely through technical aspects. Substantive democracy, the foundation of elections with integrity, also requires a commitment from all stakeholders, especially political elites, to implement democratic principles comprehensively. In line with Anthony Giddens' (1990) prediction about the uncertainties and risks of modernity, digital democracy faces a tortuous and uncertain path, either descending into a legitimacy crisis or continuing within the uncertainties of new political structures influenced by information technology. Therefore, the sustainability of a credible and trustworthy democracy requires an integration of strengthened cyber technology, normative regulations, and responsible democratic practices.

## BIBLIOGRAPHY

### *Book*

Giddens, A. (1990) *The Consequences of Modernity*. Stanford, CA: Stanford University Press.

Graham, R. S., & Smith, S. K. (2019) *Cybercrime and Digital Deviance* (1st edition). New York, NY: Roudledge.

Miller, A. R. (1971) *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.

Thomas, D. (2002) *Hacker Culture*. Menneapolis: University of Minnesota Press.

***Online* (*Journal*)**

Clark, T. C. (1968) Privacy and Freedom (Book Review by Alan F. Westin). *California Law Review*, 56(3), 911-914. https://doi.org/10.2307/3479272.

Dawson, S. (2022) Electoral Fraud and the Paradox of Political Competition. *Journal of Elections, Public Opinion and Parties*, 32(4), 793-812. doi: 10.1080/17457289.2020. 1740716.

Furnell, S. M. (2001) Categorising Cybercrime and Cybercriminals: The Problem and Potential Approaches. *Journal of Information Warfare*, *1(*2), 35–44. https://www.jstor.org/stable/ 26486092.

Kusnaldi et al. (2022) Perlindungan Data Pribadi Dalam Penyelenggaraan Pemilu: Tantangan dan Tawaran. *Lex Renaissance,* 4(7), 710-725. doi: 10.20885/JLR.vol7.iss4.art3.

Lesmana, T. et al. (2022) Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3*(2), 1-7. doi: 10.52005/ rechten.v3i2.78.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2019) Exploring the Needs of Victims of Cyber-Dependent and Cyber-Enabled Crimes: Victims and Offenders. *International Journal of Evidence-Based Research, Policy, and Practice*, *15*(1), 60–77. doi: 10.1080/15564886.2019.1672229.

Mahpudin (2019) Teknologi Pemilu, Trust, dan Post-truth Politics: Polemik Pemanfaatan Situng (Sistem Informasi Penghitungan Suara) pada Pilpres 2019. *Jurnal PolGov*, *1*(2), 157-197. doi: 10.22146/polgov.v1i2.55886.

Prosser, W. L. (1960). Privacy. *California Law Review*, *48*(3), 383-423. doi: 10.2307/3478805.

Priya, A. (2021) Case Study Methodology of Qualitative Research: Key Attributes and Navigating the Conundrums in its Application. *Sociological Bulletin*, *70*(1), 94-110. doi: 10.1177/0038022920970318.

Putra, H. (2020) Manipulasi Pemilu Dalam Proses Pencalonan Pada Pemilihan Bupati dan Wakil Bupati Sekadau Tahun 2015. *Electoral Governance Thesis*, *2*(2), 138-159. https://journal.kpu.go.id/index.php/teg/article/view/245/104.

Sandrawati, N. A. (2022) Antisipasi Cybercrime dan Kesenjangan Digital Dalam Penerapan TIK di KPU. *Electoral Governance: Jurnal Tata Kelola Pemilu Indonesia*, *3*(2), 232-257. doi: 10.46874/tkp.v3i2.655.

Saputra, W. (2023) The right to privacy: Tinjauan Terhadap Penyalahgunaan Data Pribadi Dalam Perspektif HAM. *Res Judicata*, *6*(2), 128-141. doi: 10.29406/rj.v6i2.6145.

Setiawan, H. B., & Najicha, F. U. (2022) Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data. *Jurnal Kewarganegaraan*, *6*(1), 976-982. doi: 10.31316/jk.v6i1.2657.

Silalahi, P. H., & Dameria, F. A. (2023). Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cybercrime Sebagai Kejahatan Transnasional. *Wajah Hukum*, *7*(2): 614-627. doi: 10.33087/wjh.v7i2.1244.

