Asian Journal of Law and Policy
Vol 1 No 1 (July 2021) eISSN: 2785-8979

Digital Tracing and Malaysia's Personal Data Protection Act 2010 amid the COVID-19 Pandemic

Olivia Tan Swee Leng
Multimedia University, Malaysia
oliviatan@mmu.edu.my
ORCID ID: 0000-0002-5628-6883
(Corresponding author)

Rossanne Gale Vergara
Multimedia University, Malaysia
rossanne.gale@gmail.com
ORCID ID: 0000-0003-2024-3977

Shereen Khan
Multimedia University, Malaysia
shereen.khan@mmu.edu.my
ORCID ID: 0000-0002-6665-9145

ABSTRACT

Digital tracing is a proven effective means for the Malaysian government to trace and control the spread of COVID-19. However, the process of tracing and tracking in order to manage the spread of the pandemic have in many ways compromised personal information to third party applications. Malaysia is not the only country that uses digital tracing to manage the spread of the pandemic. Various countries have chosen different methods for digital contact tracing to manage the spread of COVID-19 and some are less respectful of privacy than others. This paper analyses Malaysia's Personal Data Protection Act 2010 (PDPA) and its effectiveness in protecting personal data during the pandemic as Malaysians continue to utilise the contact tracing mobile applications such as MySejahtera and SELangkah. The researchers applied doctrinal research method and analysed the current Malaysian legislation on data protection. It should be noted that the PDPA does not apply in the case of government collection and would not require federal and state agencies to be transparent in their data management.

® (2021) 1 Asian Journal of Law and Policy 47–62
https://doi.org/10.33093/ajlp.2021.3

Published by MMU Press. URL: https://journals.mmupress.com/ajlp

Keywords: COVID-19, Digital tracing, Personal data protection, Privacy

Received: 20 Nov 2020, **Accepted:** 31 Mar 2021, **Published:** 28 Jul 2021

1. Introduction

The novel coronavirus 2019 (COVID-19) first appeared in Wuhan, China in late 2019 and quickly spread to becoming a worldwide pandemic. As of writing this article, the total global COVID-19 cases as of 29 April 2021 is 149,216,984 with 3,144,028 deaths.[1] Countries are still battling the disease, including Malaysia. Malaysia continues to manage the virus with support from the community by following relevant ministries' Standard Operating Procedures (SOPs) to keep the spread of COVID-19 to a minimum. Malaysia targets to inoculate 80% of the population by February 2022. However, even with vaccines currently in the process of being distributed, only 1,369,749 or 2.6% of the population have been vaccinated as of 28 April 2021.[2] That said, the threat of COVID-19 still exists and the community is advised by the government to adhere to the SOPs and not be complacent with their physical hygiene and physical distancing.

The first case of COVID-19 in Malaysia was detected on 25 January 2020 with three Chinese nationals in close contact with an infected person in Singapore.[3] Soon after this, on 4 February 2020 the first Malaysian was confirmed with COVID-19, who had returned from Singapore.[4] Since February 2020, Malaysia has implemented SOPs and the COVID-19 Act 2020. Due to the pandemic's negative impact on both the health and economy of the nation, the government gazetted the COVID-19 Act 2020 on 23 October 2020 to be in effect for two years with the purpose of providing temporary relief to those affected economically by the pandemic.[5] Currently, Malaysia ranks 43rd out of 222 countries in total number of COVID-19 cases. The United States tops the list with the highest number of COVID-19 cases followed by India in second place.[6] Malaysia's COVID-19 total number of confirmed cases as of 29 April 2021 is 404,925 with the total death of 1,492 cases.[7] That said, Malaysia's COVID-19 cases is still at a manageable level compared to the rest of the world. In Bloomberg's COVID-19 Resilience Ranking, Malaysia ranks in 20th place.[8] The COVID-19 Resilience Ranking

1 World Health Organisation, 'WHO Coronavirus Disease (COVID-19) Dashboard' <https://covid19.who.int/>.

2 Josh Holder, 'Tracking Coronavirus Vaccinations Around the World' *New York Times* (12 July 2021) <https://www.nytimes.com/interactive/2021/world/covid-vaccinations-tracker.html >.

3 Asita Elengoe, 'COVID-19 Outbreak in Malaysia' (2020) 11 Osong Public Health Res Perspect <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7258884/> at page 94.

4 ibid.

5 Bernama 'Covid-19 Act to cushion impact of pandemic takes effect tomorrow' *Free Malaysia Today* (Kuala Lumpur, 22 October 2020) <https://www.freemalaysiatoday.com/category/nation/2020/10/22/covid-19-act-to-cushion-impact-of-pandemic-takes-effect-tomorrow/>.

