

**COVID-19 PANDEMIC POLICIES IN MALAYSIA AND
THE ISSUES OF PRIVACY AND DATA PROTECTION**

BY

ALAA SAKKA

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

2023

COVID-19 PANDEMIC POLICIES IN MALAYSIA AND
THE ISSUES OF PRIVACY AND DATA PROTECTION

BY

ALAA SAKKA

A dissertation submitted in fulfilment of the requirement for
the degree of Master of Comparative Laws

Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia

APRIL 2023

ABSTRACT

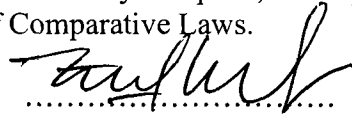
COVID-19 pandemic has drastically altered civilization, and it will require a long-term historical perspective to fully comprehend its effects. It is obvious that current advances, whether or not they concern privacy and tech, will have an impact on the way society develops in the future. The data-driven initiatives created in response to COVID-19 have already changed how society engages with technology and privacy ideas, from widespread public health testing to individual communication tools. Personal data is classified as one of the most valuable and desirable commodities, especially in the era of digitization and the emergence of modern technologies. In view of the COVID-19 pandemic crisis and policy measures taken in Malaysia, there is need to protect individual's privacy and personal data. This research aims to study and analyse the privacy and data protection implications of COVID-19 pandemic laws and policies in Malaysia between 2020 and 2022. The research relies on the analytical approach to study relevant legislation. Descriptive assessment method was used to assess the current laws and policies on the protection of personal data. The qualitative and doctrinal method was used in surveying and analysing the literature. The study noted that although there are laws on privacy and personal data protection in Malaysia, there is still room to improve the laws to address loopholes and challenges that emerged during COVID-19 pandemic. Therefore, the research proposes some suggestions and recommendations in order to improve the Malaysian legislation and bring it in line with international standards.

خلاصة البحث

لقد أحدثت جائحة كوفيد-19 تغييراً جذرياً في الحضارة، وسيطلب منظوراً تاريخياً طويلاً لفهم آثار ذلك التغيير بشكل كامل. من الواضح أن التطورات الحالية سواء أكانت تتعلق بالخصوصية والتكنولوجيا أم لا سيكون لها تأثير على الطريقة التي يتطور بها المجتمع في المستقبل. لقد غيرت المبادرات القائمة على البيانات التي تم إنشاؤها استجابة لجائحة كوفيد-19 بالفعل كيفية مشاركة المجتمع مع أفكار التكنولوجيا والخصوصية، من اختبار الصحة العامة على نطاق واسع إلى أدوات الاتصال الفردية. وتصنف البيانات الشخصية كواحدة من أكثر السلع القيّمة والمرغوبة ولا سيّما في عصر الرقمنة وظهور التقنيات الحديثة. بالنظر إلى أزمة جائحة كوفيد-19 وتدابير السياسة المتخذة في ماليزيا، هناك حاجة لحماية خصوصية الفرد والبيانات الشخصية. يهدف هذا البحث إلى دراسة وتحليل الآثار المترتبة على الخصوصية وحماية البيانات وفقاً لقوانين وسياسات جائحة كوفيد-19 في ماليزيا بين عامي 2020 و 2022. يعتمد البحث على المنهج التحليلي لدراسة التشريعات ذات الصلة. كما تم استخدام المنهج التقييمي الوصفي لتقييم القوانين والسياسات الحالية المتعلقة بحماية البيانات الشخصية. وكذلك تم استخدام الأسلوب النوعي والعقائدي في مسح الأدبيات وتحليلها. وخلصت الدراسة إلى أنه على الرغم من وجود قوانين بشأن الخصوصية وحماية البيانات الشخصية في ماليزيا، لا يزال هناك مجال لتحسين تلك القوانين لمعالجة الثغرات والتحديات التي ظهرت خلال جائحة كوفيد-19. وعليه يقترح البحث بعض الاقتراحات والتوصيات من أجل تحسين التشريع الماليزي وجعله يتماشى مع المعايير الدولية.

APPROVAL PAGE

I certify that I have supervised and read this study and that in my opinion, it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Comparative Laws.



.....
Sonny Zulhuda
Supervisor

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Comparative Laws.

