*Proceeding* of
The Sunan Ampel International Conference of Political and Social Sciences (SAICoPSS),
Faculty of Social and Political Sciences UIN Sunan Ampel Surabaya
Volume 1, 2023, 254-266
DOI: https://doi.org/10.15642/saicopss.2023.1..254-266

# ANALYSIS OF THE INDONESIAN GOVERNMENT'S EFFORTS IN OVERCOMING PUBLIC DATA LEAK CASES

**Sintya Dewi Rahma[1], Bonifasius Ananda Putra[2], Lukman Fahmi Djarwadit**

[1]Universitas Sebelas Maret, Surakarta, Indonesia
sintyadrhm@student.uns.ac.id
[2]Universitas Sebelas Maret, Surakarta, Indonesia
putrabonifasius22@student.uns.ac.id t
Universitas Sebelas Maret, Surakarta, Indonesia lukman.f.d@staff.uns.ac.id

ABSTRACT

Public data leaks pose significant challenges to individuals' privacy and national security in the digital age. This paper provides a focused analysis of the Indonesian government's efforts to address public data leak incidents. It begins with an overview of the increasing prevalence of data leaks in Indonesia, emphasizing the need for effective government responses. The analysis delves into the existing legal framework and regulations governing data protection and cybersecurity, highlighting their strengths and limitations. It assesses the government's initiatives, policies, and technological measures designed to prevent and mitigate data leaks, with case studies illustrating specific incident responses. Challenges and constraints faced by the government, such as enforcement issues and resource limitations, are examined. International best practices are also considered to provide comparative insights.The analysis concludes with recommendations for strengthening the government's efforts, emphasizing policy improvements, legal reforms, and capacity building. This paper underscores the pivotal role of government action in safeguarding public data, privacy, and human security in the digital era.

**Keywords:** Data Leak, Cybersecurity, Privacy, Government Efforts, Indonesia

## INTRODUCTION

Many people often ask whether Indonesia is actually ready to face the era of digitalization and information openness or not. This question is always disturbing and, unfortunately, continues to find relevance when various cases of data leakage of private/public information or state-owned data occur repeatedly. In fact, this country has not been able to provide maximum protection for public data. The state is more often helpless when other parties so easily and frequently harvest their citizens' personal data. What's even sadder is that the leaked data mostly comes from data from government agencies.

An unforgettable example of this case occurred in 2021, where data on 279 million BPJS Health participants was allegedly leaked. No half-hearted, what was leaked was

data on population identification numbers (NIK), names, addresses, e-mails, even personal photos. These data were then suspected of being bought and sold. The previous year, the General Election Commission (KPU) also reported the alleged leak of data on millions of permanent voter lists (DPT). In the same year, there were also reports that data on 1.3 million Ministry of Education and Culture employees was leaked, although this was later denied by the ministry. Last year, Indonesia was again shocked by the data leak by a hacker who claimed to be named Bjorka. Data at a number of agencies, both government institutions and corporations, was hacked and leaked. In fact, it was not only the personal data of Indonesian citizens that was leaked, but also confidential letters and documents from the State Intelligence Agency (BIN) to President Joko Widodo.[1]

Repeated data leaks are actually a disaster. This is a serious problem because in the end it will also be related to the security and sovereignty of the country. EvenIndonesia is ranked third with the highest number of accounts experiencing data leaks in the third quarter of 2022. With more than 12 million hacked accounts and cases increasing every month, the government must improve to deal with attacks.hacker in the digital space for public safety. This hacking action not only violates social norms, but can also cause public unrest. Therefore, a clear legal umbrella is needed to reduce the number of hacks of personal data. For this purpose, the Ministry of Communication and Information of the Republic of Indonesia (Kominfo) immediately drafted the Draft Law on Personal Data Protection (PDP). Quoted from the kominfo.id site, the Minister of Communication and Information, Johnny G Plate, said that completing the bill is a top priority to maintain the sovereignty and security of public data.[2] This article will discuss cases of data leaks that have occurred in Indonesia, the government's efforts to overcome the problem of data leaks, and the challenges that exist in the government's efforts.

