Kathmandu School of Law Review (KSLR),
Volume 8, Issue 1, 2020, pp 50-76
https://doi.org/10.46985/kslr.v8i1.2128

Contact Tracing Apps in Asean : A Threat to Privacy and Personal Data

Agung Kurniawan Sihombing & Yogi Bratajaya***

Abstract

On March 11 2020, the World Health Organization (WHO) officially categorized the Coronavirus disease (COVID-19) as a global pandemic. The rapid spread of COVID-19 prompted governments all around the world to take steps toward controlling the pandemic and its significant socio-economic impacts. Digital technology has been relied upon to provide innovative solutions to aid efforts of stopping the spread of COVID-19. One such innovation is the development and implementation of contact tracing applications or apps. The use of these apps allows public health authorities to track confirmed cases of COVID-19 and mitigate its transmission. However, as useful as they may be, there exists a well-grounded fear that contact tracing apps may be used as a tool to broaden government surveillance powers. This is especially true among member nations of the Association of Southeast Asian Nations (ASEAN), where domestic regulations guaranteeing the right to privacy and protection of personal data are relatively weak. Additionally, ASEAN lacks a comprehensive and strong regional mechanism for the protection of human rights and personal data. This paper aims to analyze the implementation of contact tracing apps in ASEAN member states, whether its implementation fulfills the international standards of the protection of the right to privacy and personal data, as well as provide recommendations to ensure that countries do not spiral towards a state of unrestricted government surveillance.

I. Introduction

It is becoming a cliché to say how transformative [digital technologies] are, serving as a double-edged sword that may either lead to our collective human flourishing – or to our collective demise. (Statement by Nada Al-Nashif, United Nations Deputy High Commissioner for Human Rights, 8 July 2020.)

* Agung Kurniawan Sihombing earned his Bachelor of Law from Universitas Padjadjaran in Indonesia. He can be reached at agungkurniawansihombing@gmail.com.

** Yogi Bratajaya earned his Bachelor of Law from Universitas Padjadjaran in Indonesia, specializing in Public International Law. He can be reached at ybratajaya@gmail.com.

The paper was awarded the 3rd Best Paper in the International Research Paper Writing Competition, which was organized by Kathmandu School of Law Review, Amnesty International Fusion Youth Network, and the Cognition Club.

The whole world is facing an unparalleled global health crisis in its scale and impact. As of August 2020, the World Health Organization (WHO) has reported almost 18 million cases of the Coronavirus disease (COVID-19) globally, with more than 600,000 reported deaths.[1] If the pandemic is not swiftly controlled, it is bound to have devastating socio-economic impacts on countries and the livelihoods of its citizens.[2] Countries have resorted to taking drastic measures in order to control the spread of COVID-19, such as greatly increasing the capacity of their health sectors and imposing widespread lockdowns.[3]

The response from members of the Association of Southeast Asian Nations (ASEAN) to the COVID-19 pandemic has been highly varied. At the time of writing of this paper, Vietnam, for example, seems to have successfully controlled the spread of COVID-19, with only 6 reported deaths and less than 700 confirmed cases.[4] Indonesia, on the other hand, is still struggling to contain the spread of COVID-19, with more than 100,000 confirmed cases, around 5,000 deaths, and more than 2,000 new confirmed cases each day.[5]

Countries have implemented technological solutions to aid their efforts in controlling and preventing the spread of COVID-19.[6] One of the primary technology-based tools being implemented are contact tracing apps, which are mobile apps designed to track an individuals' activities and help contact tracing efforts.[7] While these apps may be helpful, various stakeholders have expressed concern, claiming that countries could use the technology beyond purposes of controlling the COVID-19 pandemic.[8] The ability

1 'Coronavirus disease (COVID-19) Situation Report – 196', *World Health Organization (WHO)*, 3 August 2020, available at https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200803-covid-19-sitrep-196-cleared.pdf?sfvrsn=8a8a3ca4_4, accessed on 3 August 2020.

2 'A UN framework for the immediate socio-economic response to COVID-19', *United Nations (UN) Sustainable Development Group*, April 2020, p. 3, available at https://unsdg.un.org/resources/un-framework-immediate-socio-economic-response-covid-19, accessed on 3 August 2020; 'A Crisis Like No Other, An Uncertain Recovery', *International Monetary Fund*, June 2020, available at https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020#:~:text=A%20Crisis%20Like%20No%20Other%2C%20An%20Uncertain%20Recovery,-Read%20full%20report&text=The%20COVID%2D19%20pandemic%20has,is%20projected%20at%205.4%20percent., accessed on 3 August 2020.

3 'Critical preparedness, readiness and response actions for COVID-19' *WHO*, 24 June 2020, pp. 3-7, available at https://apps.who.int/iris/rest/bitstreams/1283590/retrieve, accessed on 25 July 2020.

4 'Coronavirus disease (COVID-19) Situation Report – 196' (n 1); See also Anna Jones, 'Coronavirus: How 'overreaction' made Vietnam a virus success', *BBC News*, United Kingdom, 15 May 2020, available at https://www.bbc.com/news/world-asia-52628283, accessed on 27 July 2020.

5 'Coronavirus disease (COVID-19) Situation Report – 196' (n 1); See also Alya Nurbaiti, 'Indonesia's daily average of new COVID-19 cases continues to climb: WHO', *The Jakarta Post*, Indonesia, 17 July 2020, available at https://www.thejakartapost.com/news/2020/07/16/indonesias-daily-average-of-new-covid-19-cases-continues-to-climb-who.html, accessed on 27 July 2020.

6 'Tracking the Global Response to COVID-19', *Privacy International*, available at https://privacyinternational.org/examples/tracking-global-response-covid-19, accessed on 27 July 2020.

7 'Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing' *WHO,* 28 May 2020, p. 1, available at https://apps.who.int/iris/rest/bitstreams/1278803/retrieve, accessed on 25 July 2020.

8 'Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights', *Human Rights Watch (HRW)* 2 April 2020, available at https://www.hrw.org/

to track and subject individuals to surveillance would have significant implications towards human rights and the protection of personal data. For example, even with the utilization of data anonymization, a user can still be re-identified by combining pieces of information that are open to the public.[9] The fear is that this data will fall into the wrong hands and be abused for reasons outside the scope of pandemic control.

Such concerns highlight the fact that contact tracing apps have profound impacts on the right to privacy, a fundamental human right recognized within Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[10] Indeed, the United Nations (UN) has emphasized that a successful pandemic response and recovery effort must ensure respect for human rights.[11] Consequently, countries must fulfill obligations to respect and protect human rights while taking measures to control the spread of COVID-19. Any measures put in place by countries that restrict human rights must abide by the rule of law and fulfil the conditions imposed by international human rights law.[12] In order to avoid misuse by governments, any interference with the right to privacy emanating from contact tracing apps must be based on law and be non-arbitrary.[13]

However, while the realization of personal data protection has developed significantly during recent years, countries still seem reluctant to enact comprehensive domestic laws regulating this matter. This is especially the case with ASEAN countries, such as Indonesia, where their Personal Data Protection Bill (PDP Bill) was signed on January 24, 2020 by the President but has still not been finalized by the House of Representatives (DPR).[14]

This article places a focus on the implementation of contact tracing apps within ASEAN member states. The different data protection and human rights legal frameworks within

news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight, accessed on 25 July 2020; Elena Sánchez Nicolás, 'Coronavirus: Are we trading privacy for security?', *EU Observer*, 14 April 2020, available at https://euobserver.com/coronavirus/148041, accessed on 25 July 2020.

9 Kim Zetter, 'Anonymized Phone Location Data Not So Anonymous, Researchers Find', *WIRED*, 27 March 2013, available at https://www.wired.com/2013/03/anonymous-phone-location-data/, accessed on 25 July 2020.

10 *Universal Declaration of Human Rights,* 10 December 1948, UNGA 217 A (III) (UDHR), art. 5; *International Covenant on Civil and Political Rights*, 23 March 1976, 999 UNTS 171, New York, 16 December 1966 (ICCPR), art. 17.

