FIX DEFECTS IN LAW

AS the MySejahtera application controversy continues to unfold, the issue of data privacy has once again been thrust into the national limelight.

The concern is not unfounded or overblown. Malaysia's cybersecurity has been floundering with data leak debacles involving private companies and government agencies.

In 2019, a study by British tech company Comparitech ranked Malaysia the fifth worst in terms of data protection out of 47 countries. After two years of de-facto compulsory use of the app, MySejahtera has now emerged as one of the largest databases in the world (as mentioned by the health minister) with 38 million registered users.

Therefore, it has become all the more pertinent to scrutinise the app and the legal safeguards in place with regard to data privacy.

A prominent feature of MySejahtera is contact tracing, which entails the monitoring of users' geolocations.

In addition, personal information such as MyKad number, home address and contact information are recorded, not to mention the sensitive data of our health condition.

Notably, providing false information in the app is an offence under Section 22 of the Prevention and Control of Infectious Diseases Act and Section 233 of the Communications and Multimedia Act.

That said, MySejahtera should be demarcated from other run-of-the-mill apps where no such legal duties are established.

With 38 million users, MySejahtera is now one of the largest databases in the world. PIC BY GENES GULITAH

The Personal Data Protecdon Act 2010 (PDPA) is the main legislation when it comes to data privacy.

Under the PDPA, certain obligations are imposed on data users in processing personal data to safeguard the data subjects (that is, the individual who is the subject of the personal data).

The government should indeed be applauded for demonstrating genuine effort in implementing security and privacy measures on MySejahtera.

For instance, risk assessment tests are conducted periodically, and access of data is only granted to a minimum of seven people. The government also guarantees the public that the data collected will be processed in compliance with the PDPA standards.

However, as lawyers and pundits rightly point out, the guarantee does not hold water as the PDPA, in Section 3(1), explicitly exempts the government from its application.

The exemption means that citizens will be left with no legal remedy if breaches or misuse of data transpire.

Given its enormous value, the MySejahtera database is under imminent threat of cyberattacks and hacking attempts by malicious third parties.

However, the PDPA does not provide compensatory remedy to the victims.

Hapless individuals even can hardly get support from the civil courts as recent case laws indicate that privacy infringement is not an actionable tort in our country.

Simply put, invasion of privacy cannot be a ground to file a legal action. Also, the claimant will be confronted with hardship in proving his losses.

In a CCTV surveillance case, while the court took cognisance of the intrusion of privacy, the claim for monetary damages was turned down as the claimant failed to adduce compelling evidence of his losses.

Apparently, our legal framework on privacy and data protection is deficient in satisfactory redress.

Thus, it is imperative to legally bind the government — being the biggest holder of personal information — to the PDPA to enhance accountability.

Amendment is also desirable to incorporate provisions that allow compensation in cases of breach. The fundamental defects in the law must be fixed whether or not MySejahtera stays.

ONG CHENG HONG
Penang