.....
Suzi Fadhilah
Internal Examiner

I certify that I have read this study and that in my opinion it conforms to acceptable standards of scholarly presentation and is fully adequate, in scope and quality, as a dissertation for the degree of Master of Comparative Laws.

.....
Nasarudin Abdul Rahman
Internal Examiner

This dissertation was submitted to the Department of Civil Law and is accepted as a fulfilment of the requirement for the degree of Master of Comparative Laws.

.....
Mazlena Mohd Hussain
Head, Department of Civil Law

This dissertation was submitted to the Ahmad Ibrahim Kulliyah of Laws and is accepted as a fulfilment of the requirement for the degree of Master of Comparative Laws

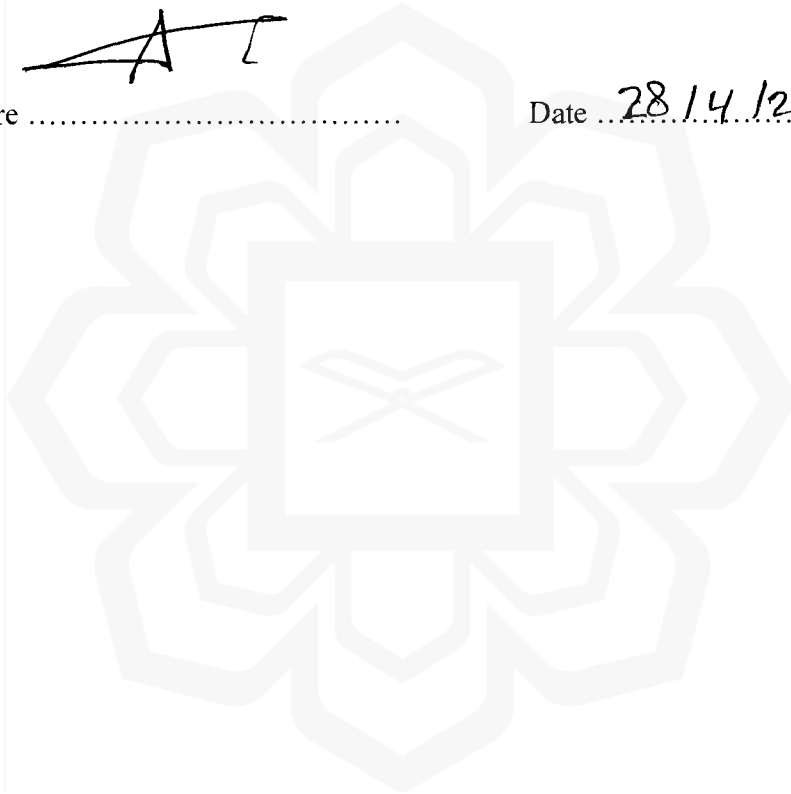
.....
Farid Sufian Shuaib
Dean, Ahmad Ibrahim Kulliyah
of Laws

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Alaa Sakka

Signature  Date ..28/4/2023.....



INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF
FAIR USE OF UNPUBLISHED RESEARCH**

**COVID-19 PANDEMIC POLICIES IN MALAYSIA AND THE
ISSUES OF PRIVACY AND DATA PROTECTION**

I declare that the copyright holders of this dissertation are jointly owned by the student and IIUM.


Copyright © 2023 by Alaa Sakka and International Islamic University Malaysia. All rights reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below.

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.
3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Alaa Sakka.



.....

Signature

28/4/2023

Date



This Dissertation is Dedicated to

My beloved parents

Eng. Mhd Ayman Sakka

&

Eng. Maha Alhomsy

For all their support, sacrifices, and prayers during my study journey.

My dear brothers and sisters for providing me with unfailing support and continuous encouragement throughout my years of study.

Thank you all.

ACKNOWLEDGMENTS

First and foremost, I would like to praise Allah (SWT) the Almighty, the Most Gracious, and the Most Merciful for His blessing given to me during my study and for granting me the ability and guidance to conduct and complete this humble dissertation. May Allah's blessing goes to His final Messenger (Peace Be Upon Him), who is the torch bearer of light and the greatest benefactor of the humanity.

It is my utmost pleasure to acknowledge the support, sacrifices, and prayers given by my parents and my siblings for providing me with unfailing support and continuous encouragement throughout my years of study. This accomplishment would not have been possible without them. I pray to Allah to reward them with all the goodness, happiness, and prosperity.