11 'COVID-19 Guidance', *UN Office of the High Commission of Human Rights (*UN OHCHR*)*, 13 May 2020, p. 1, available at https://www.ohchr.org/Documents/Events/COVID-19_Guidance.pdf, accessed on 25 July 2020.

12 'Emergency Measures and Covid-19: Guidance', UN OHCHR*,* 27 April 2020, p. 1, available at ohchr.org/Documents/Events/EmergencyMeasures_COVID19.pdf, accessed on 25 June 2020; See also Maria Pia Sacco et.al, 'Digital Contact Tracing for the Covid-19 Epidemic: A Business and Human Rights Perspective', International Bar Association, 4 June 2020, p. 2.

13 *General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, UN Human Rights Committee (HRC), 8 April 1988, U.N. Doc. HRI/GEN/1/Rev.9 (General Comment No. 16), paras 3-4.

14 'Digital Trust NewsFlash', *PwC*, May 2020, available at https://www.pwc.com/id/en/publications/digital/digital-trust-newsflash-2020-02.pdf, accessed on 30 July 2020.

the association's member states greatly affect the possibility of contact tracing apps being used to infringe upon the privacy of its users.

Countries must, therefore, put in place sufficient safeguards to avoid infringement of the right to privacy and to ensure adequate personal data protection before implementing contact tracing apps. These safeguards must not be mere promises, but be based on binding laws that are consistent with the international standards for human rights and data protection. This paper also highlights that in this age of big data and heightened multilateralism, it would be highly desirable that ASEAN provides a comprehensive, binding regional framework to guarantee that the right to privacy in the digital space is respected and free from abuse. Additional reference and comparison is made to the legal framework and system provided by the European Union (EU), which is deemed to have a better implementation in this matter. References will be made to cases resolved by the Human Rights Committee (HRC) and other international human rights courts to elaborate on relevant human rights principles.

II. Discussion

ASEAN is a regional organization formed in 1967 which currently has ten members: Indonesia, Malaysia, Singapore, Brunei Darussalam, Vietnam, Thailand, the Philippines, Laos, Cambodia, and Myanmar.[15]

In contrast to other regional organizations, ASEAN is not an institutional organization in the sense that it does not have a clear decision-making and implementation structure. Amitav Acharya has stated that the approach chosen by ASEAN countries was more dependent on 'dialogue' and 'consultative mechanism'.[16] This is reflected in Article 20 of the ASEAN Charter, which outlines that decisions will be based on consultation and consensus.[17]

The reluctance of establishing binding obligations or enforcement mechanisms within ASEAN is deeply rooted in its fundamental principles of non-interference and respect for the sovereignty of its member states.[18] These characteristics are what define the ASEAN regional mechanism, which is commonly referred to as 'the ASEAN way'. An example of this mechanism in action is the 2002 ASEAN Agreement on Transboundary Haze Pollution (AATHP).[19] While the AATHP is a binding agreement, it has no compliance mechanism to ensure that state parties adhere to its obligations.[20]

---

15 'ASEAN Member States', *Association of Southeast Asian Nations,* available at https://asean.org/asean/asean-member-states/, accessed on 4 August 2020.

16 Amitav Acharya, 'Culture, Security, Multilateralism: The 'ASEAN way' and Regional Order', *Contemporary Security Policy* p. 55, volume 19:1, 2007, p. 8.

17 *Charter of the Association of Southeast Asian Nations,* December 2008, Singapore, 20 November 2007 (ASEAN Charter), art. 20.

18 *Treaty of Amity and Cooperation in Southeast Asia Indonesia,* Bali, 24 February 1976, art. 2; ASEAN Charter, art. 2(2).

19 *ASEAN Agreement on Transboundary Haze Pollution*, 2003, Kuala Lumpur, 10 June 2002 (AATHP).

20 AATHP, art. 3(2); Prischa Listiningrum, 'Transboundary Civil Litigation for Victims of Southeast Asian

This characteristic has undoubtedly influenced ASEAN's approach to the protection of human rights and personal data. ASEAN's main human rights instrument is the ASEAN Human Rights Declaration adopted in 2012 (AHRD). The right to privacy and personal data is contained within Article 21, which states that:

> Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honor and reputation. Every person has the right to the protection of the law against such interference or attacks.[21]

Although Article 21 goes further than other human rights instruments by expressly mentioning the importance of protecting personal data, the AHRD itself has received criticism from stakeholders at the national, regional and international levels.[22] This is primarily because the declaration is non-binding and the degree of human rights guaranteed by the AHRD is considered to be below the international standard.[23]

So far, the only instrument regulating data protection is the ASEAN Framework on Personal Data Protection which was adopted at the 16th ASEAN Telecommunications and Information Technology Ministers Meeting in 2016.[24] This framework establishes seven principles of personal data protection that should be implemented, which are:[25]

1. Consent, notification, and purpose;
2. Accuracy of personal data;
3. Security safeguards;
4. Access and correction;
5. Transfers to another state or territory;
6. Retention; and
7. Accountability.

Similar to the AHRD, the framework has obvious shortcomings in that it is non-binding, not clearly implemented, and the aforementioned principles are far from sufficient compared to those established by the EU.[26] The lack of a binding general

Haze Pollution: Access to Justice and the Non-Discrimination Principle', *Transnational Environmental Law* p. 119, volume 8:1, 2019, p. 125.

21 *ASEAN Human Rights Declaration*, 18 November 2012, Phnom Penh (AHRD), art. 21.

22 'Civil Society Denounces Adoption of Flawed ASEAN Human Rights Declaration', *HRW*, 19 November 2012, available at https://www.hrw.org/news/2012/11/19/civil-society-denounces-adoption-flawed-asean-human-rights-declaration, accessed on 23 July 2020.

23 Graham Greenleaf, *Asian Data Privacy Laws: Trade & Human Rights Perspectives,* Oxford University Press, UK, 1st edition, 2014, p. 26.

24 *The 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings: Joint Media Statement*, ASEAN, 26 November 2016, Bandar Seri Begawan, para. 4.

25 *Framework on Personal Data Protection 2012*, ASEAN Telecommunications and Information Technology Ministers Meeting (Telmin), para. 6, available at https://asean.org/joint-media-statement-the-16th-asean-telecommunications-and-information-technology-ministers-meeting-and-related-meetings/.

26 Benjamin Wong, 'Data Localization and ASEAN Economic Community', *Asian Journal of International Law*

data protection regulation within ASEAN means that countries are left on their own accord to implement personal data protection legislation. Without a comprehensive framework within ASEAN, it is therefore imperative to take into account the standards of the right to privacy under international human rights law, and the impactful principles of data protection established by the EU.

A. Contact Tracing Apps and Protection Framework in ASEAN Countries

Contact tracing is an essential tool in preventing the transmission of infectious diseases.[27] It helps identify and assess individuals who have been exposed to a disease, so they can be managed to prevent onward transmission.[28] An adequate capacity for contact tracing is essential if countries want to contain the spread of a disease in a timely manner.[29] This process has been used to control previous outbreaks, such as the Severe Acute Respiratory Syndrome (SARS) epidemic, which is part of a large family of viruses similar to COVID-19.[30]

To aid in contact tracing efforts, countries have implemented contact tracing apps, which provide an easier method for health authorities to identify whether an individual has come in contact with someone who has been infected with COVID-19 or not.

As of August 2020, 7 out of the 10 ASEAN member states had implemented contact tracing apps: Indonesia, Malaysia, Singapore, Philippines, Thailand, Brunei and Vietnam.[31] Almost all contact tracing apps in ASEAN use the same form of technology, which is a low-energy bluetooth signal to determine a user's proximity with other app users.[32] If a user tests positive for COVID-19, other users who have been in direct or indirect contact with that person will be notified and contacted directly by a health official in order to take steps to self-isolate.[33]

---

p. 1, volume 10:1, 2020, p. 22.

27 'Ethical considerations' (n 7) p. 1.

28 Ibid; Mohamed E El Zowalaty and Josef D Järhult, 'From SARS to COVID-19: A previously unknown SARS- Related Coronavirus (SARS-CoV-2) of Pandemic Potential Infecting Humans - Call for a One Health Approach', *One Health* p. 1, volume 9: 100124, 2020, pp. 2-3.