6 Worldometer, 'Covid-19 Coronavirus Pandemic' <https://www.worldometers.info/coronavirus/#countries>.

7 Kementarian Kesihatan Malaysia, 'Situasi Terkini Covid-19 di Malaysia' <http://covid-19.moh.gov.my/terkini>.

8 Jinshan Hong, Rachel Chang and Kevin Varley, 'The Covid Resilience Ranking The Best and Worst Places to Be as Variants Outrace Vaccinations' *Bloomberg* (28 June 2021) <https://www.bloomberg.com/graphics/covid-resilience-ranking/>.

shows where the pandemic is being handled most effectively and currently, Singapore ranks 1st due to their rapid response in rolling out vaccines and bringing down locally transmitted cases to nearly zero.[9] Furthermore, according to the Bloomberg Resilience Ranking findings, 'success in containing COVID-19 with the least disruption appears to rely less on being able to order people into submission and more on governments fostering a high degree of trust and societal compliance.'[10] Countries in the top ten of the rankings have demonstrated this, including shutting their borders, hand sanitizing, wearing face masks and investment in public health infrastructure such as systems for contact tracing.

1.1 Malaysia COVID-19 Outbreak Response

At the onset of the COVID-19 outbreak, Malaysia's Prime Minister Muhyiddin Yassin announced the first phase of Movement Control Order (MCO) effective from 18 March 2020 to 31 March 2020, which was extended three times. The first extension was until 14 April 2020. The second until 28 April 2020 and a third time until 12 May 2020. During the MCO, borders were closed to all incoming foreigners and Malaysians' travel was also restricted. Essential services were open for limited operation such as supermarkets and food delivery.

On 4 May 2020, lockdown restrictions were eased during the Conditional Movement Control Order (CMCO). During the CMCO, the goal was to re-open the economy by setting SOPs for businesses and ensuring social distancing. It was at this time the government of Malaysia developed MyTrace and MySejahtera apps to curb the spread of the disease. The development of the apps are with the cooperation of the National Security Council (NSC), Ministry of Health, Malaysian Communications and Multimedia Commission (MCMC) and other agencies to manage any outbreak.[11] The MySejahtera mobile app was introduced by the Ministry of Health in collaboration with the National Security Council (NSC) and Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), to assist the government in monitoring, managing and mitigating the COVID-19 outbreak by collecting data from citizens through health self-assessments.[12] In addition to these is Gerak Malaysia, associated with Royal Malaysia Police (PDRM) and developed by MCMC to deliver a digital ID that verifies motivations for travel. Initially, the application was also used by the PDRM to manage interstate travel permits.

The next phase in MCOs was the Recovery MCO (RMCO) which was effective from 10 June 2020 to 31 August 2020, with more lenient restrictions. Under this phase, interstate travel was permitted, except for areas placed under Enhanced MCO (EMCO), which are locations with large cases of COVID-19 under strict lockdown.[13] Residents in locations under EMCO for 14 days are restricted to their homes, business are required to shut down, all

[9] ibid.

[10] ibid.

[11] MySejahtera <https://mysejahtera.malaysia.gov.my/intro_en/>.

[12] Qishin Tariq, 'Govt launches pilot project to monitor spread of Covid-19 pandemic via app' *The Star* (6 April 2020) <https://www.thestar.com.my/tech/tech-news/2020/04/06/govt-launches-app-to-monitor-spread-of-covid-19-pandemic>.

roads are blocked and a medical base established in the area to conduct COVID-19 testing. Moreover, food and supplies are provided to the residents during the 14-day quarantine.

During the RMCO, the Prime Minister permitted domestic tourism and travel. More restrictions were relaxed to allow the public to carry out their daily activities in compliance with SOPs. The SOPs are accessible to the public via the Malaysia's National Security Council website.[14] Other than activities allowed or prohibited and the maximum capacity of personnel allowed, the SOPs also emphasised digital tracing. This means that applications such as MySejahtera and SELangkah (another digital tracing app for the state of Selangor and integrated with MySejahtera) with QR scan code are to be placed on all public buildings and facilities entrances. Vendors must comply with the SOPs or face paying a fine of RM50,000. Although, vendors and consumers alike may not be aware of the risk that personal data collected may be tampered with and compromised. That said, companies must still comply with the Personal Data Protection Act 2010 and government SOPs.[15]

2. Personal Data Protection Act 2010

The Personal Data Protection Act 2010 (PDPA) is an Act that regulates the processing of personal data in regards to commercial transactions. It was gazetted in June 2010. The penalty for non-compliance is between RM100 thousand to RM500 thousand and or between 1 to 3 years imprisonment. According to the Department of Personal data Protection, 'the main objective of this law is to regulate the processing of personal data in commercial transactions by data users and protect the interests of data subjects.'[16]

Section 2(2) of the PDPA indicates that not all data obtained are fully protected. The PDPA is enforced by the Commissioner of the Department of Personal Data Protection (the commissioner), it is based on a set of data protection principles akin to that found in the Data Protection Directive 95/46/EC of the European Union (EU) and, for this reason, the PDPA is often described as a European-style privacy law. An important limitation to the PDPA is that it does not apply to the federal and state governments.