I would like to extend my heartfelt gratitude and thank my supervisor Assoc. Prof. Dr. Sonny Zulhuda who generously provided knowledge and expertise for his enduring supervision, thoughtful understanding, and valuable guidance throughout the period of this study.

In addition, I would like to thank all the helpful library staff of the International Islamic University Malaysia (IIUM), as well as all the academic and administrative staff of the Ahmad Ibrahim Kulliyah of Laws (AIKOL).

Lastly, Praise Highly be to the Almighty Allah for His endless mercy, guidance, and assistance in successfully completing the efforts of writing this humble research. Praise be to Allah always and forever.

TABLE OF CONTENTS

Abstract	i
Abstract in Arabic	ii
Approval Page.....	iii
Declaration	iv
Acknowledgments.....	vii
List of Figures	x
List of Cases.....	xi
List of Statutes	xii
CHAPTER ONE: INTRODUCTION.....	1
1.1 Background to the Research	1
1.2 Statement of the Problem.....	3
1.3 Objectives of the Research.....	5
1.4 Research Questions	5
1.5 Literature Review.....	6
1.6 Research Methodology	13
1.7 Scope and Limitations of the Study	15
1.8 Chapterization	15
CHAPTER TWO: COVID-19 PANDEMIC LAWS AND POLICIES AND THE INTERSECTION WITH THE RIGHT TO PRIVACY AND DATA PROTECTION.....	18
2.1 Introduction.....	18
2.2 Covid-19 Pandemic and the Public Policy Measures	20
2.3 The Laws and Policies During Health Emergencies in Malaysia.....	22
2.3.1 The Constitutional Power	23
2.3.2 The Prevention and Control of Infectious Diseases Act 1988 (Act 342).....	26
2.3.3 Security Laws	28
2.3.4 The Covid-19 Related Orders.....	30
2.3.4.1 Movement Control Order.....	30
2.3.4.2 Conditional Movement Control Order.....	31
2.3.4.3 Recovery Movement Control Order	31
2.3.4.4 Enhanced Movement Control Order.....	32
2.4 Emerging Legal Issues and Challenges in Malaysia.....	33
2.4.1 Surveillance by Government	34
2.4.2 Surveillance by Employers.....	38
2.4.2.1 The Monitoring of Individuals.....	39
2.4.2.2 Protecting Employee Privacy.....	42
2.4.3 Privacy of Students During the Pandemic.....	43
2.4.3.1 Campus Personal Surveillance.....	45
2.4.3.2 Protecting Education Privacy.....	47
2.5 Legal Framework for the Protection of Privacy and Data Protection in Malaysia.....	48
2.5.1 Right to Privacy in Malaysia	50

2.5.2 Personal Data Protection Law in Malaysia	56
2.6 Conclusion	63
CHAPTER THREE: ISSUES AND CHALLENGES IN THE COVID-19 TRACING APPLICATION.....	65
3.1 Introduction.....	65
3.2 Contact Tracing Application.....	66
3.3 Human Contact Tracing.....	69
3.4 Tracking of Digital Contacts.....	72
3.4.1 Centralized Digital Contact Tracing.....	74
3.4.2 Decentralized Digital Contact Tracing.....	75
3.5 The Legal Issues in Contact Tracing Programs	77
3.6 MySejahtera Tool.....	80
3.6.1 Applicability of PDPA 2010 to Personal Data Processing via MySejahtera.....	81
3.6.2 Data Collection.....	82
3.6.3 The Purposes of Data Use	84
3.6.4 Is the Data Secure?	86
3.6.5 Is it Open to Access?	89
3.6.6 Retention of Personal Data.....	90
3.7 Conclusion	92
CHAPTER FOUR: SURVEILLANCE DURING COVID-19 PANDEMIC IN MALAYSIA.....	94
4.1 Introduction.....	94
4.2 What is Surveillance?	96
4.3 Why is Surveillance an Issue During Pandemic.....	99
4.4 Surveillance During Covid-19 Pandemic in Malaysia.....	101
4.4.1 Data Surveillance	104
4.4.2 Surveillance of Movement	109
4.4.3 Surveillance at Work.....	116
4.4.3.1 Remote Surveillance and Time Tracking	119
4.4.3.2 Tracking Biometric and Health Data	122
4.5 Conclusion	124
CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS	126
5.1 Conclusion	126
5.2 Recommendations.....	129
BIBLIOGRAPHY	133