29 'Ethical considerations' (n 7) p. 1.

30 Dejian Lai, 'Monitoring the SARS Epidemic in China: A Time Series Analysis', *Journal of Data Science*,, volume 3, 2005, p. 290.

31 Kevin Shepherdson, 'How intrusive are contact-tracing apps in ASEAN?', *TECHINASIA*, 24 June 2020, available at https://www.techinasia.com/intrusive-asean-contacttracing-apps, accessed on 30 July 2020.

32 Rizki Fachriansyah and Ardila Syakriah, 'Indonesia Develops Surveillance App to Bolster Contact Tracing Tracking', *The Jakarta Post*, Indonesia, 30 March 2020, available at https://www.thejakartapost.com/news/2020/03/30/covid-19-indonesia-develops-surveillance-app-to-bolster-contact-tracing-tracking.html, accessed on 15 July 2020; 'Mobile Location Data and Covid-19: Q&A', *HRW,* 13 May 2020, available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa, accessed on 25 June 2020.

33 'PeduliLindungi', Indonesian Ministry of Communication and Information Technology (MoCIT), available at https://pedulilindungi.id/, accessed on 15 July 2020; 'MyTrace, a Preventive Counter Measure and Contact Tracing Application for COVID-19 - FAQ', Malaysian Ministry of Science, Technology and Innovation (MoSTI), available at https://www.mosti.gov.my/web/en/mytrace/#1588521061720-1739856b-c49b, accessed on 13 July 2020; Aarron Holmes, 'Singapore is using a high-tech surveillance

The table below indicates the contact tracing app implemented in each ASEAN member state, along with the guarantees to the right to privacy and personal data protection surrounding it.

Table A.1. Comparison of ASEAN member States' legal framework for the protection of privacy and personal data, and the availability of Covid-19 Contact Tracing apps

No.	ASEAN countries	Ratification of ICCPR	General Data Protection Act	Covid-19 Contact Tracing apps
1	Indonesia	Yes.	-	PeduliLindungi.
2	Malaysia	No.	Personal Data Protection Act 2010.	MyTrace.
3	Singapore	No.	Personal Data Protection Act 2012 (No. 26 of 2012).	TraceTogether.
4	Brunei	No.	-	BruHealth.
5	Vietnam	Yes.	-	Bluezone.
6	Thailand	Yes.	Personal Data Protection Act, B.E. 2562 (2019) (not enforced).	ThaiChana.
7	Philippines	Yes.	The Republic Act No. 10173 (Data Privacy Act of 2012) and the Implementing Rules and Regulations of the DPA.	StaySafe.Ph (and several others).
8	Laos	Yes.	Law on Electronic Data Protection No. 25/NA (2017).	-
9	Cambodia	Yes.	-	-
10	Myanmar	No.	-	-

1. Indonesia

On 30 March 2020, the Indonesian Ministry of Communication and Information Technology (MoCIT), in collaboration with the State-Owned Enterprises Ministry, developed the contact tracing app PeduliLindungi to help the government track and trace confirmed cases of COVID-19.[34] In addition to Bluetooth technology, PeduliLindungi uses geolocation from the phone's GPS to notify users when they are about to enter red zones, which are locations with confirmed COVID-19 cases.[35] The PeduliLindungi website states that the data stored by the app is encrypted and that only health officials

app to track the coronavirus, keeping schools and businesses open. Here's how it works', *Business Insider*, 24 March 2020, available at https://www.businessinsider.com/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3?r=US&IR=T, accessed on 24 July 2020; 'Vietnam launches Covid-19 contact tracing app', *Vietnam Insider*, 21 April 2020, available at https://vietnaminsider.vn/vietnam-launches-covid-19-contact-tracing-app/, accessed on 25 July 2020; 'StaySafe.ph mobile app with contact tracing, scan area features now on Google Play', *ManillaStandard.net*, 15 May 2020, available at https://manilastandard.net/tech/gadgets/323804/staysafe-ph-mobile-app-with-contact-tracing-scan-area-features-now-on-google-play.html, accessed on 25 July 2020.

34 Fachriansyah and Syakriah (n 32).

35 'Contact tracing apps: A new world for data privacy', *Norton Rose Fulbright*, July 2020, available at https://www.nortonrosefulbright.com/en-id/knowledge/publications/d7a9a296/contact-tracing-apps-a-new-world-for-data-privacy#indonesia, accessed on 25 July 2020.

will access the data where the user is at risk of being infected with COVID-19.[36]

The implementation of PeduliLindungi is authorized by Decree of the MoCIT No. 171 year 2020, which expressly provides that the app may only be used during the COVID-19 pandemic, subject to other decisions.[37] It is this caveat, along with the lack of transparency around the PeduliLindungi app that has drawn concerns over the right to privacy. On 26 June 2020, the Indonesian Representative to the ASEAN Intergovernmental Commission on Human Rights, along with numerous other human rights and digital rights organizations, sent an open letter to the MoCIT requesting more transparency and strong user privacy protections in the PeduliLindungi App.[38] The letter highlighted that there existed no privacy policy for PeduliLindungi, along with the lack of any safeguards provided by law for how PeduliLindungi collects data, where the data is stored and for how long, and who has access to the data.[39]

Indonesia recognizes the right to privacy based on the decisions of its constitutional court and by virtue of Articles 31 and 32 of Law No. 39 about Human Rights enacted in 1999.[40] In terms of data protection, Indonesia does not have a general data protection act, but there are certain regulations aimed at governing the use of electronic data, mainly Law No. 11 of 2008 on Information and Electronic Transaction as amended with Law No. 19 of 2016 (ITE Law).[41] The ITE Law has been interpreted so that the obligations apply to both the private and public sector.[42] Article 26 of the ITE Law is pivotal since it outlines an individual's right to personal data and grants the right to remedy over its abuse.[43] To bolster personal data protection within Indonesia, a PDP Bill is currently being discussed by the DPR.[44] One of the main points under the PDP Bill is that criminal sanctions may be imposed on entities misusing personal data.[45]

---

36 'PeduliLindungi' (n 33).

37 *2020 Decree of the Indonesian Minister of Communications and Information Technology No. 171* (MoCIT Decree No. 171), 2020, Indonesia, para. 5.

38 'Open Letter to KOMINFO Requesting for Strong User Privacy Protections in the PeduliLindungi App', *ELSAM,* 26 June 2020, available at https://elsam.or.id/open-letter-to-kominfo-requesting-for-strong-user-privacy-protections-in-the-pedulilindungi-app/, accessed on 27 July 2020.

39 Ibid.

40 *1999 Law No. 39 concerning Human Rights*, Indonesia, 1999, arts. 31-32; *KPKPN v KPK*, Indonesia Constitutional Court Case Number 006/PUU-I/2003; *Mulyana v KPK*, Indonesia Constitutional Court Case Number 012-016-019/PUU-IV/2006.

41 *Law No. 11 of 2008 on Information and Electronic Transaction as amended with Law No. 19 of 2016* (ITE Law), Indonesia 2008; 'Personal Data Protection in ASEAN', *ZICO*, April 2019, available at https://zico.group/publication/personal-data-protection-in-asean/, accessed on 24 July 2020.

42 Greenleaf, *Asian Data Privacy Laws* (n 23) p. 386.

43 ITE Law, art. 26.

44 'Indonesia: President submits draft data protection bill to the House of Representatives', *OneTrust DataGuidance*, 28 January 2020, https://www.dataguidance.com/news/indonesia-president-submits-draft-data-protection-bill-house-representatives, accessed on 10 August 2020.

45 Brinanda Lidwina Kaliska and Kurniawan Tanzil, 'A Guide to the Upcoming Indonesian Data Protection Law (Final Draft Law January 2020)', *Makarim & Taira S*., February 2020, p. 7, available at https://www.makarim.com/uploads/78289_M&T%20Advisory%20-%20A%20Guide%20To%20The%20Upcoming%20Indonesian%20Data%20Protection%20Law%20(February%202020).pdf, accessed on 9 August 2020; Michael S. Carl and Revaldi N. Wirabuana, 'Prohibitions, Restrictions Under Indonesia's Personal Data Protection Draft Law', *SSEK*, 12 June 2020, available at https://www.ssek.com/blog/

The use of contact tracing apps within Indonesia has highlighted the importance of strong protections of the right to privacy and increased the urgency for the enactment of a comprehensive general data protection law.