Having said that, the processing of information by a credit reporting agency is also exempted from the PDPA. In the past, credit reporting agencies did not fall under the purview of any regulatory authority in Malaysia, drawing heavy criticism for inaccurate

[13] Adib Povera, 'CMCO to end, Replaced with RMCO until Aug 31' *New Straits Times* (Kuala Lumpur, 7 June 2020) <https://www.nst.com.my/news/nation/2020/06/598700/cmco-end%C2%A0replaced-rmco-until-aug-31>.

[14] National Security Council (MKN), 'SOP PKP Recovery' <https://www.mkn.gov.my/web/ms/sop-pkp-pemulihan/>.

[15] Department of Personal Data Protection, 'Operating Procedures for the Collection, Processing and Storage of Personal Data by Business Premises during the Conditional Movement Control Order'<https://www.pdp.gov.my/jpdpv2/pengumuman/tatacara-pengendalian-bagi-aktiviti-pengumpulan-pemprosesan-dan-penyimpanan-data-peribadi-oleh-premis-perniagaan-semasa-perintah-kawalan-pergerakan-bersyarat-pkpb/>.

[16] Department of Data Protection, Malaysia <https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/background/?lang=en>.

credit information reporting. The Credit Reporting Agencies Act 2010 (Act 710), which came into force on 15 January 2014, now provides for the registration of persons carrying on credit reporting businesses under the regulatory oversight of the Registrar Office of Credit Reporting Agencies, a division under the Ministry of Finance, which is charged with developing a regulated and structured credit information sharing industry.

2.1 Offences and Punishment

The below is a list of offences and penalties under PDPA (Act 709) and subsidiary legislation.[17]

LIST OF OFFENCES AND PENALTIES UNDER THE PERSONAL DATA PROTECTION ACT 2010 (ACT 709) AND SUBSIDIARY LEGISLATION

No.	SECTIONS/REGULATIONS	OFFENCES	PUNISHMENTS
PERSONAL DATA PROTECTION ACT 2010			
1.	Subsection 5(2) Principles of personal Data protection	Processing of personal data that does not comply with personal Data protection principles	A fine not exceeding RM 300,000 or to imprisonment for a term not exceeding 2 years or to a second
2.	Subsection 16(4) Registration certificate	To process personal data without a certificate of registration issued under 16 (1) (a)	A fine not exceeding RM 500,000 or to imprisonment for a term not exceeding 3 years or to a second
3.	Subsection 18 (4) Revocation of registration	Processing personal data after registration is canceled	A fine not exceeding RM 500,000 or to imprisonment for a term not exceeding 3 years or to a second
4.	Subsection 19 (2) Submission of Certificate of Registration	Failure to submit certificate of registration to the Commissioner after registration certificate	A fine not exceeding RM 200,000 or to imprisonment for a term not exceeding 2 years
5.	Section 29 Non-compliance practice	Does not comply with the provisions of the practice applicable to users of the data	A fine not exceeding RM 100,000 or to imprisonment for a term not exceeding 1 year or to a second

[17] Personal Data Protection Act 2010 (Act 709).

6.	Section 37 (4) Notification of refusal to comply with data correction request	Do not comply with the matters claimed under subsection 37 (2) of the ACT	A fine not exceeding RM 100,000 or to imprisonment for a term not exceeding 1 year or both
7.	Subsection 38 (4) Withdrawal of consent to process private data	Do not discontinue the processing of personal data after receiving notice of withdrawing consent from data subject	A fine not exceeding RM 100,000 or to imprisonment for a term not exceeding 1 year or both
8.	Subsection 40 (3) Processing of sensitive personal data	Processing of sensitive personal data that does not comply with subsection 40 (1) of the Act	A fine not exceeding RM 200,000 or to imprisonment for a term not exceeding 2 years or both
9.	Subsection 42 (6) To prevent processing which may result in damage or distress	Do not comply with the provisions of the Commissioner under subsection 42 (5)	A fine not exceeding RM 200,000 or to imprisonment for a term not exceeding 2 years or both
10.	Subsection 43 (4) Right to prevent processing for direct marketing purposes	Do not comply with the provisions of the Commissioner under subsection 43 (3)	A fine not exceeding RM 200,000 or to imprisonment for a term not exceeding 2 years or both
11.	Subsection 108 (8) Enforcement notices	Did not comply with an enforcement notice	A fine not exceeding RM 200,000 or to imprisonment for a term not exceeding 2 years or to both
12.	Subsection 113 (7) Search and seizure with warrant	A person who, without lawful authority, breaks, tampers with or damages the seal referred to in subsection (6) or removes any computer, book, account, computerized data or other document, signboard, card, letter, pamphlet, leaflet, notice, equipment, instrument or article under seal or attempts to do so commits an offence	A fine not exceeding RM 50,000 or to imprisonment for a term not exceeding 6 months or to both
13	Section 120 Obstruction to search	Any person who refuses to grant access to an Authorised Officer B) to secure, prevent, melt, or delay any authorised	Imprisonment for a term not exceeding 2 years or a fine not exceeding RM 10,000 or both