LIST OF FIGURES

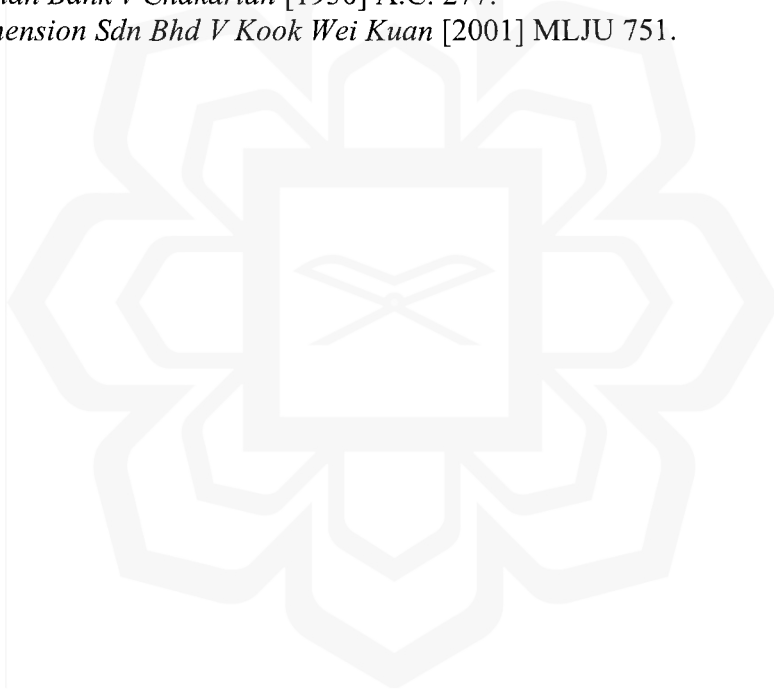
Figure 1 Police Permit Form during Lockdown - Permit Pergerakan Perintah Kawalan Pergerakan (PKP). 111

Figure 2 QR coded wristband (top center), digital login and registration step (left), and Stay Home Notice (right). 113



LIST OF CASES

- Dato' Seri Anwar Ibrahim v The New Straits Times Press (M) Sdn Bhd & Anor* [2010] 2 MLJ 492 (HC).
- Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors* [2022] 11 MLJ 898.
- Halsey v. Esso Petroleum Co Ltd* [1961] 1 W.L.R 683.
- Madhavan Nair v Government of Malaysia* [1975] 2 MLJ 286.
- Newlake Development Sdn Bhd v Zenith Delight Sdn Bhd & Ors* [2021] 11 MLJ 729.
- Ngeow Voon Yean v Sungei Wang Plaza Sdn Bhd/Landmarks Holding Bhd* [2006] 5 MLJ 113.
- Sivarasa Rasiah v. Badan Peguam Malaysia & Anor* [2010] 3 CLJ 507.
- Teh Cheng Poh v. Public Prosecutor* [1979] 1 MLJ 50 (PC).
- The Ottoman Bank v Chakarian* [1930] A.C. 277.
- Ultra Dimension Sdn Bhd V Kook Wei Kuan* [2001] MLJU 751.



LIST OF STATUTES

International Instruments

International Covenant on Civil and Political Rights 1966 (ICCPR)
Privacy Framework Act of the Organization for Economic Co-operation and Development (OECD) 1980 (Revised 2013)
Universal Declaration of Human Rights 1948 (UDHR)

Europe

EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data 2016
European Convention for the Protection of Human Rights and Fundamental Freedoms 1950

Malaysia

Civil Law Act 1956 (Act 67) (Revised 1972) (Reprint 1993 and 1999)
Communications and Multimedia Act 1998 (Act 588)
Computer Crimes Act 1997 (Act 563)
Employment Act 1955 (Act 265)
Federal Constitution 1957
Medical Act 1971 (Act 50)
National Security Council Act 2016 (Act 776)
Occupational Safety and Health Act 1994 (Act 514)
Official Secrets Act 1972 (Act 88)
Penal Code (Act 574)
Personal Data Protection Act 2010 (Act 709)
Police Act 1967 (Act 344)
Prevention and Control of Infectious Diseases (Measures within Local Infected Areas) Regulations 2020
Prevention and Control of Infectious Diseases Act 1988 (Act 342)
Temporary Measures for Reducing the Impact of Coronavirus Disease 2019 (COVID-19) Act 2020 (Act 829)