2. Malaysia

Malaysia's national contact tracing app, MyTrace, was developed by the Ministry of Science, Technology and Innovation (MoSTI) along with multiple other ministries, International Islamic University Malaysia and Google.[46] The MoSTI has allayed concerns over the right to privacy, stating that the data will be stored decentralized on the user's phone, and that the data stays on the phone only for 21 days.[47] Regarding who may access the data, the MoSTI stated that data may only be accessed with the permission of the user.[48] Furthermore, MyTrace does not collect data emanating from geolocation, and any data gathered would be anonymized.[49]

Despite reassurances made by the MoSTI, there is still a growing concern that MyTrace could infringe upon the right to privacy and personal data. These concerns arise over apparent weaknesses in Malaysia's legal data protection framework. Malaysia's principal data protection law is the Personal Data Protection Act (PDPA) enacted in 2010.[50] Although the PDPA adheres towards the main principles of data protection,[51] its scope is limited and only applies towards 'any personal data in respect of commercial transactions'.[52] Article 3(1) of the PDPA clearly provides that it 'shall not apply to the Federal Government and State Governments'.[53] Furthermore, Malaysia has neither signed nor ratified the ICCPR. In the absence of binding obligations imposed either nationally or internationally, the Government should take concrete steps to ensure that the use of MyTrace is consistent with the goal of controlling the pandemic.

3. Singapore

Singapore's contact tracing app, TraceTogether, was developed by the Government Technology Agency (GovTech) together with Singapore's Health Minister.

---

prohibitions-restrictions-under-indonesia-s-personal-data-protection-draft-law, accessed on 9 August 2020; 'Draft Data Protection Law in Indonesia', *Rödl & Partner,* p.1, available at https://www.roedl.net/fileadmin/user_upload/Roedl_Italia/Newsletters/Indonesian_Draft_Data_Protection_Law.pdf, accessed on 9 August 2020.

46 'MyTrace FAQ' (n 33).

47 Rashvinjeet S. Bedi, 'Data from Covid-19 app MyTrace kept on phone, not govt servers, says Khairy', *The Star*, 8 May 2020, available at https://www.thestar.com.my/news/nation/2020/05/08/data-from-covid-19-app-mytrace-kept-on-phone-not-govt-servers-says-khairy, accessed on 13 July 2020.

48 Ibid.

49 'Covid-19: 'MyTrace' app to help in contact tracing, says senior minister', *Malay Mail*, 3 May 2020, available at https://www.malaymail.com/news/malaysia/2020/05/03/covid-19-mytrace-app-to-help-in-contact-tracing-says-senior-minister/1862624, accessed on 13 July 2020.

50 *Laws of Malaysia. Act 709. Personal Data Protection Act 2010* (Malaysia PDPA), 2010, Malaysia.

51 Greenleaf, *Asian Data Privacy Laws* (n 23), pp. 324-329.

52 Ibid, p. 322.

53 Malaysia PDPA, art. 3(1).

TraceTogether is an open-source app shared under the GPL-3.0 open-source license.[54]

In terms of data privacy protection, Singapore is ahead of other ASEAN countries. Singapore enacted the PDPA in 2012, which took effect in January 2013.[55] It applies to all organizations that use, collect, or display Singaporean personal data, in or outside of Singapore. The PDPA established the Personal Data Protection Commission, which makes advisory guidelines that provide interpretation of the implementation of the PDPA.[56]

Despite having adequate data protection regulations, Singaporeans have expressed rejection towards TraceTogether. This can be seen from a petition, which now has more than 50,000 signatures, saying no to a wearable contact tracing device.[57] This rejection is further reflected by a survey which shows that 45% of respondents did not download TraceTogether.[58] These views arose due to past violations of data privacy in Singapore, such as the case in 2018 where a hacker managed to copy hospital record data of about 1.5 million patients.[59]

4. Philippines

StaySafe.Ph, Philippine's COVID-19 monitoring app, was developed by the Department of Health and Multisys Technology Corporation (Multisys). In addition to StaySafe. Ph, on 13 April 2020 the Department of Health (DOH) launched the DataCollect application, which collects data from hospitals and relevant stakeholders. This data will then be displayed on the COVID-19 Tracker website to provide relevant information about dissemination and prevention of COVID-19.[60] In Cebu, the provincial government mandated the use of the WeTrace app developed by Genii Hut Technologies Incorporated. Additionally, other contact tracing apps are also available within the Philippines.[61]

---

54 'Tech and Covid-19: open source needed for acceptance and success of contact tracing apps', *Information Age*, 28 April 2020, available at https://www.information-age.com/tech-covid-19-open-source-needed-contact-tracing-apps-acceptance-123489218/, accessed on 24 July 2020.

55 *The Personal Data Protection Act 2012 (Act 26 of 2012),* 2012, Singapore. See also Greenleaf, *Asian Data Privacy Laws* (n 23), p. 290.

56 'Singapore-Data Protection Overview', *OneTrust Data Guidance*, November 2019, available at https://www.dataguidance.com/notes/singapore-data-protection-overview, accessed on 25 July 2020.

57 Roxanne, 'People's rights infringed: Petition created to reject the use of wearable contact tracing device', *The Online Citizen*, 10 June 2020, available at https://www.onlinecitizenasia.com/2020/06/10/peoples-rights-infringed-petition-created-to-reject-the-use-of-wearable-contact-tracing-device/, accessed on 25 July 2020.

58 Dewey Sim and Kimberly Lim, 'Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?', *South China Morning Post*, 18 May 2020, available at https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether, accessed on 25 July 2020.

59 Ibid.

60 'DOH Launches New Covid-19 Tracker and Doh Datacollect App Press Release /13 April 2020', *Department of Health Kagawaran ng Kalusugan*, 13 April 2020, available at https://www.doh.gov.ph/doh-press-release/DOH-LAUNCHES-NEW-COVID-19-TRACKER-AND-DOH-DATACOLLECT-APP, accessed on 24 July 2020.

61 Gelo Gonzales, 'LIST: Coronavirus contact tracing apps in the Philippines', *Rappler*, 14 April 2020, available

Protection of personal data in the Philippines is regulated under Republic Act No. 10173 or the Data Privacy Act 2012 (DPA). The DPA regulates the processing of personal information, which is considered a fundamental right.[62] Philippines has also enacted the Implementing Rules and Regulations of the DPA (IRR). Both the DPA and IRR apply to the government and private sector.[63]

The Interagency Task Force (IATF) against COVID-19 has encouraged the signing of a tracing activity contract, the contents of which are based on the provisions of the PDPA.[64] The IATF also added that the Department of Information and Communications Technology and the National Privacy Commission should give certification to StaySafe.Ph to indicate that the app is technically feasible and complies with data privacy law.[65]

Nonetheless, concerns of data protection still arise because there is doubt that the DOH would have adequate personnel to run StaySafe.ph. Furthermore, citizens may not be able to download the app since around 20 million of the population still use mobile phones with 2G signals.[66] Several human rights and digital rights organizations have sent an open letter to the Philippine government calling for increased safeguards in the app. These safeguards are achieved by releasing the white paper and source code, and conducting human rights and privacy impact assessments, among others.[67]

5. Thailand

On May 28, 2020, Thailand launched its contact tracing app named Thai Chana - translated as 'Thailand wins'. Thai Chana allows authorities to monitor the movements of their communities so that medical personnel can identify the location of someone who is at risk of infection or identify places where new cases may spread. Users are required to scan QR codes with their mobile phones every time they enter or exit certain places.[68]

Before launching Thai Chana, the government encouraged the use of Mor Chana (Doctors win), which used Bluetooth and GPS to identify individuals who had come

at https://rappler.com/technology/features/coronavirus-contact-tracing-apps-philippines, accessed on 24 July 2020; Deepali Roy, 'Innovative apps support Philippines' fight against COVID-19', *Geospatial World*, 27 May 2020, available at https://www.geospatialworld.net/blogs/innovative-apps-support-philippines-fight-against-covid-19/, accessed on 24 July 2020.