[1] Media Indonesia. (2023, July 8). Kebocoran data tidak terbendung. Mediaindonesia.com. https://mediaindonesia.com/editorials/detail_editorials/3061-kebocoran-data-tidak-terbendung
[2] ITS News. (2022, November 2). Menyikapi Kasus Kebocoran Data Pribadi di Era Digital. ITS News. https://www.its.ac.id/news/2022/11/02/menyikapi-kasus-kebocoran-data-pribadi-di-era-digital/

## DATA LEAK CASES IN INDONESIA

In fact, data leaks belonging to users of a number of applications in Indonesia have been occurring frequently for several years. The personal information that was confiscated made them worried because it could be used as a field for cyber crime by the perpetrators. Not surprisingly, the public is questioning the performance of the Ministry of Communication and Information (Kominfo), which is considered to be most responsible for the leak of this personal information. Moreover, the latest case of leaking customer SIM number data is not the first time this has happened.

The following is a list of several data leak cases in Indonesia, starting from data from the Social Security Administering Agency (BPJS), President Joko Widodo's vaccine certificate to the latest regarding Population and Civil Registration (Dukcapil) data.

a. Social Security Administering Agency (BPJS) Data Leak

The BPJS Health data leak case first shocked the Indonesian public via Twitter social media in May 2021. It was recorded that 279 million BPJS Health user data was sold on the online forum site Raidforums.com for 0.15 bitcoin or around Rp. 87.6 million.The data leak of 279 million people is indicated to involve names, telephone numbers, addresses, salaries and population data. It is possible that ASN data was also included in the data leak. Because ASN and TNI-Polri soldiers are also BPJS Health participants.This calculation is based on the impact of massive hacking of personal contact numbers and social media accounts. This data can be used for cyber crimes such as irresponsible use of online loans.[3]

b. Bank Republik Indonesia (BRI) Customer Data Leak

Data on two million BRI Life customers was allegedly leaked and sold online. Information about leaking customer data BRI Life was uploaded by a Twitter account on Tuesday, July 27 2021. In the upload, it was written that the perpetrator threatened to sell

[3] Burhan, F. A. (2021, June 25). Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun - Teknologi Katadata.co.id. Katadata.co.id. https://katadata.-co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehatan-disebut-bikin- rugi-negara-rp-600-triliun

BRI Life's sensitive data. Hackers allegedly stole 250 gigabytes of customer data from the insurance company and sold it for US$ 7,000 or Rp. 101.5 million. BRI Life management conducted an investigation into the data breach case. Management stated that there was intrusion by cybercriminals into the BRI Life Syariah system. However, management claims the system is separate from the main BRI Life system and the amount of data contained is not as much as the hacker claims.[4]

c. President Joko Widodo's Vaccine Certificate

The Indonesian mass media and social media were shocked about the second stage of Covid-19 vaccination certificate belonging to Indonesian President Joko Widodo (Jokowi) which was 'leaked' and circulated on Twitter. As for the information circulating on Twitter, it was said that Jokowi had received his second vaccination on January 27 2021 using the Sinovac vaccine.The Ministry of Health (Kemenkes) finally explained that there was a lot of false information (hoax) along with the leak of President Jokowi's Population Identification Number (NIK) and there was no evidence of leakage of personal data in the applicationCare Protect. The National Cyber Crypto Agency (BSSN) and the Ministry of Communication and Information (Kominfo) also stated that certificate access uses features in the Peduli Protect system.[5]

d. State Electricity Company (PLN) User Data Leak

In 2022, issue related data leaks occurred again, namely leaks of customer data from the State Electricity Company (PLN). Hacker with the account name @loliyta claims to have stolen 17 million PLN customer data on the breached.to site on a hacker forum called Breach Forum. The perpetrator offers several types of customer data, such as field ID,

[4] Hidayat, A. A. N. (2021, July 29). Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi. Tempo. https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regula si?page_num=3

[5] Sidik, S. (2021, September 5). Geger Sertifikat Vaksinasi Jokowi Bocor, Ini Respons Kemenkes. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20210905121451-37-273736/geger-sertifikat-vaksinasi-jokowi-bocor-ini-respons-kemenkes

customer ID, consumer name, address, energy type, meter number and KWH amount.One independent cyber security researcher, Afif Hidayatullah, believes that the data leak really came from PLN.[6]