United Kingdom

Regulation of Investigatory Powers Act 2000

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE RESEARCH

Since the emergence of COVID-19 in Malaysia in March 2020, the Malaysian government has issued Standard Operating Procedures (SOP) to control the spread of the pandemic, starting with a Movement Control Order (MCO) at the time, followed by a Conditional Movement Control Order (CMCO), and others. The states began entering the stage of the recovery plan, due to the decrease in the number of injuries in them. Nevertheless, standard operating procedures for pandemic control are easing over time, as the country entered the stage of transition to endemicity, which would see various sectors give more flexibility to enable people to return to a semi-normal life after fighting COVID-19 for more than two years.

The standard operating procedures include precautionary measures to facilitate access and know the possible cases of infection by tracking the contacts and the specific location of the person through their movement through certain apps that enable them to know the person's name, identification number, health status, temperature, time of entry and exit, and the location for either employees or clients, which leads to an increase privacy and data protection risks. When implementing these standard operating procedures (SOPs), consideration must be given to compliance with the data security measures and privacy and data protection act.

Data privacy is now more important than ever, in this current pandemic that all countries around the world are going through. Technology expanded and developed beginning in the nineties and included the World Wide Web, social media platforms,

cryptocurrencies, the Internet of Things and many more, as well as Internet-based communications from e-mail, simple message boards, chat rooms and other technologies currently used, such as contact tracing and access to personal data, whether in education, health, and employment, especially in the time of COVID-19. All of these technologies have the ability to collect, analyse, store and use data. In this pandemic, everyone is increasingly relying on these technologies for the reason that many countries around the world are in lockdown due to COVID-19.

Among the technological uses adopted at the time of the emergence of the virus, is the use of a contact tracing application that enables the Ministry of Health to know active COVID-19 cases near 1 km from the place of residence of citizens registered in this app. The Ministry of Health is constantly providing news and updates to citizens regarding the Coronavirus through this app, which allows citizens to take precautions and beware of infection. The role of conscious citizens and employees is to be ready to provide their personal information for the necessity of tracing their contact information, which helps the government to limit the spread of the COVID-19 virus.

The processing of personal data of citizens is subject to the Personal Data Protection Act 2010 (PDPA). For example, in private hospitals, patient data is subject to the PDPA, while in public hospitals, patient data will not be subject to the PDPA but rather is subject to the Common Law right to privacy. Thus, this leads to an increase in citizens' concerns about how this data is managed and used, and their fear in the event of failure to know who is responsible for leaking the data if it is leaked.

To avoid and facilitate obstacles among countries, some countries have approved and issued COVID-19 vaccine passports, which allow travel to countries that have signed a mutual agreement to accept this passport, but only under certain restrictions and clauses. For example, the European Union's proposal allows any EU

citizen who has already been vaccinated to travel freely to all member states of the European Union but not to non-EU countries.

1.2 STATEMENT OF THE PROBLEM

The established trend in Malaysia at the start of the COVID-19 crisis was to use contact tracing app to track active COVID-19 cases, register for the vaccine, and certify the vaccination. These programs took personal data of the user, such as the person's name, identity number, residential address, phone number, temperature, and time of entry and exit. However, after the start-up phase of these programs, these programs began to develop problems. Firstly, there is the possibility of encountering problems in handling and preserving this sensitive data and not being exposed to disclosure, and the accumulation of this data. According to Dr. Noor Hisham Abdullah, The Malaysian Director General of Health, the MySejahtera contact tracking application used in Malaysia is being used responsibly, but according to him, this does not make him and the citizens confident that the data collected from the application will not be abused or misused.¹ The Director-General of Health has stated, according to Exodus Privacy,² MySejahtera collects a lot of location data through a contact tracing app. In addition, there are a plethora of different possibilities that are of great concern, such as: pair with Bluetooth devices, call directly to phone numbers, search for accounts on your phone, read your contacts, read the contents of any external storage on your phone such as SD cards, edit or delete the contents of your SD cards, prevent your phone from sleeping,

¹ Zan Azlee, "COMMENT | Privacy Issues with MySejahtera," *Malaysiakini*, 20th November, 2020, <https://www.malaysiakini.com/columns/551758> (accessed 14 September, 2021).