		Officer C) refuses to give information in respect of an offence or suspected offence to an authorized officer	
14	Subsection 129 (5) Personal data transfer to place outside Malaysia	Do not comply with the matters set out in subsection 129 (1)-Transferring personal data about a data subject to a place outside Malaysia, other than a place determined by the Minister, upon recommendation by the Commissioner, by notification published in the Gazette	A fine not exceeding RM 300,000 or to imprisonment for a term not exceeding 2 years or both
15	Subsection 130 (7) Unlawful Collection personal data etc	Commits an offence As set out in section 130	Fine not exceeding RM 500,000 or imprisoned for a period not exceeding 3 years or both.
16	Subsection 131 (1) and (2) Abetment and Attempt punishable as offences	131 (1) A person who abets the commission of or who attempts to commit any offence under this Act shall be guilty of that offence and shall, on conviction, be liable to the punishment provided for that offence 131 (2) A person who does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall, on conviction, be liable to the punishment provided for the offence: Provided that any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence.	Provided that any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence. Provided that any term of imprisonment imposed shall not exceed one-half of the maximum term provided for the offence.
17	141 (2)	141(1) (a) and (b)	Fine not exceeding RM

	Confidentiality obligations		100,000 or imprisoned for a period not exceeding 1 year or both
PERSONAL DATA PROTECTION REGULATIONS 2012			
18	Regulation 12	Violating sub-regulation 3 (1), 6, 7 and 8	Penalty is not exceeding RM 250,000 or imprisoned for a term not more than 2 years or both

The PDPA punishments are too lenient and the list of punishments are not exhaustive. PDPA is currently being reviewed by the Ministry of Communications and Multimedia to streamline international requirements on personal data protection including key takeaways of the European Union's General Data Protection Regulation 2018 (GDPR)[18]. A further point to note is that the PDPA only regulates personal data in the context of commercial transactions. As such, there is also some ambiguity as to whether a nominal user of social media (i.e., for recreational and social use) would enjoy the protection offered by the PDPA. The Act is silent as to the data protection aspect of human resource data obtained from the management from employees. There are some online applications running a portal that indirectly commercialises their products, PDPA ought to address this method of transaction explicitly.

In addition to the above, most of the obligations under the PDPA apply to a 'data user' as defined under section 2 of PDPA ('a person who either alone or jointly in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor'). Hence, a 'data processor' who processes personal data solely on behalf of a data user is not bound directly by the provisions of the PDPA.

Section 45(2)(c) of PDPA stipulates that the information must relate directly or indirectly to a data subject who is identifiable from the information or other information in the possession of the data user. A central issue for the application of the PDPA is the extent to which information can be linked to a particular person. If data elements used to identify the individual are removed, the remaining data will become non-personal information, and the PDPA will not apply.

3. Cybersecurity and Data Breach

Due to the likelihood that the majority of internet users store or use their personal data online, it is highly likely that their personal data are also at risk to cybersecurity threats and data breaches. Moreover, public and private sector companies have largely migrated to

[18] EU General Data Protection Regulation (2018), OJ L 127.

cloud services to store data, which also includes private data. That said, the biggest mobile data breach in Malaysia occurred in October 2017, whereby 46.2 million mobile subscribers' data was stolen and leaked to the dark web.[19] In January 2019, it was reported that more than one million Universiti Teknologi Mara (UiTM) students' personal data (names, MyKad number, home and email addresses, mobile numbers, etc.) enrolled between 2000 and 2018 was leaked online between February and March 2018.[20] However, 'the screenshot published in a blog was in a format that is not used by any of UiTM's systems and showed the information was processed by hackers.'[21] More recently, India-based cybersecurity start-up Technisanct reported that hundreds of thousands of credit card details from Southeast Asian countries have been leaked online.[22]