e. SIM Number Data Leak

In 2022, the Indonesian social media world was also shocked by the news that 1.3 billion SIM card registration or registration data in Indonesia was allegedly sold. A number of Twitter accounts conveyed this information. They said the data seller admitted to getting 1.3 billion data from the Ministry of Communication and Information (Kominfo). The data that was reportedly leaked was said to be rejected. Because it contains the Population Identification Number (NIK), telephone/cellphone number, name of the service provider or providers, up to the registration date. A total of 1.3 billion SIM card registration data was also allegedly priced at IDR 742 million. The perpetrator even distributed free samples of 2 million user data.[7]

f. Passport Data Leak

Recently, in July 2023 to be precise,The Ministry of Communication and Information will provide clarification to the Directorate General of Immigration, Ministry of Law and Human Rights regarding the alleged leak of passport data for 34,900,867 Indonesian citizens. Director General of Informatics Applications at the Ministry of Communication and Information, Semuel A. Pangerapan, stated that an initial investigation had been carried out by the Personal Data Protection Investigation Team, both from the website that offered the data and information from the public. The Ministry of Communication and Information found that there were similarities with passport data.The Ministry of Communication and Information also coordinates with related parties in accordance with

[6] Saskia, C. (2022, September 2). 3 Kasus Kebocoran Data di Indonesia dalam Sebulan, dari PLN, IndiHome, hingga Nomor SIM Card Halaman all (R. Nistanto, Ed.). KOMPAS.com. https://tekno.kompas.com/read/2022/09/02/10260777/3-kasus-kebocoran-data-di-indonesia-dalam-sebulan-dari-pln-indihome-hingga?page=all

[7] Nabilla, F. (2022, September 2). 11 Daftar Kasus Kebocoran Data di Indonesia, Sebulan Tiga Kali Kejadian! Suara.com. https://www.suara.com/news/2022/09/02/115017/11-daftar-kasus-kebocoran-data-di-indonesia-sebulan-ti ga-kali-kejadian

applicable regulations, namely the National Cyber and Crypto Agency (BSSN), as well as the Directorate General of Immigration, Ministry of Law and Human Rights. On the other hand, Akuncom - a cyber security company - believes the leaked data is "valid", because there are two passport numbers and NIKIM which are only held by the owner and authority.[8]

g. Population and Civil Registration Data (Dukcapil) Leaks

Not only passport data, this year Indonesia was also shocked again by the alleged leak of Dukcapil data. Previously, the hacker with the anonymous name "RRR" sold 34 million passport data and 1.3 trillion telephone SIM card registration data, now the hacker is offering 337 million data allegedly from the Ministry of Home Affairs Dukcapil in online forums.hacker Breach Forums. Cyber security expert, Alfons Tanujaya, said that referring to the number which exceeds the total population of Indonesia, there is a possibility that the data contains information on residents who have died. Millions of core data of Indonesian citizens is suspected to "copies raw" from the dukcapil.kemendagri.go.id server because it contains 69 columns, 28 of which contain important personal information. Of the one million sample data that can be accessed, the leaked information contains population identification numbers (NIK), names complete, date of birth, birth certificate number, blood type, religion and marital status. Then marriage certificate number, divorce certificate number, date of marriage, date of divorce, and what is quite worrying is physical abnormalities. There is also data on final education, type of work, father's NIK, mother's NIK, father's full name, and mother's full name.[9]

## LEGAL FRAMEWORK AND REGULATIONS

Indonesia has made tremendous progress in establishing a legislative framework for data protection and cybersecurity. These frameworks and institution are in the form of:

[8] BBC News Indonesia. (2023, July 7). Sebanyak 34 juta data pemegang paspor diduga “bocor” – “Yang menderita rakyat, pemerintah paling dapat malu.” BBC News Indonesia. https://www.bbc.com/indonesia/articles/c9e7e9grjmko

[9] BBC News Indonesia. (2023b, July 18). Peretasan: 337 juta data Dukcapil Kemendagri diduga bocor, pakar siber: “Ini paling parah karena memuat data nama ibu kandung.” BBC News Indonesia. https://www.bbc.com/indonesia/articles/c51v25916zlo

a. The Electronic Information and commerce Law (UU ITE)