Skog, A. D., Wimelius, H., & Sandberg, J. (2018) Digital Disruption. *Business & Information Systems Engineering*, *60*(4), 431-437. doi: 10.1007/s12599-018-0550-4.

Warren, S. D., & Brandeis, L. D. (1890) The Right to Privacy. *Harvard Law Review*, *4*(5), 193-220. doi: 10.2307/1321160.

### ***Online*** **(*Article in Website*)**

Annual Report: European Data Protection Supervisor, 2019 (2020, January 17). Available at https://edps.europa.eu/sites/edp/files/publication/2020-03-17_annual_report_2020_en _0.pdf.

Bialik, C. (2012, August 21) Voter Fraud: Hard to Identify (Aricle in *The Wall Street Journal*). Available at https://www.wsj.com/articles/SB10000872396390443864204577621732936167586.

Clinten, B., & Wahyudi, R. (2022, September 01) Data 1,3 Milyar Nomor HP Diduga Bocor, Ada NIK dan Nama Operator. Available at https://tekno.kompas.com/read/2022/09/01/12230827/data-13-miliar-nomor-hp-indonesia-diduga-bocor-ada-nik-dan-nama-operator?page=all.

CNNIndonesia.com (2019, July 15) 5 Alasan Mengapa Data Pribadi Perlu Dilindungi. Available at https://www.cnnindonesia.com/teknologi/20190715201531-185-412391/5-alasan-menga pa-data-pribadi-perlu-dilindungi.

"Cybercrime". Available at https://www.oxfordlearnersdictionaries.com/definition/english/cybercrime.

"Cybercrime". Available at https://www.merriam-webster.com/dictionary/cybercrime.

Dennis, M. A. Cybercrime. Available at https://www.britannica.com/ topic/cybercrime (2023, December 19).

dpr.go.id (2022, September 13) Keamanan Data di Indonesia Mudah Jebol, Perlindungan Data Pribadi Jadi PR Pemerintah. Available at https://www.dpr.go.id/berita/detail/id/40663/t/Keamanan-Data-di-Indonesia-Mudah-Jebol-Perlindungan-Data-Pribadi-Jadi-PR-Pemerintah.

Fatoni (2025, March 12) Pengguna Internet Indonesia Tembus 212 Juta Orang pada Tahun 2025. Available at https://tagar.co/pengguna-internet-indonesia-tembus-212-juta-orang-pada-tahun-2025/

Graham, R. S. (2017, October 19). The Difference Between Cybersecurity and Cybercrime, and Why it Matters. Available at https://theconversation.com/the-difference-between-cybersecurity-and-cybercrime-and-why-it-matters-85654.

Hardiansyah, Z. (2022, September 12) Rentetan Aksi Hacker Bjorka dalam Kasus Kebocoran Data di Indonesia Sebulan Terakhir. Available at https://tekno.kompas.com/read/2022/09/12/11000027/rentetan-aksi-hacker-bjorka-dalam-kasus-kebocoran-data-di-indonesia-sebulan.

"Identity Theft". Available at https://www.merriam-webster.com/dictionary/identity/theft.

Joseph, O., & McLoughlin, F. (2019) Electoral Justice System Assessment Guide. Available at https://www.eods.eu/library/IDEA_2019_ElectoralJusticeSystemAssessmentGuide.pdf.

Justice.gov (2019, May 23) WikiLeaks Founder Julian Assange Charged in 18-Count Superseding Indictment. https://www.justice.gov/opa/pr/wikileaks-founder-julian-assange-charged-18-count-superseding-indictment.

KumparanTECH (2020, May 06) Bukalapak Akui 13 Juta Data yang Dijual Hacker adalah Peretasan di Maret 2019. Available at https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G/.

Kusnandar, V. B. (2022, January 25) Jumlah Kapasitas Data BI yang Bocor (24 Januari 2022). Available at https://databoks.katadata.co.id/datapublish/2022/01/25/kebocoran-data-bank-indonesia-terus-bertambah-naik-jadi-74-gb.