62 *Republic Act 10173 – Data Privacy Act of 2012,* 2012, Philippines.

63 'Personal Data Protection in ASEAN' (n 41).

64 Gelo Gonzales (n 61).

65 Miguel R. Camus, 'StaySafe.ph developer: Trust issues hound contact tracing app', *inquirer.net*, 16 July 2020, available at https://technology.inquirer.net/100896/staysafe-ph-developer-trust-issues-hound-contact-tracing-app, accessed on 25 July 2020.

66 Ibid.

67 'Open Letter Request Strong Privacy Protection', *Association for Progressive Communications*, July 2020, available at https://www.apc.org/en/pubs/open-letter-request-strong-user-privacy-protections-philippines-covid-19-contact-tracing, accessed on 25 July 2020.

68 'Thai Covid-19 app raises privacy concerns', *UCA News*, 19 May 2020, available at https://www.ucanews.com/news/thai-covid-19-app-raises-privacy-concerns/88069, accessed on 25 July 2020.

in contact with patients infected with COVID-19.[69] Mor Chana is mainly used to help medical personnel pinpoint potential outbreaks of COVID-19 and mitigate its spread.[70]

Thailand's Ministry of Digital Economy and Society (DES) claimed that the launch of the aforementioned apps have taken into account relevant privacy policies and will follow privacy protection measures. Confidence in government efforts have resulted in more than 90% of Bangkok residents using Thai Chana.[71]

Thailand's data protection regulation is centered on the Personal Data Protection Act, B.E. 2562 (PDPA) enacted in May 2019 which replaced the Official Information Act (1997).[72] The PDPA aims to protect individual personal data and applies to both the private and public sectors.[73]

Unfortunately, the implementation of the PDPA was postponed until May 2021 by way of Royal Decree to Postpone the Personal Data Protection Act B.E. 2562 (2019). This delay was caused by the COVID-19 outbreak which has prevented almost all sectors from meeting the requirements contained within the PDPA.[74] On July 17, 2020, however, the Ministry of DES issued an interim Notification of Standards for Maintenance of Security of Personal Data.[75] This notification serves to fill the gap of data protection regulation until the PDPA comes into force in 2021 by setting minimum security standards for personal data.[76]

6. **Brunei**

On 16 May 2020, the Brunei Government launched its contact tracing app BruHealth following a statement to ease COVID-19 restrictions.[77] BruHealth requests its users to

---

69 'Thailand Launches Mor Chana Mobile App to Enhance Contact Tracing Efforts to Help Stop the Spread of Covid-19', *Big Chilli*, 13 April 2020, available https://www.thebigchilli.com/news/thailand-launches-mor-chana-mobile-app-to-enhance-contact-tracing-efforts-to-help-stop-the-spread-of-covid-19, accessed on 25 July 2020.

70 'Getting to Know Thai Chana "Platform"', *Bangkok Tribune*, 24 May 2020, available at https://bkktribune.com/getting-to-know-thai-chana-platform/, accessed on 25 July 2020.

71 'CRC is now available to download "Thai Win App"', *Ministry for Digital Economy and Society*, 28 May 2020, available at https://www.mdes.go.th/news/detail/2650-**ศบค--เปิดให้ดาวน์โหลด--แอปไทยชนะ--ได้แล้ววันนี**, accessed on 24 July 2020.

72 *The Personal Data Protection Act B.E. 2562,* 2019, Thailand. See also Greenleaf, *Asian Data Privacy Laws* (n 23), p. 357.

73 'Thailand Personal Data Protection Act', *Baker McKenzie*, 28 May 2019, available at https://www.bakermckenzie.com/en/insight/publications/2019/05/thailand-personal-data-protection-act, accessed on 27 July 2020.

74 Dhiraphol Suwanprateep, 'Postponement of Thailand's Personal Data Protection Act (PDPA)', *Lexology*, 13 May 2020, available at https://www.lexology.com/library/detail.aspx?g=c628a738-f929-4987-b6db-b0ee00e69b30, accessed on 25 July 2020.

75 'PDPA Update: Thailand Issues Security Standards for Personal Data', *Tilleke & Gibbins*, 30 July 2020, available at https://www.tilleke.com/resources/pdpa-update-thailand-issues-security-standards-personal-data, accessed on 30 July 2020.

76 'Delayed Implementation of Thailand's Personal Data Protection Act', *Hunton Andrews Kurth*, 29 May 2020, available at https://www.huntonprivacyblog.com/2020/05/29/delayed-implementation-of-thailands-personal-data-protection-act/, accessed on 30 July 2020.

77 'Launch of the BRUHEALTH Application', *Ministry of Finance and Economy*, 19 May 2020, available at

input their health conditions in order to be marked as one of five different colors, each with its own meaning regarding the user's health.[78] The answers given will be adjusted to the background of the individual concerned, such as if the individual has been admitted to the hospital in recent weeks. This app also equips a mandatory Bluetooth-based monitoring system.[79] If the user provides inaccurate information or turns off the Bluetooth, he/she will be charged with the Infectious Diseases Act.[80]

Although the Second Finance and Economy Minister stated that the government will pay attention to the security of BruHealth, and has cooperated with the relevant sectors to ensure no information breach occurs, concerns still arise considering Brunei does not have a comprehensive data protection law. Until now, data protection in Brunei is based on the 2014 Data Protection Policy.[81]

7. Vietnam

Bluezone, Vietnam's contact tracing app, was launched on 18 April, 2020. Bluezone was developed by the technology firm Bkav and Vietnam's Ministry of Information and Communications. Nguyen Tu Quang, CEO of Bkav, provided that the operation of Bluezone would be carried out transparently, paying attention to the importance of maintaining privacy.[82]

He stated that the data processed would be encrypted and stored in the user's own cell phone. In addition, Bluezone is an open-source app so that other countries can use it without fear of conflicting data processing.[83] The Vietnamese government has supported the use of Bluezone to help with containing COVID-19.[84]

Despite the steps taken to ensure security and transparency, Vietnam citizens cannot rely upon binding legislation since Vietnam does not have a comprehensive data protection law. Protection of personal data in Vietnam is spread over several different laws, one of which is the Law on Cyber Security 2018, which only focuses on giving the government authority to control the flow of information, not to protect personal data.[85] Without any

https://www.mofe.gov.bn/Lists/News/DispForm.aspx?ID=129, accessed on 25 July 2020.

78 Sareen Han, 'Gov't rolls out BruHealth contact tracing app as restrictions loosened', *The Scoo*p, 14 May 2020, available at https://thescoop.co/2020/05/14/govt-launches-bruhealth-contact-tracing-app/, accessed on 25 July 2020.

79 Ibid.

80 James Kon, 'Public urged to be honest with BruHealth app', *Borneo Bulletin*, 17 May 2020, available at https://borneobulletin.com.bn/2020/05/public-urged-to-be-honest-with-bruhealth-app/, accessed on 24 July 2020.

81 'Personal Data Protection in ASEAN' (n 41).

82 Ngoc Thuy, 'Vietnam Launches First Ever Contact-Tracing App to Curb Covid-19', *Hanoi Times*, 19 April 2020, available at hanoitimes.vn/vietnams-first-ever-contact-tracing-app-solves-similiar-apps-issues-information-minister-311800.html, accessed on 25 July 2020.

83 Ibid.

84 Ibid.

85 *Law on Cyber Security No: 24/2018/QH14*, 2018, Vietnam. See also 'Personal Data Protection in ASEAN' (n 41).

regulatory safeguards in place, nothing would bind the Vietnamese Government from abusing the technology and using it for purposes other than protecting public health.

