



PERSONAL DATA PROTECTION AND THE RIGHT TO PRIVACY ON SOCIAL MEDIA

By : Lim Jing Xie (limjingxie@unisel.edu.my & Nabila Ayuni Abdul Malek (nabilaayuni@uitm.edu.my)

The generation today, especially post COVID-19 era, tend to spend most of the time online. The use of social media has spiked tremendously over the years, leading to alarming concerns about data breaches online. The intersection between privacy and cybersecurity leads to many concerns among internet users.

In the year 2020, there have been plans by the Ministry of Communications and Multimedia (KKMM) to discuss possible amendments to the **Personal Data Protection Act 2010 (PDPA)** after identifying gaps and lacuna within the PDPA when compared to personal data legislation with other ASEAN countries.

With this recognition, there have been calls for the attention for the protection, where Judge Cooley calls 'the right to be left alone'. Privacy refers to 'the condition or state of being free from public attention to intrusion into or interference with one's acts or decisions'.

It is one of the values flowing from the principles of human dignity and autonomy. Data privacy is the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information.



Unlike other jurisdictions, in Malaysia, we do not have specific laws or regulations to protect personal data on the internet except the **PDPA**, which deals with personal data and focuses on regulating the processing of 'personal data' in commercial transactions. However, it is impliedly mentioned in **Article 5(1) of the Federal Constitution**, where it was provided that *"No person shall be deprived of his life or personal liberty save in accordance with the law"*.

It was in the case of **Sivarasa Rasiah v Badan Peguam Malaysia & Anor [2010] 3 CLJ 507** where the court held that the term 'personal liberty' in **Article 5 (1) of the Federal Constitution** to include other rights such as the right to privacy.

The court was of the view that the right to privacy is recognized under **Article 5(1) of the Federal Constitution**, but is not enforceable between private individuals, thus dismissing the plaintiff's claim against the defendants, as stated in **Toh See Wei v Teddric Jon Mohr & Anor [2017] 1 LNS 1815**.

This means that an individual could not rely on the alleged breach of right under **Article 5 of the Federal Constitution** to make any claim against the defendants who are private individuals.



On social media, data protection is governed by terms of use agreements and privacy policies on respective social media platforms. The policy is a promise binding between the website and user, bearing the traits of a contract and enforceable at law.

The privacy statement and disclaimers should not be a shield for social media websites whenever an invasion of privacy or data breach happens. For the **PDPA** to be applicable on social media, the data or information concerned must be "personal data".

The **PDPA** defines "personal data" as any information in respect of commercial transactions, which is :

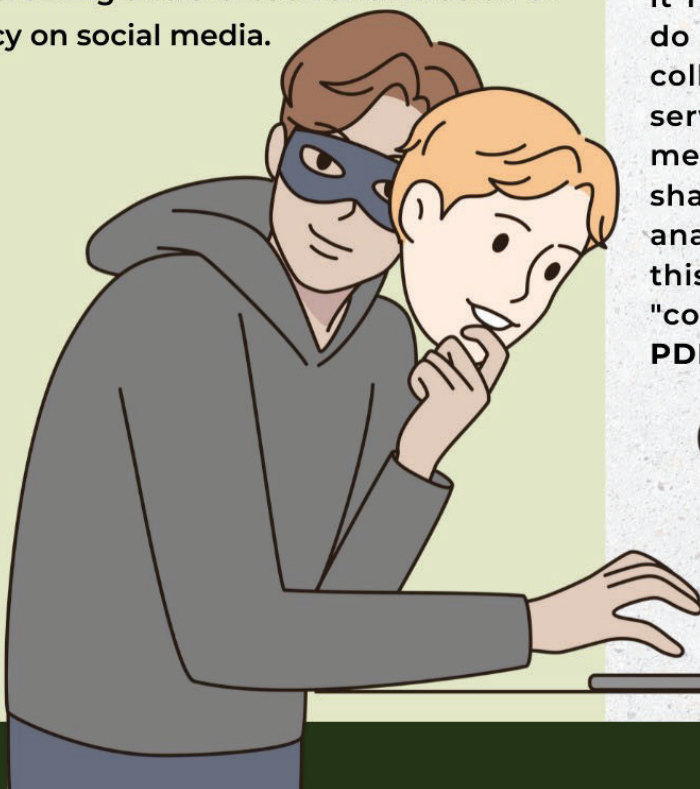
- a) all or part of it shall be processed by means of equipment operating automatically in response to instructions and directions given for that intention;
- b) taken and collected for the purpose that all or part of it would be processed by means of such equipment; or
- c) recorded as a certain part of relevant filing system or with the purpose of including it as a part of a relevant filing system.



Besides, it must be noted that the **PDPA** only applies to commercial transactions. There must be a commercial element in the collection and operation of the personal data concern. Electronic commerce, which is more commonly known as e-commerce, involves the sale and purchase of goods purely in electronic methods. Data and information collected in large volumes make it a vulnerable and appealing target for cybercriminals and online hackers.

This is because Big Data enables the data users to identify patterns and trends which may predict people's dispositions and are able to show the users advertisements and posts which might be of interest.

Assuming that commercial elements were present in the data collection, which the data could reveal human activities known as the big data, it would be a breach of the **PDPA** if the identities of the user could be conclusively determined through the information gathered. This might cause data profiling and a breach and invasion of privacy on social media.



Under the **PDPA**, it clearly states that it regulates information concerned commercial transactions. As applicable in most commercial websites, the **PDPA** requires that there is a privacy policy, where the website could state that they will treat the data collected as they wish. The websites are allowed to share or sell personal information as long as it has been lawfully given, and notice has been given to the data subject.



For example, in Facebook's Data Policy, it has been clearly mentioned that they do provide information that they have collected to vendors on Facebook, their service providers and company. This means that whatever a person posts or share online would be collected and analysed by these business entities, then this information would be considered "commercial transactions" under the **PDPA**.



This means that as long as they comply with the consent to disclose requirement, websites are free to state in their privacy or data policy that they would treat the user's personal data any way they wish, which is like a privilege or immunity from liability when privacy breach happens. The PDPA needs to be complied with as a breach of the PDPA comes with heavy fines and/or imprisonment.

For example, the penalty for breaching the 7 Principles set out under the PDPA is a fine of up to RM300 thousands only and/or imprisonment of up to 2 years. Modern legislation penalising invasion of privacy as a whole is still absent. Thus, it is timely for our lawmakers to come up with our own legislation that provides protection for all types of privacy instead of adopting the common law.