Lidwina, A. (2020, September 01) Berapa Kerugian Negara-negara di Dunia Akibat Peretasan Data? Available at https://databoks.katadata.co.id/datapublish/2020/09/01/berapa-kerugian-negara-negara-di-dunia-akibat-peretasan-data.

Lokadata (2020) Kebocoran Data Menurut Sektor, Juni (2020). Available at https://lokadata.beritagar.id/chart/preview/kebocoran-data-menurut-sektor-juni-2020-1597308426.

Muhammad, N. (2023, August 10) Mayoritas Masyarakat Tidak Yakin dengan Tingkat Keamanan Siber di Indonesia. Available at https://databoks.katadata.co.id/datapublish/2023/08/10/mayoritas-masyarakat-tidak-yakin-dengan-tingkat-keamanan-siber-di-indonesia.

Muhammad, N. (2023, September 20) Indeks Kesiapan Digital Asia Tenggara, Skor Indonesia Tergolong Rendah. Available at https://databoks.katadata.co.id/datapublish/2023/09/20/indeks-kesiapan-digital-asia-tenggara-skor-indonesia-tergolong-rendah.

Naurah, N. (2022, November 21). Meninjau Tingkat Kasus Kebocoran Data Global, Apakah RI Aman? Available at https://goodstats.id/article/meninjau-tingkat-kasus-kebocoran-data-global-apakah-ri-aman-gsBoq.

Norris, P. (2020) Electoral Integrity in the 2020 U.S. Elections. Available at PEI-US-2020-Report-(Electoral_Integrity).pdf.

Nwosu, C. (2022, June 01) Visualizing The 50 Biggest Data Breaches From 2004-2021. Available at https://www.visualcapitalist.com/cp/visualizing-the-50-biggest-data-breaches-from-2004-2021/#google_vignette.

Purnamasari, D. D. (2023, September 09) Meski Raih Penghargaan Tinggi, Koalisi Masyarakat Sipil Nilai Keterbukaan Atas Layanan Publik Masih Rendah. Available at https://www.kompas.id/baca/polhuk/2023/09/08/koalisi-masyarakat-sipil-keterbukaan-pemerintah-di-layanan-publik-masih-rendah

Sahara, W. (2021, September 03). Deretan Kasus Kebocoran Data Pribadi dalam Dua Tahun Terakhir. Available at https://nasional.kompas.com/read/2021/09/03/18445501/deretan-kasus-kebocoran-data-pribadi-dalam-dua-tahun-terakhir?page=2#google_vignette.

Siregar, H. R. (2023, November 30) Data DPT di KPU Bocor Akibat Celah Internal. Available at https://newsletter.tempo.co/read/1803327/data-dpt-di-kpu-bocor-akibat-celah-internal.

Sugiharti, R. (2022, September 19) Peretasan Data dan Krisis Kepercayaan Masyarakat. Available at https://mediaindonesia.com/kolom-pakar/523462/peretasan-data-dan-krisis-kepercayaan-masyarakat.

Tamtomo, A. B., & Galih, B. (2022, August 09) Infografik: Kasus-kasus Besar Kebocoran Data Pribadi di Indonesia. Available at https://www.kompas.com/cekfakta/read/2022/09/08/101500782/infografik--kasus-kasus-besar-kebocoran-data-pribadi-di-indonesia.

The Conversation (2023, October 06) Privasi Dalam Pemilu: Data Pribadi Rentan Disalahgunakan Jelang Tahun Politik, Kualitas Demokrasi Dipertaruhkan. Available at heconversation.com/privasi-dalam-pemilu-data-pribadi-rentan-disalahgunakan-jelang-tahun-politik-kualitas-demokrasi-dipertaruhkan-215078.

U.S Departement of Justice [Criminal Division] (2023, August 11) Identity Theft. Available at https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

What To Know About Identity Theft (2021, April Edition) Available at https://consumer.ftc.gov/articles/what-know-about-identity-theft.

Widi, S. (2023, July 06) Deret Kasus Kebocoran Data RI Pada 2023, dari BSI hingga Paspor. Available at https://dataindonesia.id/internet/detail/deret-kasus-kebocoran-data-ri-pada-2023-dari-bsi-hingga-paspor.