B. The Ability of Contact Tracing Apps to Infringe upon the Right to Privacy

The right to privacy is regarded as a fundamental human right, recognized within domestic constitutions of countries all around the globe before being guaranteed by the international human rights framework.[86] One of the first instances of the international recognition for the right to privacy is Article 12 of the UDHR, which provides that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[87]

Article 17 of the ICCPR imposes a binding treaty obligation upon its state parties to guarantee the right to privacy. The wording of Article 17 reflects Article 12 of the UDHR except that Article 17 is divided into two paragraphs.[88] The right to privacy is also contained within regional human rights instruments, such as Article 8 of the European Convention of Human Rights (ECHR) and the aforementioned Article 21 of the AHRD.[89]

This section will place a focus upon the standard for the protection of the right to privacy established by the HRC and the European Court of Human Rights (ECtHR) since the ASEAN human rights framework as it stands, currently falls short compared to the extensive jurisprudence of the HRC and ECtHR. The standards established by the international human rights framework should guide countries implementing contact tracing apps so that the right to privacy is not unjustifiably infringed.

1. Scope of the Right to Privacy

'Privacy' is a sweeping concept, granting individuals the right to freedom from unwarranted and unreasonable intrusions into one's individual autonomy.[90] According

---

86 *Basic Law for the Federal Republic of Germany*, 1949, art. 10; *Constitution of Spain*, 1978, s. 18; *Constitution of the Federative Republic of Brazil*, 1988, art. 5(X); *The Constitution of The Republic of South Africa*, 1996, art. 14; Birutė Pranevičienė, 'Limiting of the Right to Privacy in the Context of Protection of National Security', *Jurisprudence* p. 1609, volume 18: 4, 2011, p. 1612; Oliver Diggelmann & Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right' *Human Rights Law Review* p. 441, volume 14:3, 2014, p. 441.

87 UDHR, art. 12.

88 ICCPR, art. 17.

89 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 3 September 1953, 213 UNTS 221, Rome, 4 September 1950 (ECHR), art. 8(1); AHRD, art. 21; See also *American Convention on Human Rights*, 18 July 1978, 1144 UNTS 123, San José, 22 November 1969, art. 11.

90 Sara Joseph & Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Materials, And Commentary*, Oxford University Press, UK, 3rd edition, 2013, pp. 533-534; See also Samuel D. Warren &

to Manfred Nowak, the scope of individual autonomy is 'the field of action [that] does not touch upon the liberty of others, where one may withdraw to shape one's life according to one's own (egocentric) wishes and expectations'.[91] This broad application of the term privacy has been adopted and applied by both the HRC and the ECtHR.[92]

One crucial aspect of the right to privacy is data protection. The HRC in its General Comment No. 16 and Concluding Observations has recognized that the right to privacy may be violated by the gathering and holding of personal information.[93] Regionally, the right to be free from unjustified interferences on personal data is explicitly guaranteed by Article 21 of the AHRD.[94] The ECtHR has, on multiple occasions, dealt with cases of data protection when interpreting state parties' obligations under Article 8 of the ECHR.[95] In *Rotaru v. Romania*, the ECtHR held that privacy encompasses public information that is systematically collected and held by the authorities.[96]

Therefore, even if users have consented to have their movements tracked by contact tracing apps, a violation of the right to privacy may still arise since it gives countries the ability to conduct the systematic collection and storage of personal data. If countries do not adhere to the conditions established by international human rights instruments, contact tracing apps may just be a stepping stone towards unlimited surveillance of individuals.

2. Obligation to Guarantee the Right to Privacy

Besides imposing a negative obligation upon member states to 'respect' the right to privacy, the aforementioned international instruments also impose a positive obligation upon state parties to 'protect' the right to privacy.[97] This is reflected in the second

Louis D. Brandeis, 'The Right to Privacy' *Harvard Law Review* p. 193, volume 4:5, 1890, pp. 213-216.

91 Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary*, NP Engel, Germany, 2nd edition, 2005, p. 378.

92 'Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights', *American Civil Liberties Union (ACLU)*, March 2014, pp. 12-4, available at https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf, accessed on 27 July 2020; 'Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence', *European Court of Human Rights*, 31 August 2019, para. 2, available at https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf, accessed on 26 July 2020.

93 General Comment No. 16 (n 13), para. 10; *Concluding Observations on France*, HRC, 31 July 2008, U.N. Doc. CCPR/C/FRA/CO/4, para. 22; *Concluding Observations on Spain*, HRC, 5 January 2009, U.N. Doc. CCPR/C/ESP/CO/5, para. 11.

94 AHRD, art. 21.

95 *Rotaru v. Romania*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2000, 5 European Court of Human Rights: Reports of Judgements and Decisions, Application no. 28341/95; *S. and Marper v. The United Kingdom*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2008, 5 European Court of Human Rights: Reports of Judgements and Decisions, Applications nos. 30562/04 & 30566/04, paras. 71-77; *M.M. v. The United Kingdom*, European Court of Human Rights, 2012, ECHR 1906, Application no. 24029/07.

96 Ibid, para. 43.

97 Ineta Zimele, 'Privacy, Right to, International Protection', *Max Planck Encyclopedias of International Law,* 2009, para. 2.

sentence of Article 12 of the UDHR, the second paragraph of Article 17 of the ICCPR and the second sentence of Article 21 of the AHRD.[98]

The HRC in its General Comment No. 16 reaffirmed that the obligations imposed by Article 17 require countries to adopt legislative and other measures to ensure that the right to privacy is protected.[99] According to the HRC, it is state legislation above all that must guarantee the protection of the right to privacy.[100] Although this positive obligation is not mentioned explicitly within the ECHR, the ECtHR has affirmed that there may be positive obligations, such as adopting measures to secure the right to privacy in the relations of individuals.[101]

In relation to contact tracing apps, it is not enough that countries only refrain from violating the right to privacy. Countries should also implement positive measures to ensure that the right to privacy is protected while using the app.

3. **Limitations upon the Right to Privacy**

The right to privacy guaranteed by the aforementioned international instruments is what is known as a qualified right, meaning that countries can justify interferences with the right as long as they are in accordance with the law, in pursuit of a legitimate aim and necessary in a democratic society.[102] To put it another way, the HRC in the case of *Van Hulst v. The Netherlands* held that any interference with the right to privacy must be in accordance with the conditions provided by Article 17(1).[103] The conditions are as follows: the interference must be provided for by law, be consistent with the purpose and objectives of the ICCPR and be reasonable in the particular circumstances of the case.[104] The aforementioned elements must be cumulatively met, meaning that even if the use of contact tracing apps meet the legitimate aim of securing the right to life in preventing the spread of COVID-19, if its implementation is not provided for by law, then it may still constitute a violation of the right to privacy.[105]

a. *Legitimate aim*

Most of the times where the right to privacy has been infringed, there exists competing

98 UDHR, art. 12; ICCPR, art. 17(2); AHRD, art. 21.

99 General Comment No. 16 (n 13), para. 1.

100 Ibid, para. 2.

101 *Evans v. The United Kingdom*, European Court of Human Rights, 2007, Judgment on Merits and Just Satisfaction, 1 European Court of Human Rights: Reports of Judgments and Decisions, Application no 6339/05, para. 75; *Lozovyye v. Russia*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2018, ECHR 361, Application no. 4587/09, para. 36.

102 'COVID-19: Human Rights Implications of Digital Contact Tracing Technology', *Scottish Human Rights Commission*, 18 May 2020, para. 11, available at https://www.scottishhumanrights.com/media/2028/contact-tracing-briefing-180520-final.pdf, accessed on 24 June 2020.

103 *Van Hulst v The Netherlands*, HRC, 2004, Communication no. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999, para. 7.3.

104 Ibid.

105 Ibid; Matisse Barbaro, 'Government Interference with the Right to Privacy: Is the Right to Privacy an Endangered Animal?', *Canadian Journal of Human Rights* p. 127, volume 6:1, 2017, p. 148.

interests at stake.[106] The roll-out of COVID-19 contact tracing apps is no exception. The competing interests at stake are the human right to privacy and the interest of preventing the spread of COVID-19. Any measures that interfere with the right to privacy must pursue a legitimate aim, that is the existence of a 'pressing social need'.[107]

Admittedly, the implementation of contact tracing apps by countries pursues the legitimate aim of controlling the spread of COVID-19, which is crucial to protecting the right to life guaranteed under Article 6 of the ICCPR.[108] Protecting public health in itself has been expressly included within the ICCPR and the ECHR as a legitimate interest to allow for restrictions of certain human rights, such as the right to privacy.[109] The urgency of these measures is reflected by the WHO's characterization of the disease as a pandemic in March of 2020.[110]

b. *In accordance with the law*

No interference with the right to privacy can take place except where it is in accordance with the law.[111] However, this does not provide governments with unlimited discretion in enacting law authorizing interference with the right to privacy. The law itself must be consistent with the aims and objectives of the ICCPR and be in compliance with public international law.[112] The law must be accessible to the public, foreseeable and specific in order to avoid abuse of power.[113]

Foreseeability requires the domestic law to allow individuals to adequately foresee the circumstances and conditions by which the authorities can justify measures interfering with their privacy, so that those individuals may act accordingly.[114] As for the

---

106 Pranevičienė (n 86), p. 1611. See also *Roche v. The United Kingdom*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2005, 5 European Court of Human Rights: Reports of Judgments and Decision, Application no. 32555/96, para. 157; *Hämäläinen v. Finland*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2014, 4 European Court of Human Rights: Reports of Judgments and Decisions, para. 65.

