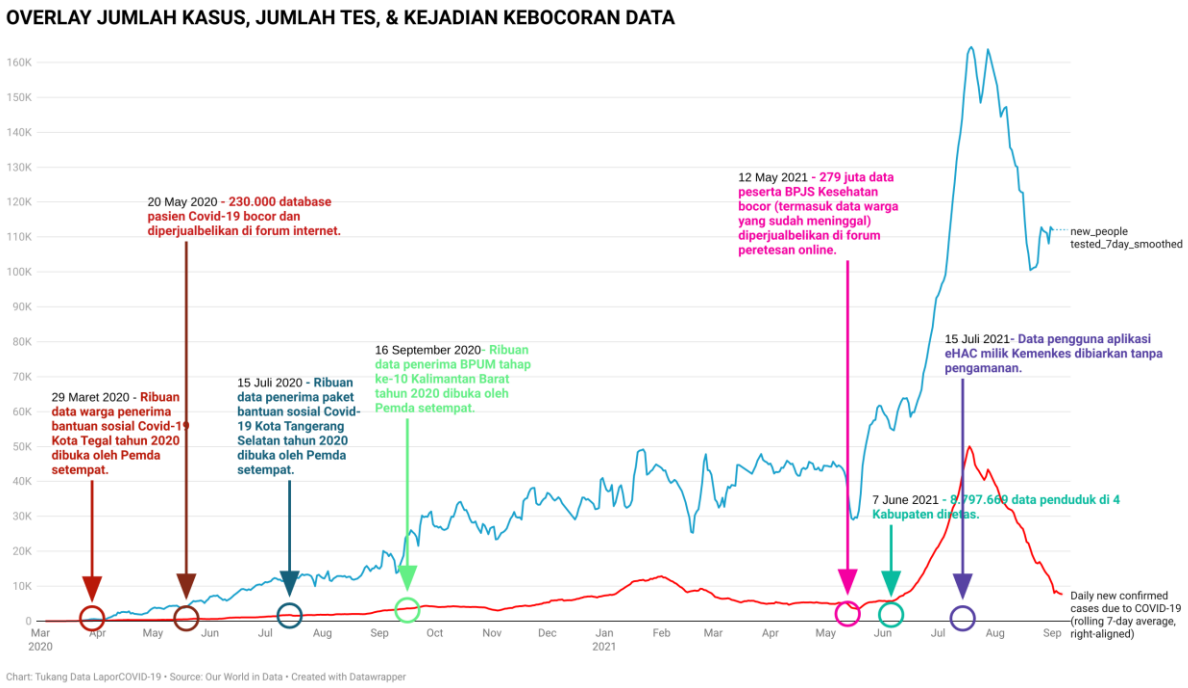
PRESS RELEASE

Failures in Saving Lives and Protecting Citizen's Personal Data

After reports of COVID-19 patients' data being sold, now allegedly, there are data leaks of the data from eHAC and even the President's vaccine certificate. How far our data security goes?



Following points are translation for points inside the graph

- 29 March 2020 > Thousands of data belonging to people who received the 2020 Covid-19 social aid in Tegal City were made available by the local government (Pemda).

- 20 May 2020 > Database that contained 230.000 Covid-19 patients' data was breached and traded on internet forums.
- 15 July 2020 > Thousands of data belonging to people who received the 2020 Covid-19 social aid in Southern Tangerang City were made available by the local government (Pemda).
- 16 September 2020 > 279 million data of Social Health Insurance Administration Body (BPJS) members (including the ones who already passed away) were being traded in hacker's online forums.
- 12 May 2021> Thousands of data belonging to those who received the 10th stage of Micro Business Productive Assistance (BPUM) were opened by local governments in 2020.
- 7 June 2021 > 8.797.669 data from citizens who lived in 4 districts were hacked.
- 15 July 2021> Ministry of Health's application, eHAC had their user's data left without protection.

the Reoccurrence of Events

This is not the first the government has failed to protect its citizen's data. In May 2020, the government was troubled with the leakage of Covid-19 patient data that was being sold on the internet. This time data from the eHAC, an application specialized for testing and tracing for Covid-19, is reported to be leaked. Repeated data leaks have signalled that the government has yet to seriously ensure the security of each citizen's identity and their own digitalized personal data. Although the digitalization process has been done and dusted, there are still incidents that have shown that digital infrastructures are not fully prepared yet.