² "MySejahtera, "Exodus Privacy," (accessed 22 September, 2021), <https://reports.exodus-privacy.eu.org/en/reports/my.gov.onegovappstore.mysejahtera/latest>. "Exodus Privacy" is a French non-profit research center working in conjunction with the Yale University Privacy Laboratory, which aims to create awareness of cybersecurity, especially when it comes to privacy and unethical data collection online.

and edit your contacts.³ Malaysia has been ranked fifth worst out of 47 countries in terms of protecting personal data, according to a tech study conducted by the British company Comparitech before the start of the COVID-19 pandemic.⁴ By the report, Malaysia was classified as a country with "some safeguards but weakened protection".⁵ Thus, according to the British company's study, data protection is weak in Malaysia, and therefore the data may fall into the wrong hands easily, and the mistake may also cause the unintentional disclosure of information and data to others.

Secondly, when certain businesses and organizations are allowed to operate during the period of the restraining order, there is a risk of an increased potential for a data security breach. Thus, cyber threats may increase as opportunists take advantage of the situation. Companies or organizations that handle personal data must ensure that adequate security measures are in place and that adequate safeguards are in place to ensure that personal data records do not fall into the wrong hands. For data collected through electronic means, persons granted access to personal data must be adequately trained and reminded to follow internal disclosure protocols. When sensitive data is leaked, they will be responsible for these leaks but who is responsible in this case, such as hospitals, public and private sectors, apartment complexes, shopping malls, etc., or when a third party is involved in providing a vaccine or data protection (provider, Ministry of Health or third party) and also when transferring such sensitive data internationally.

³ Azlee, "COMMENT | Privacy Issues with MySejahtera," *Malaysiakini*, (accessed 14 September, 2021).

⁴ Ashley Tang, "Study: Malaysia the Fifth-Worst Country for Personal Data Protection," *The Star*, 16 October, 2019, <https://www.thestar.com.my/news/nation/2019/10/16/study-malaysia-the-fifth-worst-country-for-personal-data-protection> (accessed 22 September, 2021); "Malaysia Ranks '5th Worst' in Privacy Study," *Malaysiakini*, 16 October, 2019, <https://www.malaysiakini.com/news/496024> (accessed 22 September, 2021).

⁵ Ibid.

1.3 OBJECTIVES OF THE RESEARCH

1. To examine the policy measures taken by the Malaysian government to address COVID-19 pandemic between 2020 to 2022.
2. To analyse the privacy and data protection implications from the implementation of COVID-19 pandemic laws and policies in Malaysia from 2020-2022.
3. To analyse legal issues and challenges arising from the implementation of COVID-19 tracing application and surveillance measures in Malaysia from a data protection perspective.
4. To recommend improvements on the enforcement of data protection laws in Malaysia particularly during the health emergency.

1.4 RESEARCH QUESTIONS

1. What are policy measures taken by the government in response to the COVID-19 pandemic between 2020-2022?
2. What are the privacy and data protection implications from the implementation of COVID-19 laws and policies in Malaysia from 2020-2022?
3. What are legal issues and challenges arising from the implementation of tracing apps and surveillance measures in Malaysia in relation to privacy and data protection?
4. What aspects that should be taken into consideration for the improvement of the existing data protection laws in Malaysia?

1.5 LITERATURE REVIEW

The researcher has consulted several primary and secondary sources of information for writing a review of the literature pertaining to the study. The important sources consulted for this purpose are the Library, Google Scholar, journal articles, books, thesis, reports, and Web-search.

The study acquires references that include user privacy and data protection at the time of the Corona pandemic in Malaysia and how to deal with it. The protection of confidential information is a concern for both government and individuals, with significant consequences and loss if private and sensitive data falls into the hands of an unauthorized person or if such information is compromised.

Anna Elena Unker had mentioned in her article on the applicability of Article 9 of the Regulation (European Union) 2016/679 on the protection of sensitive personal data during the COVID-19 pandemic that compels both strict rules and deadlines on both controllers and processors of personal data.⁶ Given the huge flow of information circulating in every area of people daily activities, the balance of the relationship between the data subject and the observer must be fair and transparent. What happens, however, when this delicate balance is upset by catastrophes that directly affect people health, whether on a regional or global scale? To what extent does the Regulation fulfil its goal of safeguarding data subjects' rights? Compared to Malaysia, and since it is not a member of the European Union, it has its own personal data protection law, which this dissertation will discuss issues related to how this law deals with the Corona pandemic.