Having said that, the Malaysia Computer Emergency Response Team (MyCERT) provides assistance in handling incidents such as intrusion, identity theft, malware infection, cyber harassment and other computer security-related incidents.[23] They operate the Cyber999 computer security incident handling and response help centre as well as the Cybersecurity Malaysia Malware Research Centre.[24] The MyCERT Incident Statistics indicates that in 2020 there were a total of 10,790 incidents reported, with 'fraud' ranked the highest reported incident (7,593 incidents) or taking up 70% of the reported incidents and the highest spike in incidents reported in the month April (1,488 incidents).[25] This shows that even though Malaysia has agencies to report cybercrime incidents to, the incidents still occur. As long as businesses are conducted online, or online services are used i.e. purchasing products on online platforms (Amazon, Lazada, Shopee), which require entering personal data, the personal data entered and stored are at risk of being hacked. Therefore, a secure connection and good cyber hygiene are necessary in protecting personal data. Cyber hygiene is a practice that users do to maintain the system health and improve online security. This is clearly a practice that needs improvement for all internet users, not just in Malaysia. According to the Internet Users Survey 2020 by the Malaysian Communications and Multimedia Commission, 'smartphones are the most popular device to access the internet, reaching a usage level of 98.7% in 2020.'[26] This is how the majority of Malaysians connect to the internet and conduct their daily lives, such as communicating and social networking.

[19] Cristina Lago, 'The biggest data breaches in Southeast Asia' *CSO Asean* (18 January 2020) <https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html>.

[20] Veena Babulal and Beatruce Nita Jay, 'UiTM to probe claims of data breach' *New Straits Times* (Kuala Lumpur, 25 January 2019) <https://www.nst.com.my/news/nation/2019/01/454429/uitm-probe-claims-data-breach>.

[21] ibid.

[22] 'Data breach involving Malaysia, Singapore credit card details' *The Star* (Hong Kong, 07 March 2020) <https://www.thestar.com.my/business/business-news/2020/03/07/data-breach-involving-malaysia-spore-credit-card-details>.

[23] MyCERT, 'About us' <https://www.mycert.org.my/portal/full?id=d8032294-04b2-4ba0-9e46-62c898bb4983>.

[24] ibid.

[25] MyCERT, 'Incident Statistics' <https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=4997a4a8-b05d-47d4-8e51-3c5b063a67fd>.

[26] MCMC 'Internet Users Survey 2020' <https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS-2020-Report.pdf>.

However, this also shows that due to this increased use of smartphones, it is also necessary for Malaysians to practise good cyber hygiene while using their smartphones to protect their personal data.

3.1 Digital Innovation

One of the challenges for data protection is the digital innovation aspect. The vast majority of companies store their data through cloud computing to save costs such as running electricity for physically storing a system in the company. Businesses and governments are shifting to the cloud to store data pertinent to work, which also includes personal data. However, some organisations remain resistant to the cloud's considerable attractions due to lingering concerns about data security in cloud computing. The main security risks of cloud computing are compliance violations, identity theft, malware infections data breaches, diminished customer trust and potential revenue loss.[27]

Generally, the regulatory framework has not designed specific rules outside the application of the seven principles in the PDPA to deal with data privacy issues created by cookies, online tracking, cloud computing, the internet of things or big data, although the government of Malaysia encourages digital innovation, especially during the pandemic era i.e. COVID-19 as a means or tool of communication, transaction, social media and tracing tool to control the spread of the pandemic.

The standard operating procedures are quite challenging to manage data protection, especially when the applications developed are from third parties and not government or government agencies related.

3.2 Cases on Breach of Privacy

In Malaysia, 'invasion of privacy' is not an actionable tort. This principle is based on court decisions in *Ultra Dimension Sdn Bhd v Kook Wei Kuan*[28] and *Dr. Bernadine Malini Martin v MPH Magazine Sdn Bhd & Ors.*[29]

The Court of Appeal in *Maslinda bt Ishak v Mohd Tahir bin Osman & Ors*[30] seems to have implicitly recognised the tort of privacy in Malaysia by allowing *Maslinda*'s claim and holding the respondents liable for violating privacy.[31] Subsequently, *Lee Ewe Poh v Dr Lim Teik Man & Anor*[32] became the first Malaysian case that recognised invasion of privacy as an actionable tort. The Court departed from English law by taking a different approach. It was

[27] Akamai, 'What are the Security Risks of Cloud Computing?' <https://www.akamai.com/us/en/resources/data-security-in-cloud-computing.jsp>.

[28] Universal Declaration of Human Rights, Art 12.

[29] *Dr Bernadine Malini Martin v MPH Magazine Sdn Bhd & Ors* [2004] 5 Current Law Journal 285.

[30] *Maslinda bt Ishak v Mohd Tahir bin Osman & Ors* [2009] 6 Malayan Law Journal 826.

[31] *Sivarasa Rasiah v Badan Peguam Malaysia & Anor* [2010] 2 Malayan Law Journal 333, at para 6.