This is the foundation of these legislation, including many areas of digital commerce, data protection, and cybersecurity. This legislation empowers the government to take action against cybercrime and data breaches, safeguarding the security and integrity of electronic data. UU ITE, which was enacted in 2008 and later updated in 2016, has developed to meet the demands of the digital era. It discusses numerous elements of electronic transactions, such as electronic signatures and papers, as well as the usage and security of electronic systems. One of UU ITE's primary goals is to prevent cybercrime and secure electronic information. It gives the Indonesian government the authority to prosecute certain cyber-crimes such as hacking, data breaches, and online defamation. The law also covers the roles of internet service providers, content suppliers, and users in ensuring the security and integrity of electronic data. However, UU ITE has been chastised for possible abuse, notably in situations of free expression and slander. The provisions of the legislation have provoked disputes regarding the balance between cybersecurity and individual rights, making it a topic of continuous debate and prospective amendments in Indonesia.[10]

b. The Freedom of Information Act (Undang-Undang Keterbukaan Informasi Publik or UU KIP):

Also known as Law No. 14 of 2008 on Public Information Disclosure, is a key piece of legislation in Indonesia that aims to promote openness and public access to government information. This law, passed in 2008, is critical in increasing government accountability and allowing individuals to receive information about the acts and decisions of public institutions. UU KIP implements openness standards, requiring government entities to share information to the public upon request. It broadens the definition of "public information" to include any information maintained by government entities, subject to specific exclusions and constraints, such as national security and personal privacy. The law also compels agencies to make certain types of information available to the public

[10] SIPPN. (2023, May 14). Berita SIPPN - Mengenal Undang-Undang ITE. SIPPN - CARIYANLIK. https://sippn.menpan.go.id/berita/58352/rumah-tahanan-negara-kelas-iib-pelaihari/mengenal-undang-undang-ite

ahead of time. This law provides journalists, civil society groups, and people with critical access to government records, papers, and data. It supports the notion that openness and accountability are necessary components of a functioning democracy. UU KIP is a cornerstone of Indonesia's attempts to develop a culture of openness and citizen engagement in government activities by providing methods for citizens to seek and receive information from public entities.[11]

c. The Indonesian Government rule on Information and Documentation Management (Peraturan Pemerintah Nomor 66 Tahun 2010 or PP No. 66/2010)

This is a key rule that describes the principles and methods for managing government documents and information. This legislation, enacted in 2010, intends to promote the methodical and effective administration of government records and data, while also fostering openness, accessibility, and accountability in the public sector. The Public Procurement Procedure No. 66/2010 defines rules for categorizing government documents depending on their sensitivity and relevance. It describes the methods for creating, maintaining, storing, and disposing of government documents. The rule highlights the need of preserving and protecting significant materials, as well as making information available to the public. This rule is critical in improving the Indonesian government's information and documentation management. It contributes to the larger purpose of encouraging openness, accountability, and efficient governance by establishing rules and processes for how government information should be handled and preserved. It guarantees that government documents and data are properly kept and that the public may access them when needed, in line with Indonesia's commitment to transparency and good governance.[12]

[11] RSJD Soedjarwadi. (n.d.). Tentang Keterbukaan Informasi Publik. Ppid.rsjd-Sujarwadi.jatengprov.go.id. http://ppid.rsjd-sujarwadi.jatengprov.go.id/halaman/detail/tentang-keterbukaan-informasi-publik-#:~:text=U ndang%2DUndang%20No.%2014%20tahun

[12] Hukum Online. (2023). Peraturan Pemerintah Nomor 66 Tahun 2010 - Pusat Data Hukumonline. Hukumonline.com. https://www.hukumonline.com/pusatdata/detail/lt4cb2becd53181/peraturan-pemerintah-nomor-66-tahun-2 010

d. The National Cyber and Crypto organization (Badan Siber dan Sandi Negara, or BSSN),

Indonesia also has a government organization in charge of coordinating and implementing the country's cybersecurity policies and initiatives. The BSSN is the central authority for all cybersecurity problems and plays a critical role in protecting the country's digital infrastructure and sensitive government data.[13] Among BSSN's key roles and functions are:

1. Coordination of Cybersecurity activities: The BSSN is in charge of coordinating cybersecurity activities across multiple government departments, ministries, and organizations. It aims to guarantee that cyber risks and events are dealt with in a coordinated and effective manner.
2. Policy Development: The agency is involved in the development of national cybersecurity policies, strategies, and standards. It contributes to the development of Indonesia's legislative and regulatory environment for cybersecurity.
3. Incident Response: BSSN monitors and responds to cybersecurity incidents such as cyberattacks and breaches. It is working to lessen the effect of these occurrences and to avoid future assaults.
4. Capacity Building: BSSN works to improve Indonesia's cybersecurity capabilities by providing government agencies and companies with training, resources, and direction.
5. Worldwide Collaboration: The agency works with worldwide partners and organizations to share information and knowledge on best practices in cybersecurity and emerging threats.[14]