⁶ Ana-Elena Iunker, "Applicability of Article 9 of the Regulation (EU) 2016/679 on the Protection of Personal Sensitive Data during COVID-19 Pandemic", *Conferinta Internationala de Drept, Studii Europene si Relatii Internationale 2020* (2020): 357-368.

Gitanjali Deep had mentioned in the article “Data privacy landscape during COVID-19: Exploring some of the major data privacy regulations and trends”, considering the current global pandemic, data privacy regulations are more important than ever.⁷ Historically with the advent of the Internet, the era of electronic communication has dawned all over the world. Beginning in the 1990s, improvements in Internet-based communication technology grew beyond simple email, message boards, and chat rooms to encompass the World Wide Web, biometric data, Geographical information system (GIS technologies), social media platforms, cryptocurrencies, the Internet of Things, and many other things. All of these technologies are capable of collecting, analyzing, storing, and utilizing data in cyberspace. With so many places worldwide under quarantine owing to COVID-19, everyone is becoming increasingly reliant on this technology. The method people gather, keep, utilize, and safeguard this information has had, and will remain to have, a substantial impact on topics such as personal privacy, safety, terrorism, national security, the economy, and others. In her article, she discussed the implications of the issues affecting society in light of the COVID-19 pandemic, which the whole world is facing, from mandatory closures that force companies and individuals to work and buy online. This allows some large companies to collect and use data, such as Amazon, Apple, Google, and Facebook.⁸ She also mentioned that the need for regulation is clear and raised some other issues that illustrate the risks associated with inadequate cybersecurity protection for large-scale data collection and storage such as the Apple

⁷ Gitanjali Deb, “The Data Privacy Landscape during COVID-19: An Exploration of Some of the Major Data Privacy Regulations and Trends”, *DePaul Journal of Art, Technology and Intellectual Property Law*, vol. 31, no. 1 (2021): 1-67.

⁸ Rani Molla, “As CoVID-19 Surges, the World's Biggest Tech Companies Report Staggering Profits - Despite Antitrust Investigations and a Recession, Big Tech is doing Great,” *Vox*, 30 October, 2020, <https://www.vox.com/recode/2020/10/30/21541699-big-tech-google-facebook-amazon-apple-coronavirus-profits> (accessed 25 September, 2021).

iCloud photo leak in 2014,⁹ the Equifax data breach in 2017,¹⁰ the target data breach in 2013,¹¹ the Capital One breach in 2019,¹² the 2016 US Cambridge Analytica scandal,¹³ and the Russian SolarWinds Orion hacking scandal to influence more than 18,000 global clients, including many US government agencies.¹⁴ In her article, she investigated the key current data privacy regulations in force in the United States and Europe, as well as various trends in regulation and enforcement under the General Data Protection Regulation (GDPR), and how individual, business, and government rights are faring in the massive data warfare. Gitanjali Deep presented the General Data Protection Regulation (GDPR), and since the article focused on US law, it did not include Malaysian law or a variety of other issues, which is what the researcher will address in order to discuss the laws relevant to the current dissertation.

Meanwhile, Sharon Bassan, in her article on "Data privacy considerations for telehealth consumers amid COVID-19" in 2020 in US law, discussed the effects of the notification on the privacy of patients' health information. It had recommended that patients carefully read provider privacy policies to ensure their Protected Health Information (PHI) is not at risk before switching to telehealth consultations, and that

⁹ Steve Kovach, "We Still Don't Have Assurance from Apple That iCloud Is Safe," Business Insider, (<https://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9>) (accessed 26 September, 2021).

¹⁰ Federal Trade Commission, "Equifax Data Breach Settlement," January, 2020, <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>

¹¹ Maggie McGrath, "Target Data Breach Spilled Info on as Many as 70 Million Customers," *Forbes*, 10 January, 2014, <https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=334debd9e795> (accessed 27 September, 2021).