107 *Dudgeon v. The United Kingdom*, European Court of Human Rights, Judgment on Merits, 1981, 149 European Human Rights Reports, Application no. 7525/76, para. 51.

108 Lorna McGregor, 'Contact-tracing Apps and Human Rights', *EJIL:Talk!*, 30 April 2020, available at https://www.ejiltalk.org/contact-tracing-apps-and-human-rights/, accessed on 24 June 2020.

109 ICCPR, arts. 12(3), 19(3)(b), 21, 22; ECHR, art. 8(2); *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, UN Commission on Human Rights, 28 September 1984, U.N. Doc. E/CN.4/1985/4, paras. 25-26.

110 'Timeline of WHO's response to COVID-19, *WHO*, 30 July 2020, available at https://www.who.int/news-room/detail/29-06-2020-covidtimeline, accessed on 17 July 2020.

111 General Comment No. 16 (n 13), para. 2; *Halford v. The United Kingdom*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 1997, 523 European Human Rights Reports, Application no. 20605/92, para. 49.

112 General Comment No. 16 (n 13), para. 2; *Jorgic v. Germany*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2007, 3 European Court of Human Rights: Reports of Judgments and Decisions, Application no. 74613/01, paras. 67-68; *Kononov v. Latvia*, European Court of Human Rights, Judgment on Merits and Just Satisfaction, 2010, 4 European Court of Human Rights: Reports of Judgments and Decisions, Application no. 36376/04, para. 236.

113 *Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age*, U.N. Human Rights Council, 30 June 2014, U.N. Doc. A/HRC/27/37, paras. 28-29.

114 Ibid, para. 29. See also *Shimovolos v. Russia*, European Court of Human Rights, Judgment on Merits and Just

requirement of specificity, the HRC in *Van Hulst v. The Netherlands* held that authorities may only be permitted to interfere with one's right to privacy if it is based on legislation that specifies in detail, the precise circumstances to allow such interference.[115] ASEAN member states such as Malaysia have not met this standard, as it has not enacted any form of regulation to authorize the use of contact tracing apps.

c. *Proportionality*

In terms of assessing proportionality, three main issues are relevant: the degree of the interference; availability of less intrusive means; and the procedural safeguards.[116] The proportionality element is fulfilled when the measures interfering with the right to privacy are appropriate in order to meet the established legitimate aim and that the imposed measures are the least intrusive mechanisms of achieving the results.[117] The HRC in *Toonen v. Australia* held that in order to fulfill the reasonableness requirement, the interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.[118]

Firstly, as of now there is still a lack of evidence to support the effectiveness of contact tracing apps in preventing the spread of COVID-19.[119] The WHO has stated that the effectiveness of contact tracing apps depends heavily on the technology itself and how these apps are implemented.[120] Other factors must be taken into account, such as the amount of the population that needs to use the app in order for it to be effective.[121] Countries should conduct reviews to assess whether the trade-off to the user's privacy is proportional to the goal of preventing COVID-19 transmission, and if the results prove that the app has had no significant impact towards achieving the said goal, then the app must be dismantled immediately.[122]

Secondly, governments should use contact tracing apps in conjunction with other public health measures. Contact tracing apps are only effective when there already exists a robust public health system and pandemic response within the country since these apps only serve to provide data that health officials then use to manage and isolate confirmed cases.[123] A robust public health system and an effective pandemic response includes adequate health services personnel, testing services and an effective

Satisfaction, 2011, 6 European Court of Human Rights: Reports of Judgments and Decisions, Application no. 30194/09, para. 68.

115 *Van Hulst* (n 103), para. 7.7. See also *Pinkney v Canada*, HRC, 1977, Communication no. 27/1978, U.N. Doc. CCPR/C/14/D/27/1977, para. 34.

116 'COVID-19: Human Rights Implications of Digital Contact Tracing Technology' (n 102), para. 14.

117 *Van Hulst* (n 103), para. 7.6.

118 *Toonen v. Australia*, HRC, 1994, Communication no. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992, para. 8.3; See also *Raihman v Latvia*, HRC, 2010, Communication no. 1621/2007, U.N. Doc. CCPR/C/100/D/1621/2007, para. 8.3.

119 'Ethical considerations' (n 7), p. 2.

120 Ibid.

121 Ibid.

122 Ibid.

123 Ibid, p. 1.

manual contact tracing infrastructure.[124]

Countries such as Singapore, Vietnam and South Korea who have seen a significant decline in the spread of COVID-19 did not rely upon the use of that technology alone. The use of contact tracing apps was coupled with a strong initial response to the pandemic, for example implementing strict lockdowns, mass testing of the population and rapid manual contact tracing mechanisms.[125] The preemptive daily tracking of people's movements and mass storage of people's data by the government through the use of contact tracing apps, without an already robust public health infrastructure in place, would not appear to be the least intrusive measure to protect public health.[126]

Lastly, proportionality requires that measures that interfere with the right to privacy be limited in time, space and material scope.[127] Measures should be withdrawn and terminated once the emergency is over and shall be non-discriminatory in that it does not result in disparate impacts for minorities and vulnerable groups.[128] Safeguards must be put in place in order to avoid the misuse of data by governments and companies for purposes inconsistent with the legitimate aim sought.[129] The ECtHR in the case of *M.M. v. The United Kingdom* held that these safeguards may include, *inter alia*, the circumstances in which data can be collected, the duration of data storage, how the data will be used and the circumstances in which the data may be destroyed.[130]

Countries implementing contact tracing apps must implement safeguards and ensure that once the pandemic is over, the technology will be withdrawn and any data stored is deleted.[131] For example, the last paragraph of Indonesia's Ministerial Decree authorizing the use of its contact tracing app, PeduliLindungi, provides that PeduliLingdungi will only be used during the COVID-19 emergency.[132] It may be argued that this stipulation does not go far enough, as it only guarantees the termination of the use of PeduliLindungi but does not specify whether the data will be erased after the COVID-19 pandemic.

C. Data Protection Principles and Implementation for Contact Tracing Apps

The history of personal data protection began with the Guidelines on Transborder Data Flows and the Protection of Privacy adopted by the Council of the Organisation

124 Ibid.

125 Peter Beaumont, 'Coronavirus testing: how some countries got ahead of the rest', *The Guardian*, 2 April 2020, available at https://www.theguardian.com/world/2020/apr/02/coronavirus-testing-how-some-countries-germany-south-korea-got-ahead-of-the-rest, accessed on 27 July 2020.

126 *Siracusa Principles* (n 109), para. 11; Sacco et al. (n 12), p. 8.

127 Ibid, para. 51; Sacco et al. (n 12), p. 5.

128 Ibid.

129 *Concluding Observations on France* (n 93), para. 22; 'Joint civil society statement' (n 8).

130 *M.M.* (n 95), para. 199.

131 'Mobile Location Data and Covid-19: Q&A' (n 32).