It is worth noting that the Indonesian government has been working to improve openness and data protection in the public sector. The Freedom of Information Act, in particular, is an important piece of law that encourages transparency and access to

[13] BSSN. (n.d.). Tentang BSSN | www.bssn.go.id. Badan Siber Dan Sandi Negara. Retrieved October 31, 2023, from https://www.bssn.go.id/tentang-bssn/
[14] CyberHub. (n.d.). Badan Siber dan Sandi Negara. Cyberhub.id. Retrieved October 31, 2023, from https://cyberhub.id/catalog/detail/e9d83191-2d49-46de-99f7-ded9de89d04d#:~:text=TUGAS

government information. However, it is critical to remain up to speed on the latest developments and changes in Indonesia's legislative framework governing public data protection.

## GOVERNMENT INITIATIVES AND RESPONSES

Specific steps, regulations, and initiatives undertaken in Indonesia in reaction to data breaches include:

1. Data Breach Notification Requirements:

The government has enacted legislation requiring enterprises to disclose data breaches as soon as possible. When a data breach happens, enterprises must inform both the authorities and the impacted individuals. This increases openness and helps people to take the appropriate measures.

2. Fines for Data Breach Negligence:

Indonesian regulations establish fines for firms that are careless in data security. These penalties might include fines and other legal ramifications, incentivizing firms to treat data security seriously.

3. Data Localization Requirements:

In order to improve data security, Indonesia has mandated data localization for certain categories of sensitive data. This implies that sensitive data must be held and processed within the borders of the country, decreasing the danger of unwanted access from outside entities.

4. Cybersecurity Audits and Assessments:

To detect vulnerabilities and shortcomings in government agencies' and enterprises' data protection processes, the government performs cybersecurity audits and assessments. These evaluations aid in the proactive management of potential data breach threats and the enhancement of overall cybersecurity.

5. Public Awareness and Training:

The government runs public awareness campaigns and offers training programs for people and companies to promote knowledge about data protection and cybersecurity best practices. Public education is viewed as a proactive method to avoid data leaks.

6. Data Protection Standards for Critical Infrastructure:

Specific data protection standards for critical infrastructure industries such as banking and finance have been created. These standards are intended to safeguard the security of critical systems and data in industries where data breaches might have serious effects.

7. Incident Response Protocols:

Government agencies and companies are encouraged to develop incident response protocols in order to respond to data breaches as soon as possible. These procedures outline the steps that must be performed, such as containment, investigation, and recovery.

8. Collaboration with International Partners:

In response to data breaches and cyber threats, Indonesia works with international organizations and partners to exchange information, knowledge, and resources. International cooperation is beneficial in dealing with cross-border cyber issues.[15] These particular regulations and initiatives are part of a larger plan in Indonesia to manage data breaches, secure sensitive information, and boost cybersecurity. To maintain data security and legal compliance, companies and people must keep knowledgeable about these policies and practices.

## CONCLUSION

The analysis of the Indonesian government's efforts in addressing public data leak cases highlights the critical significance of data protection and cybersecurity in the digital era. While commendable progress has been made, there remains room for improvement. The legal framework for data protection forms a basis for action, but enforcement challenges and resource limitations must be addressed to enhance its effectiveness. Government initiatives, including policies and technological measures, have shown promise in responding to data leaks. Case studies illustrate positive strides, yet the dynamic digital landscape calls for continuous adaptation. In closing, Indonesia's

[15] KOMINFO, P. (2016, October 29). Indonesia sudah miliki aturan soal perlindungan Data Pribadi. Website Resmi Kementerian Komunikasi Dan Informatika RI. https://www.kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlindungan-data-priba di/0/sorotan_media

response to public data leaks necessitates ongoing enhancements in legal frameworks, government initiatives, and public awareness. These efforts are essential for building trust in the digital environment and ensuring national data security. As Indonesia embraces the digital age, the government's commitment to safeguarding public data and human security remains central to a safer digital future. This analysis contributes to the ongoing dialogue on these crucial issues, emphasizing the need for vigilance and adaptability in an ever-evolving digital landscape.

