# Preventing data leaks for more honorable 2024 elections



**Arfianto Purbolaksono**
Research and Program Manager of the Indonesian Institute

The end of November 2023 saw a violation against the official website of the General Election Commission (KPU), which was reported to have been hacked, with approximately 204 million data points from the permanent voter list (DPT) allegedly leaked. According to a report from the Communication and Information System Security Research Center (CISSReC), a hacker calling itself "Jimbo" obtained the data and sold it for US$74 thousand, which is equal to IDR 1.2 billion.

Approximately 253 million pieces of data were hacked by Jimbo; this number shrank down to 204 million after filtration, similar to the KPU Permanent Voter List (DPT Tetap). Pratama Persadha, Chairman of the Cyber Security Research Institute CISSReC, stated that Jimbo filtered down to 204,807,203 unique data points, a number almost identical to the total number of voters in the KPU Permanent Voter List, which is 204,807,222 voters from 514 districts and cities in Indonesia and 128 representative countries.

Still in the CISSReC report, Jimbo also shared 500 samples of the data obtained, which he uploaded to BreachForums, a dark website. Jimbo managed to obtain the National Identification Number (NIK), Family Card (KK) number, Identity Card (KTP) number (including passport number for voters residing abroad), full name, gender, date of birth, place of birth, marital status, complete address, Neighborhood Association (RT), Community Unit (RW), village code, sub-district, district, and the code for the Polling Station (TPS). The hacking incident is not the first to occur. Bjorka set the trend earlier, in 2022, with 105 million of leaked KPU data. This incident should have alarmed the KPU about protecting the ongoing electoral data more securely.

Data leaks are not anything new in Indonesia. According to Surfshark, Indonesia ranks 13th-highest in the world for data breaches, as evidenced by a total of 143.7 million email address account data leaks since 2004. The number has also increased by 85 percent within the past two quarters.

Surfshark previously identified three major data leak incidents, with the first being Tokopedia in April 2020, leaking fifteen million accounts, followed by Wattpad in June 2020, with 22.9 million compromised accounts and a data breach affecting 12.6 million IndiHome accounts in August 2022.

Records from Indonesia's Ministry of Communication and Information Technology (*Kominfo*) reveal 35 data leak cases between January and June 2023. This number exceeds the annual number of data leaks reported from 2019 to 2021.

Personal data leaks can cause a number of concerns, including blackmail and threats to publish personal information or confidential information. Other threats include credit card fraud, identity theft, and online scams.

Next, leaked personal data may cause identity theft used to commit other crimes, such as bank accounts infiltrating using that obtained data. Therefore, it is crucial to protect personal data.

Indonesia has established regulations for protecting personal data, which are regulated in Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). However, the PDP law has not been effectively enacted due to several issues, including the need for more specific technical regulations such as guidelines and directives for the UU PDP.

Another issue is the absence of a specific institution responsible for personal data protection. Articles 58 to 60 of the Personal Data Protection Law (UU PDP) have stipulated the establishment of an institution for personal data protection; however, there is none authorized up to date.

Concerning the KPU data breach case, Wahyudi Djafar, the Executive Director of the Institute for the Study and Advocacy of Society (ELSAM), stated that KPU should transparently and clearly explain the extent of the data system security for the 2024 elections, as the election's integrity will potentially be impacted by this data breach.

Wahyudi Djafar also expressed another concern: the public is questioning the assessment and security audit system concerning the reliability level of KPU's information data systems, considering that the data is highly sensitive, containing personal data from voters' National Identification Numbers (NIK) to their residential addresses.

KPU's explanation and commitment are crucial to improving its data security system, as the public still perceives that personal data protection is conducted with minimum security. According to a survey result by the Kurious-Katadata Insight Center (KIC) in July 2023, the majority, or 62.6 percent of respondents, mistrusted the cybersecurity level of the Indonesian government's data storage center. As much as 19.1 percent of respondents were extremely uncertain, and 43.4 percent answered that they were uncertain.