[32] *Lee Ewe Poh v Dr Lim Teik Man & Anor* [2011] 1 Malayan Law Journal 835.

held that the defendant, by taking pictures of the plaintiff's private parts in a medical surgery without her consent, invaded the plaintiff's privacy.[33] These decisions showed shifting approaches on the tort of privacy in Malaysia, which are undoubtedly befitting in recognition of the right of privacy under Malaysian law. At this juncture, it can be seen that the Malaysian judiciary is taking the stand to recognise "privacy" protection.

Sadly, the court took a sudden turn in *Mohamad Izaham bin Mohamed Yatim v Norina Binti Zainol Abidin,*[34] where it was held that the learned judge in *Lee Ewe Poh*'s case had erred by relying on the decision of *Maslinda Ishak* because the issue of invasion of privacy was never challenged in that case. Additionally, the court struck down the plaintiff's case and held that invasion of privacy is not an actionable tort in our country.

The law of privacy in Malaysia is still grounded from common law and privacy protection from the judiciary is mainly on moral and chastity of women. Privacy rights are still mainly governed by Malaysia's Federal Constitution.

4. COVID-19 Pandemic and Data Protection

Since the position of the right to privacy in the Federal Constitution remains stagnant, Malaysia needs a wider interpretation on privacy protection amid the COVID-19 situation.

As tracking and surveillance technology appears to be an essential part in managing the pandemic, the prevalent questions by the public shall be the security of the data obtained from this tracking and surveillance technology. Referring to the earlier paragraphs, it is quite clear that the current PDPA is undergoing revision for better data protection coverage and the judicial stand for privacy is still very much depending on the Federal Constitution interpretation.

Private sector ecosystem provides a layer of innovation and also adds grey areas to the regulations. The parties handling data of citizens would have to comply with the government's regulations and it can be challenging when data breaches are neither disclosed nor reported. In addition to this, the ever-changing digital environment has not only complicated terminology, but it is also likely to introduce loopholes in the regulations. For instance, apart from personal data such as basic identity, contact details, location information and travel history and information of close contacts, health status, body temperature measurement and medical condition, which are sensitive personal data are also being processed. Sensitive personal data is subject to more stringent and additional safeguards under the PDPA. Moreover, in privacy and security concerns, it is questionable if such surveillance tools are effective enough to combat COVID-19 linked issues. For instance, when the body temperature readings are taken by infrared thermometer, some devices are faulty and inaccurate, hence data collected may not be reliable and valid. On the MySejahatera tracing application, some consumers are not keen on keying in their

[33] *Maslinda bt Ishak v Mohd Tahir bin Osman & Ors* [2009] 6 Malayan Law Journal 826, at para 8.

[34] *Mohamad Izaham bin Mohamed Yatim v Norina Binti Zainol Abidin* [2015] 7 Current Law Journal 805.

information while some give false data, even though a fine is issued for those flouting MCO SOPs.

The SOPs are established and ensures health and data security if the community follows them as intended. However, in a weak SOP and weak enforcement, data collection can be compromised and abused by hackers. There are yet to be any specific guidelines from the Malaysian Personal Data Protection Commissioner on the lawful processing of personal data on the COVID-19 pandemic. Businesses are to adhere to the PDPA 2010. The Ministry of Health has issued guidelines to event organizers to keep a record of the contact details of all participants for at least one month from the date of completion of the events. They are required to assist the Ministry of Health in carrying out contact tracing and place close contacts under home surveillance where participants are infected.

It is a violation under section 22I of the Prevention and Control of Infectious Diseases Act 1988 (PCIDA) to not furnish information required for the purposes of the PCIDA or any regulations made thereunder; Regulation 6 of the Prevention and Control of Infectious Diseases (Measures Within the Infected Local Areas) Regulations 2020 and Regulation 9 of the Prevention and Control of Infectious Diseases (Measures Within the Infected Local Areas) Regulations (No. 2) 2020 (collectively, PCIDR), which mandate compliance with the request of an authorized officer for any information relating to prevention and control of the infectious disease. Accordingly, when there is a request by the health authorities or the officers for personal data of an employee or a visitor for investigation or contact tracing purpose, employers are bound by the legal obligations under the PCIDA. This ultimately means that employers are allowed to collect and subsequently disclose the information to the health authorities and the officers without consent to comply with the legal obligations under the PCIDA and PCIDR.[35]

Furthermore, the PCIDA and PCIDR allow the collection of sensitive personal data subsequent disclosure to health authorities and officers without explicit consent.[36] Although the PCIDA and PCIDR allow the collection and disclosure of personal data to prevent and control the spread of a pandemic, employers must still 'ensure that the existing notices to their employees, contractors and visitors are sufficiently wide to cover the type of personal data and sensitive personal data being processed, the purpose and the class of third party to whom it may be disclosed, without which a supplementary notice will be required.'[37]

In the event that the purpose is omitted in the relevant notices, disclosing the information to the health authorities without consent is still possible based on the exception that the disclosure is authorized by the PCIDA and the PCIDR.[38] Moreover, notice to the individuals may be exempted for the collection and disclosure of their information to the health authorities on the basis that the information is being processed for research purposes

[35] Personal Data Protection Act 2012, s 6(2)(c).