Patient Covid-19 Data were traded in May 2020.

About 230.000 databases of Covid-19 patients in Indonesia are reportedly known to be traded on internet forums such as Raid Forum in May 2020. Some of those data are personal data and data referred to the patient's condition.

Personal Data of Social Aid Receivers are Openly Accessible

Instead of providing transparency in social aid management, several local governments offered open access to the personal private information of its citizen who received social aid for those who were affected by Covid-19 instead. Such data varied from full name, citizenship registry number (NIK), address, phone number and so on; these data were supposed to be protected and secured. The accessibility of this personal information is undoubtedly susceptible to ill-intents and abuse.

- Thousands of data of those who received Stage 10 of BPIM in West Kalimantan in 2020
- Data of those who received Covid-19 Social Aid in Southern Tangerang City in 2020
- Data of Arrangement for Covid-19 Social Aid distribution of citizens in Tegal City in 2020.

An unsecured server led to 8.797.669 citizens' data being hacked.

This is not the first flaw in the government's electronic system. Ministry of Home Affairs (KEMENDAGRI) acknowledged that four serves belonging to the Office of Population and Registry in Magelang District, Subang District, Kota Bogor, and Bekasi District were hacked. In the aftermath, data belonged to the citizens who lived in those areas to be leaked. This gives a sign that the government's infrastructure for digital security is feeble and prone to hackers.

279 million Data of the Social Health Insurance Administration Body (BPJS) were Leaked

A year after Covid-19 patients' data were leaked, we were shocked by the alleged data leak of 279 million Indonesian citizens. In which the data that were revealed included full name, identity card (KTP), phone numbers, emails, identity registration number (NID), and home address from Social Health Insurance Administration Body (BPJS). Our data were sold in the same forum for worth up to hundreds of millions of rupiah.

Ministry of Health's application, eHAC users' data were left without protection.

Security Research Team from vpnMentor exposed the fragility of the data of those who use the eHAC application. This data leak affected its users and revealed the whole infrastructure surrounding the eHAC application itself, including private notes from hospitals and Indonesian government officials who also used that application. Before this, the citizens were highly encouraged to use the government-owned application, although there were barely any explanations or guarantees for its security.

Contradictory Logic

- Citizen's data are supposed to be protected and secure, are in fact, being left available without security measures.
- Data for testing in each district or city are supposed to be made available to the public for epidemiologic purposes and are not accessible instead.
- Data for vaccines budget management and budget absorption, medical devices and equipment procurement and economic recovery are being covered up instead.
- Data regarding Post Immunization Adverse Events (KIPI) are supposed to be announced, and on the contrary, those data were not conveyed to the public.

Government's Responsibilities

Unfortunately, these data leakages may keep reoccurring as long as the data management is not carefully managed and the data security aspect is overlooked. The government can not be absent regarding the security of their citizen's data. Leaking personal data to the public comes with the consequences of triggering criminal activities that may threaten people's safety and

security. This also includes discrimination toward people with diseases considered taboo by the masses.

Therefore, LaporCovid-19 urges the government to:

1. *Ensure the preparedness of digital infrastructures measurements that are safe and secured.*
2. *Ensure that the personal data of every citizen is safe from any digital crimes.*
3. *Open public access to transparent data surveillance.*
4. *Make it accessible for people to see the data for the Covid-19 emergency budget and budget absorptions from vaccines, medical equipment, and devices, as well as other economic recovery measures.*