

# Indonesia Has Yet to Pass Personal Data Protection Bill

Friday, 28 May 2021 WIB, By: Salma




Indonesia is now investigating the alleged data leak of more than 270 million citizens believed to be from the Health Care and Social Security Agency (BPJS). The news first appeared on social media, saying that the data was on sale on the hacker forum. This major leak has once again reflected the vulnerability of data protection in the country. It still has no law that specifically regulates data protection and guarantees the security of personal information.

UGM Director of Information Systems and Resources Widyawan assessed that the community would be seriously affected if the government could not resolve this matter. As for the government itself, there would be a decline in trust as the public considered the abilities of government institutions to manage and secure digital data and infrastructure remained questionable. Their reputation would be at stake.

“People will regard the institutions that have data leak cases as weak and untrustworthy for failing to safeguard their data. They will no longer trust the institutions and also question the capabilities of other institutions regarding data security,” he said on Wednesday (26/5).

According to Widyawan, the leakage will result in people facing nonconsensual exposure to their private information, such as a residential and email address, date of birth, financial information,



identity card photo, phone number, etc. They also become potential victims of identity theft as these data could target them for illegal marketing and online fraud.

He added that the cybersecurity risk would always exist. Data in electronic form and stored in a computer system connected to the Internet would result in higher cybersecurity risk. Hence the security and protection of data required continuity and priority. Often, institutions neglected this matter and would respond only when an incident occurred.

“The problem lies in awareness and priority. Data leaks in electronic systems can occur due to the exploitation of security holes. Security is not only about technology but also about other elements involved in the system, including the people and processes,” he explained.


Widyawan said that the number of cybersecurity incidents had consistently increased from year to year, both in terms of the number (quantity) and the variety of attacks (quality). Some reports showed the rising occurrence of cases of ransomware and attacks related to IoT/Cyber-physical systems. Thus, he believed the government should handle data crime seriously to reduce the risk of loss. It was also necessary to establish a law on data security, especially considering the massive use of digital technology nowadays in many aspects of life, such as government administration, economy and business, and education, due to the pandemic situation.

“Indonesia still lacks human resources or experts in cybersecurity. We also need improvement in the international security standard application, for example, ISO/IEC 27001, ISO/IEC 15408. Lastly, it would be useful if we can establish a cyber agency that will regularly audit and test the security of electronic service providers, especially those storing massive amounts of data,” said Widyawan.

UGM Public Policy and Management lecturer Professor Wahyudi responded to the BPJS leak by urging authorities to collaborate and thoroughly investigate the case. Supporting the argument from Widyawan earlier, Wahyudi emphasized the need for the Personal Data Protection Bill to pass into law.

“I think this incident shows how important it is to have Personal Data Protection Act. If we do not have the regulatory tools, the government cannot take firm action against those who leak data,” said Wahyudi.

He added that data leakage would result in many potential cybercrimes, adding more cases to the existing doxing, dark web phenomena, cyberbullying, etc. The government had also discovered that more than 11 million data related to citizen identity numbers (called in Indonesia as NIK/*Nomor Induk Kependudukan*) were freely accessible on the Internet.



The lack of digital literacy among Indonesians was also the factor that allowed the crime to happen. Many were unaware that they should be careful in exchanging identity cards or other personal data with friends, colleagues, and everyone in general.

According to him, Facebook was found guilty of leaking its 87 million user data last year. But, the company did not compensate the victims from Indonesia because of the nonexistent Personal Data Protection Act in the country.

“What the Indonesian Ministry of Communication and Information Technology does is only take down the information and those accounts that leak the data or punish the crimes once they occur. There is no comprehensive guarantee of security for the people,” he concluded.

Author: Agung Nugroho

Photo: Kompas.com

## **Related News**