[36] Personal Data Protection Act 2012, s 40(1)(b)(i), 40(1)(b)(ii) and s 40(1)(b)(iii).

[37] Personal Data Protection Act 2012, s 7.

[38] Personal Data Protection Act 2012, s 39(b)(ii).

to identify, test and isolate the affected persons in order to prevent the spread of the virus and not for any other purpose, provided the identity of the affected persons are not disclosed.[39]

5. Retention of Personal Data

Personal data may be retained for as long as it is necessary for the containment of COVID-19 and should be permanently deleted or removed when the COVID-19 outbreak is over.[40] Despite the challenging nature of this pandemic, organisations should be cognizant of their responsibilities under the PDPA 2010 when processing the personal data of individuals. As the number of infected individuals in the country continues to grow, the same amount of personal data, including sensitive personal data, are being processed and transmitted between organisations and the health authorities. In this regard, the demand to strengthen data security measures and the exercise of data minimization is necessary. The penalty for organisations that improperly handle or unlawfully use the personal data collected is a fine and a term of imprisonment for breaching the PDPA 2010.

In relation to personal data and digital tracing, global demand for data security continues to grow with emerging technologies being deployed across the world in a race against time to trace and track close contacts of infected persons. Contact tracing via mobile apps and electronic tracking devices across Asian countries such as China[41], South Korea[42], Hong Kong[43], Taiwan[44] and Singapore[45], facilitates instant contact tracing, which enables enforcement of quarantine and alerting users of possible exposure. Thus, western countries such as the United States of America, United Kingdom[46], Ireland[47] and Germany[48] have followed Asian countries in their experience with contact tracing by announcing their

[39] Personal Data Protection Act 2012, s 45(2)(c).

[40] Personal Data Protection Act 2012, s 10.

[41] 'China launches coronavirus "close contact detector" app' *BBC News* (11 February 2020) <https://www.bbc.com/news/technology-51439401>.

[42] Ivan Watson and Sophie Jeong, 'Coronavirus mobile apps are surging in popularity in South Korea' *CNN Business* (Seoul, 28 February 2020) <https://edition.cnn.com/2020/02/28/tech/korea-coronavirus-tracking-apps/index.html.>.

[43] Zoe Low, 'Covid-19: inbound travellers from Europe, US to be issued Bluetooth quarantine wristbands at Hong Kong airport' *South China Morning Post* (Hong Kong, 25 March 2020) <https://www.scmp.com/news/hong-kong/society/article/3076994/coronavirus-inbound-travellers-europe-united-states-will-be>.

[44] Yimou Lee, 'Covid-19: Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring' *Reuters* (Taipei, 20 March 2020) <https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK>.

[45] Fathin Ungku, 'Singapore launches contact tracing mobile app to track coronavirus infections' *Reuters* (Singapore, 20 March 2020) <https://www.reuters.com/article/us-health-coronavirus-singapore-technolo/singapore-launches-contact-tracing-mobile-app-to-track-coronavirus-infections-idUSKBN2171ZQ>.

[46] Hannah Devlin, 'NHS developing app to trace close contacts of coronavirus carriers' *The Guardian* (London, 31 March 2020) <https://www.theguardian.com/uk-news/2020/mar/31/nhs-developing-app-to-trace-close-contacts-of-coronavirus-carriers>.

initiatives to develop similar contact tracing apps. In Europe for instance, the pan-European mobile tracking app is compliant with the European Union's data protection laws and has being explored to facilitate contact tracing within its countries and across borders.[49]

While digital contact tracing has showen promise in quicker contact tracing to assist in identifying infected persons and premises, appropriate security measures must be incorporated to protect the personal data of users against cybersecurity threats. For instance, the technical drawback for Bluetooth has the potential to turn up a large number of false positives due to the inaccuracies in the distance recorded. Bluetooth does not triangulate the location. Hence, an approximate distance is recorded. In order for a Bluetooth-based contact tracing application to be effective, a substantial number of people will need to install the app. Although signing in the MySejahtera app is required prior to entering a business premise, the SOPs still allow those without MySejahtera to record their details in a physical book maintained by the business. Thus, while digital surveillance allows faster and wider coverage to contact tracing, unless it is mandatory for the whole population to download the contact tracing app, the process of effectively and efficiently identifying affected persons and premises will be delayed. Hence, it is necessary to go to digital tracing to speed up the contact tracing process. However, at the same time, the app and the collection/storage of the data must be secure in order to protect the personal data of the population.