¹² Emily Flitter and et al, "Capital One Data Breach Compromises Data of Over 100 Million," *The New York Times*, 29 July, 2019, <https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html> (accessed 27 September, 2021).

¹³ Alexandra Ma and et al, "Facebook Understood How Dangerous the Trump-linked Data Firm Cambridge Analytica Could Be Much Earlier Than It Previously Said. Here's Everything That's Happened Up Until Now," Business Insider, (<https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3>) (accessed 28 September, 2021).

¹⁴ Alex Marquardt and et al, "Microsoft Identifies More Than 40 Organizations Targeted In Massive Cyber Breach," *CNN*, 17 December, 2020, <https://edition.cnn.com/2020/12/17/politics/microsoft-hack-organizations/index.html> (accessed 28 September, 2021).

consumer data privacy should be protected through one of two alternative regulatory interventions: the authority of the Federal Trade Commission (FTC) under article 5, or Health Insurance Portability and Accountability Act (HIPAA) business partner agreements and this is what the researcher covered in her article.¹⁵ In this research, the current study fills this gap through Malaysian law. Sensitive personal data is subject to stricter and additional safeguards under the Personal Data Protection Act (PDPA).

Other relevant studies have been conducted in the context of ecommerce and electronic banking. In light of COVID-19, many governments had tended to use electronic payments in place of cash in daily expenses, and some countries had provided emergency payments to citizens as financial assistance in light of these economic conditions that all countries are going through. In their article on “Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency”, Eli Rainey, and Stacey Steel explain the social and economic policy choices involved in the design of the central bank digital currencies (CBDC) and the consequences of these choices for privacy.¹⁶ Geopolitical and private issues, as well as preventing criminal abuses of the financial system, are among the top priorities. Industry innovation competes with privacy and may jeopardise it. As “losses” associated with current CBDC models, they identify and define four significant privacy risks: loss of freedom, loss of individual control, loss of anonymity, and loss of organizational control. As their study concludes, solutions such as CBDCs have not adequately addressed user concerns about privacy.

Additionally, Tiffany C. Li conducted a study on “Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis”, which led to the use of

¹⁵ Sharon Bassan, “Data Privacy Considerations for Telehealth Consumers amid COVID-19”, *Journal of Law and the Biosciences*, vol. 7, no. 1 (January-June 2020): 1-12.

¹⁶ Ellie Rennie and et al, “Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency”, *Law, Technology and Humans*, vol. 3, no. 1 (2021): 6-17.

modern technologies, including drones, to monitor active cases of COVID-19 as well as to monitor social distancing.¹⁷ In the article, she addressed these privacy and technology problems specifically in light of the pandemic, arguing that the lens of the pandemic reveals the need for large-scale and small-scale reform of privacy law, focusing on technical realities and social prominence, and with a critical awareness of digital and political inequality, formulating normative recommendations while putting these concepts in mind. In this dissertation, the researcher will discuss this problem from the perspective of Malaysian laws on privacy and technology related-matters focusing on violation of privacy and civil liberties by the government and companies in sectors such as health care, employment, education, commerce and industry.

Regarding contact tracing, Divya Ramjee, Pollyanna Sanderson, and Imran Malek wrote on COVID-19 and Digital Contact Tracing on Regulating the Future of Public Health Surveillance, with regard to digital surveillance tools and technologies for monitoring, tracking and notification of the public health response to the COVID-19. They recommended that the United States should establish a federal public health monitoring network with the help of digital tools, particularly given that waves of COVID-19 are expected to continue well into 2021 and while the threat of other emerging infectious diseases continues.¹⁸ Meanwhile, Laura Bradford, Mateo Aboy, and Kathleen Liddell have written on “COVID-19 Contact Tracing Apps about Privacy Stress Testing, the GDPR, and Data Protection Regimes”, that Google and Apple recently announced their intention to build interfaces to allow contact tracing Bluetooth using Android and iPhone devices. They had a look at the compatibility of the proposed Apple/Google Bluetooth exposure notification system with Western privacy and data

¹⁷ Tiffany C. Li, “Privacy in Pandemic: Law, Technology, and Public Health in the COVID-19 Crisis”, *Loyola University Chicago Law Journal*, vol. 52, no. 3 (Spring 2021): 767-866.

¹⁸ Divya Ramjee and et al, “COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance”, *Cardozo Law Review De-Novo 2021* (2021): 101-161.