On the other hand, 30 percent of respondents were confident about the cybersecurity level in Indonesia. 22 percent of respondents expressed high confidence and the remaining 8.1 percent trusted the cybersecurity system. Less than 7.5 percent responded that they did not have the faintest idea. The KPU needs to provide proper explanations and assurances regarding the confidentiality of electoral data. It is crucial to prevent public skepticism of the election results.

The KPU must take numerous measures to prevent future election data leaks. Firstly, by explaining to the public about the recurring hackings, making them more transparent and accountable.

Secondly, the KPU should openly involve multiple stakeholders in securing data related to the 2024 elections, which include civic tech, the private sector, civil society groups, and mass media. A multi-stakeholder partnership is expected to address vulnerabilities in data leaks at KPU, which might have involved weak security infrastructure and human resources.

Finally, it encourages the Election Supervisory Board (*Bawaslu*) to work with civil society groups and mass media to monitor and criticize the KPU information system services, as it will force KPU to seriously improve the conduct of elections. A strong KPU promotes public participation in monitoring and reporting any electoral violations and ensuring the integrity of the 2024 election.

# The traitor drone

It seems that this has not been regulated in the laws of war, whether it's allowed or not. It is happening more and more frequently: killing enemies from a distance. Without any prior declaration of war. An Iranian intelligence general was killed a few days ago. The assassin was thousands of kilometers away. In another country.

The general was on a visit to Damascus, Syria. At 10:30 a.m., he was in a multi-story building commonly used by Iranian military officials; Iran and Syria have a very strong relationship.

Then, in the hot afternoon, a drone hovered in the Syrian sky. An unmanned drone suddenly launched a weapon, precisely hitting its target.

The building was destroyed, engulfed in flames. Brigadier General Sadegh Omidzadeh was instantly killed, as was his deputy, Hajj Gholam, with their three other staff members.

From an intelligence perspective, the building meets the requirements of a "safe place" as it is located in a complex of embassy buildings from various countries. Such areas are usually considered safe from attacks. However, this long-distance attack resembles long-range sniper tactics, where it can hit the target precisely without affecting or disturbing other, neighboring, buildings.

Target accuracy is set on a computer, indicating that the traditional sniper's role has been automated. This drone technology no longer needs a sniper to seek a precise shooting position; they can perform the task from anywhere.

This time, it was Israel's job. Iran once lost a general in a nearly similar way. The assassin was not Israel, but its big boss: the United States.

The general, Qasim Solaimani, was also on a visit to another country: Iraq. Once the vehicle carrying Soleimani's convoy was on a highway outside Baghdad, an aerial weapon struck the car. It exploded, and the general was killed instantly. The shots were also launched by an unmanned drone.

A month ago, a senior Hamas official in Beirut, Lebanon, was also killed in a targeted drone strike. He was a deputy leader of Hamas: Saleh al-Arouri.

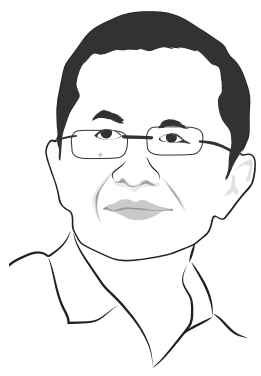
So I was thinking... "Why would they not just assassinate Vladimir Putin in the same way? Or Kim Jong-un. Even Ayatollah Khamenei, for that matter".

It is possible that Israel and America might have planned that. Perhaps they have not found intelligence sources to provide these figures' whereabouts. Israel and America's most abominated icons. They haven't identified the right traitors yet.

I can only imagine how hard it would be to protect such people in times like these. There would be no need to deploy troops to Jayawijaya (the mountains of Papua) anymore. All assassins can delegate all the challenging "wet jobs" to Mr. Drone.

However, drones are not intelligent, without the assistance of the other party – the traitors.

I can imagine the many double-faced traitors in Lebanon, Syria, Iraq, Palestine, and Gaza right now, as without them, drones are just flying unmanned lurkers. The traitors are the ultimate key.



**Dahlan Iskan**
Former SOE Minister