6. Conclusion

Malaysians want a safe environment in terms of health security and data security and the challenge for the existing government is to study the best practices from other jurisdictions and introduce the best model law to Malaysia for data protection.

The best practice study should reflect the EU-enacted General Data Protection Regulation (GDPR) where individual privacy rights are better defined in the Regulation. In a 2021 research by the DLA Piper, the GDPR data breach survey stated that there was a '19% increase in the number of breach notifications, from 287 to 331 breach notifications per day, in the past year, continuing the trend of double-digit growth for breach notifications.'[50]

---

[47] Reuters Staff, 'Ireland to roll out voluntary phone tracker app to tackle coronavirus' *Reuters* (Dublin, 29 March 2020) <https://www.reuters.com/article/health-coronavirus-ireland/ireland-to-roll-out-voluntary-phone-tracker-app-to-tackle-coronavirus-idUSL8N2BM0GR>.

[48] Douglas Busvine, 'Germany aims to launch Singapore-style coronavirus app in weeks' *Reuters* (Berlin, 30 March 2020) <https://www.reuters.com/article/us-health-coronavirus-germany-tech/germany-aims-to-launch-singapore-style-coronavirus-app-in-weeks-idUSKBN21H26Z>.

[49] Foo Yun Chee, 'EU privacy watchdog calls for pan-European mobile app for virus tracking' *Reuters* (Brussels, 6 April 2020) <https://www.reuters.com/article/us-health-coronavirus-tech-privacy/eu-privacy-watchdog-calls-for-pan-european-mobile-app-for-virus-tracking-idUSKBN21O1KJ>.

[50] Ross McKean, Ewa Kurowska-Tober and Heidi Waem 'DLA Piper GDPR fines and data breach survey: January 2021' <https://www.dlapiper.com/en/us/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/>.

Although the GDPR is currently one of the more comprehensive data protection laws out there, it is not without criticism. Therefore, if Malaysia decides to walk the same path as GDPR, lessons learned and improvements will need to be incorporated into Malaysia's data protection law. As mentioned above, there were increased activities by data protection authorities in 2020, but the GDPR fines did not match with the data breach numbers. More specifically, the tech giant Twitter was fined, which many found to be significantly less than expected, and the punishment only took place almost two years after the breach disclosure, which led to strong criticism of GDPR's effectiveness.

The highest individual GDPR fines in the EU were issued by France, Germany, and Italy. In the last year's report, Austria was one of the leaders in the biggest individual GDPR fine issued so far. However, the order was changed after the overturning of the 18 million euro GDPR fine at the end of 2020.[51] Germany was fined €9.55 million for 1&1 Telecom and €14.5 million to Deutsche Wohnen SE), while France still holds the first position of highest fined issued with the €50 million Google fine.

The Malaysia PDPA does not apply in the case of government collection and would not obligate federal and state agencies to be transparent in their data management. This will be rectified by public consultation paper on PDPA and had made its round in February 2020.[52]

During Malaysia's movement control orders, whether it be MCO, CMCO or EMCO, operations were limited to essential services only. That said, as essential services including food outlets are frequently being visited by people, there is now an increased risk of breach of data security as mentioned in the previous paragraphs. Purchasing food and services online has increased due to the pandemic, and without proper cyber hygiene and a secure platform, this exposes the customers' data amounts to a data breach. That said, cyber threats continue to rise as opportunists take advantage of the situation. Public and private sector businesses handling personal data need to ensure that sufficient security measures and adequate safeguards are in place to protect personal data from cyber-criminals. For data collected through electronic means, personnel who are given authority to access the personal data must be adequately trained and reminded to follow internal protocols on disclosure. As for cyber hygiene, anti-virus and anti-malware software should be installed and updated and a backup/recovery system must be in place. Organisations should review existing privacy notices and wherever necessary, revise these to ensure that they cover any new data fields being collected in light of the COVID-19 pandemic, and the purposes for processing may need to be updated as well.

Lastly, although there is no definitive proof that the digital tracing itself is the means for success in tracking and curbing the spread of COVID-19, technology has played a pertinent and pivotal role in this pandemic and will likely continue to do so in many aspects of digital

[51] '5 biggest GDPR fines so far' Data Privacy Manager <https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/>.

[52] Department of Personal Data Protection, 'Public Consulation Paper No. 01/2020' <https://www.pdp.gov.my/jpdpv2/assets/2020/02/Public-Consultation-Paper-on-Review-of-Act-709_V4.pdf>.

and social life. Hence, the government must ensure it is being used appropriately without endangering the people to security and privacy abuse.

Acknowledgement

The authors acknowledge the assistance of the Multimedia University in the preparation of this article.

Funding Information

The authors received no funding from any party for the research and publication of this article.