## REFERENCES

BBC News Indonesia. (2023a, July 7). Sebanyak 34 juta data pemegang paspor diduga "bocor"

– "Yang menderita rakyat, pemerintah paling dapat malu." BBC News Indonesia. https://www.bbc.com/indonesia/articles/c9e7e9grjmko

BBC News Indonesia. (2023b, July 18). Peretasan: 337 juta data Dukcapil Kemendagri diduga bocor, pakar siber: "Ini paling parah karena memuat data nama ibu kandung." BBC News Indonesia. https://www.bbc.com/indonesia/articles/c51v25916zlo

BSSN. (n.d.). Tentang BSSN | www.bssn.go.id. Badan Siber Dan Sandi Negara. Retrieved October 31, 2023, from https://www.bssn.go.id/tentang-bssn/

Burhan, F. A. (2021, June 25). Kebocoran Data BPJS Kesehatan Disebut Bikin Rugi Negara Rp 600 Triliun - Teknologi Katadata.co.id. Katadata.co.id. https://katadata.co.id/desysetyowati/digital/60d58c9c4538a/kebocoran-data-bpjs-kesehata n-disebut-bikin-rugi-negara-rp-600-triliun

CyberHub. (n.d.). Badan Siber dan Sandi Negara. Cyberhub.id. Retrieved October 31, 2023, from

https://cyberhub.id/catalog/detail/e9d83191-2d49-46de-99f7-ded9de89d04d#:~:text=TUGAS

Hidayat, A. A. N. (2021, July 29). Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi. Tempo. https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-pr oteksi-dan-regulasi?page_num=3

Hukum Online. (2023). Peraturan Pemerintah Nomor 66 Tahun 2010 - Pusat Data Hukumonline. Hukumonline.com.

https://www.hukumonline.com/pusatdata/detail/lt4cb2becd53181/peraturan-pemerintah-n omor-66-tahun-2010

ITS News. (2022, November 2). Menyikapi Kasus Kebocoran Data Pribadi di Era Digital. ITS News.

https://www.its.ac.id/news/2022/11/02/menyikapi-kasus-kebocoran-data-pribadi-di-era-di gital/

KOMINFO, P. (2016, October 29). Indonesia sudah miliki aturan soal perlindungan Data Pribadi. Website Resmi Kementerian Komunikasi Dan Informatika RI. https://www.kominfo.go.id/content/detail/8621/indonesia-sudah-miliki-aturan-soal-perlin dungan-data-pribadi/0/sorotan_media

Media Indonesia. (2023, July 8). Kebocoran data tidak terbendung. Mediaindonesia.com. https://mediaindonesia.com/editorials/detail_editorials/3061-kebocoran-data-tidak-terben dung

Nabilla, F. (2022, September 2). 11 Daftar Kasus Kebocoran Data di Indonesia, Sebulan Tiga Kali Kejadian! Suara.com. https://www.suara.com/news/2022/09/02/115017/11-daftar-kasus-kebocoran-data-di-indo nesia-sebulan-tiga-kali-kejadian

RSJD Soedjarwadi. (n.d.). Tentang Keterbukaan Informasi Publik.

Ppid.rsjd-Sujarwadi.jatengprov.go.id.

http://ppid.rsjd-sujarwadi.jatengprov.go.id/halaman/detail/tentang-keterbukaan-informasi- publik-#:~:text=Undang%2DUndang%20No.%2014%20tahun

Saskia, C. (2022, September 2). 3 Kasus Kebocoran Data di Indonesia dalam Sebulan, dari PLN, IndiHome, hingga Nomor SIM Card Halaman all (R. Nistanto, Ed.). KOMPAS.com.

https://tekno.kompas.com/read/2022/09/02/10260777/3-kasus-kebocoran-data-di-indones ia-dalam-sebulan-dari-pln-indihome-hingga?page=all

Sidik, S. (2021, September 5). Geger Sertifikat Vaksinasi Jokowi Bocor, Ini Respons Kemenkes. CNBC Indonesia.

https://www.cnbcindonesia.com/tech/20210905121451-37-273736/geger-sertifikat-vaksi nasi-jokowi-bocor-ini-respons-kemenkes

SIPPN. (2023, May 14). Berita SIPPN - Mengenal Undang-Undang ITE. SIPPN - CARIYANLIK.

https://sippn.menpan.go.id/berita/58352/rumah-tahanan-negara-kelas-iib-pelaihari/menge nal-undang-undang-ite