132 MoCIT Decree No. 171, para. 5.

for Economic Co-operation and Development (OECD) in 1980.[133] This was followed by UN General Assembly Resolution 68/167 adopted in 2013[134] and then in the same year where OECD revised its guidelines to strengthen the existing framework. In 2015, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2005 was updated to adapt to the global scale of personal data usage.[135] These frameworks influenced the minimum standards of personal data protection in ASEAN member states. However, low standards of protection and unclear implementation provided by the OECD and APEC became the significant weaknesses of these frameworks.[136]

The next groundbreaking and legally binding step in data protection law was in 2016 when the European Commission enacted the General Data Protection Regulation (GDPR) to replace the 1995 Data Protection Directive. Although enforced within the scope of the EU, the GDPR has a strong global influence.[137]

Influenced by the increased multilateralism among countries, the GDPR applies extraterritorially.[138] This means that organizations located outside of the EU must meet the requirements of the GDPR if they want to process the personal data of EU citizens.[139] The requirements that must be implemented are the seven main principles of personal data protection.[140] Some experts even say that the GDPR is better than other global personal data protection efforts.[141]

The strong principles and clear guidelines contained within the GDPR emphasize its importance as the standard for robust protection of data privacy. The global impact of the GDPR is cemented by the fact that countries, even those with an already established data protection law, are borrowing the innovations of the GDPR to reassess and

133 Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy', *International Data Privacy Law* p. 6, volume 1:1, 2011, p. 6.

134 *The right to privacy in the digital age*, 18 December 2013, UNGA A/RES/68/167. See also 'Data Protection Regulations and International Data Flows: Implications for Trade and Development', *UNCTAD*, 2016, p. 24, available at https://www.tralac.org/images/docs/9500/data-protection-regulations-and-international-data-flows-implications-for-trade-and-development-unctad-april-2016.pdf, accessed on 25 July 2020.

135 Graham Greenleaf, 'Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories', *Journal of Law, Information and Science* p. 1, volume 23:1, 2014, p. 17. See also 'APEC Privacy Framework (2015)', *Asia-Pacific Economic Cooperation*, August 2017, available at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015), accessed on 30 July 2020.

136 Graham Greenleaf, 'Five years of the APEC Privacy Framework: Failure or promise?', *Computer Law and Security Report* p. 28, volume 25:1, 2009, p. 31; Ellyce R Cooper & Alan Charles Raul, 'APEC Overview', in Alan Charles Raul (ed.), *The privacy, Data Protection and Cybersecurity Law Review*, Law Business Research Ltd, London, 4th edition, 2017, p. 30; Prapanpong Khumon, 'Regulation for Cross-Border Privacy in Southeast Asia: An Institutional Perspective', *29th European Regional ITS Conference*, International Telecommunications Society, Trento, 2018, p. 2.

137 Pranaya Dayalu & M. Punnagai, 'GDPR: A Privacy Regime', *International Journal of Trend in Scientific Research and Development* p. 713, volume 3:4, 2019, p. 713.

138 Ibid, p. 715.

139 Jan Philipp Albrecht, 'How the GDPR Will Change the World', *European Data Protection Law Review* p. 287, volume 2:3, 2016, p. 288.

140 Dayalu & Punnagai (n 137), p. 713.

141 'Data protection Regulations and International Data Flows: Implications for Trade and Development' (n 134), p. 58; Beata A. Safari, 'Intangible Privacy Rights: How Europe's GDPR will Set A New Global Standard for Personal Data Protection', *Seton Hall Law Review* p. 809, volume 47:3, 2017, p. 811.

implement data protection regulations of their own.[142]

Unfortunately, the ASEAN Framework on Personal Data Protection lacks the key principles contained within the GDPR. ASEAN should follow the steps of countries around the world and look to achieve the same degree of data protection as that of the GDPR. This is especially true with contact tracing apps. Implementation of contact tracing apps must take into account the principles of personal data protection in order to avoid the abuse of personal data. This means that although the GDPR does not bind ASEAN member states, its principles described in the points below are crucial in achieving the comprehensive protection of personal data.

The seven key principles for processing personal data and the general steps for their fulfillment are as follows:

1. Lawfulness, fairness, and transparency

This principle requires that the processing of personal data must be lawful, fair and transparent. The validity of data processing is demonstrated by the existence of legitimate interests.[143] Fairness concerns whether the data taken is relevant for a particular purpose; and transparency concerns whether data subjects are aware of how their data is used.[144] To simply apply it, individuals subject to COVID-19 monitoring must be made aware of what data is gathered and how it will be used.

Lawfulness dictates that the processing of personal data must be clear and specific in order to be lawful. This is closely related to user consent.[145] In countries such as New Zealand and China, contact tracing apps are mandatory and have become a factor to the success in controlling the pandemic.[146] While other countries may not adopt this mandatory, the data gathered based on a user's consent must only be used for specific purposes. If along the line, this data would be used for other purposes, then the users must be asked for further consent.

Regarding transparency, data controllers must always use clear and plain language to

---

142 'Asia Pacific Data Protection and Cyber Security Guide 2018', *Hogan Lovells*, 2018, p. 4, available at https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2018/ab-data-protection-and-cybersecurity.pdf, accessed on 25 July 2020; 'Asia Pacific Data Protection and Cybersecurity Guide 2020' *Hogan Lovells*, 2020, p. 3, available at http://documents.jdsupra.com/2380c6d9-41fd-48bb-9f78-3fba5aa25e52.pdf, accessed on 25 July 2020. See also 'Personal Data Protection in ASEAN' (n 41).

143 *Regulation (EU) 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, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 25 May 2018, OJ 2016 L 119/1, Brussels, 27 April 2016 (GDPR), art. 6(1)(f).

144 Ibid, art. 5.

145 'Artificial Intelligence and Data Protection How the GDPR Regulates AI', *Center for Information Policy Leadership*, 2020, p. 5, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf, accessed on 25 July 2020.

146 'The case for the mandatory use of a COVID-19 tracing app', *Medical Brief*, 20 May 2020, available at https://www.medicalbrief.co.za/archives/the-case-for-the-mandatory-use-of-a-covid-19-tracing-app/, accessed on 26 July 2020.

convey how and for what data the data is being used.[147] One way this is achieved is by making the apps open source, which allows the public to see whether developers have adequate data protection systems in place. Monitoring user data processes is crucial for transparency, and data rights organizations are encouraging governments to make their contact tracing apps open source.[148]

2. Purpose limitation

Under this principle, personal data must be collected for specified and legitimate purposes and not processed further for incompatible purposes.[149] The legitimate purpose must be clearly stated from the beginning of the project, and data processing must be consistent with the initial purpose agreed upon by the subjects. Documentation is an important method to ensure that data processing remains in accordance with its original purpose.[150] The purpose of contact tracing apps is clear, which is to help governments and health officials to monitor and prevent the spread of COVID-19. However, there is a possibility that the data may be used for other purposes such as surveillance and law enforcement.[151]

It is crucial, then, that the use of contact tracing apps must be strictly limited by two main principles, namely necessity and proportionality.[152] These two principles dictate that an action must be appropriate to achieve a legitimate goal pursued and does not exceed the limits of what is appropriate and necessary to achieve those goals.[153]

3. Data minimization

This principle requires that minimum amount of data must be collected to meet the intended objective.[154] To identify whether an organization is storing the appropriate amount of data, it must clearly convey the reasons for storing that data. Storage of data must also be periodically checked to determine whether it is still relevant to its purpose, and if not, then any excessive data must be deleted.[155]

---

147 'Guide to the General Data Protection Regulation (GDPR)', *Information Commissioner's Office (ICO)*, 2018, p. 20, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, accessed on 24 July 2020.

148 Maikel Mardjan & Asim Jahan, 'Using Open Source for security and privacy protection', *Read the Docs,* 2015, available at https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/10-using-oss.html, accessed on 25 July 2020.

149 GDPR, art. 5(1)(b); Sumroy & Donovan (n 140), p. 5.

150 'Guide to the General Data Protection Regulation (GDPR)' (n 147), p. 21.

151 'Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak', *European Data Protection Board*, 2020 (Guidelines 04/2020), p. 7, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf, accessed on 25 July 2020.

152 Ibid.

153 'EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data', *European data Protection Supervisor*, 2019, available at https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en, accessed on 26 July 2020.

154 GDPR, art. 5(1) (c).

155 'Guide to the General Data Protection Regulation (GDPR)' (n 147), p. 27.

In the case of contact tracing apps, the organization is expected to only collect relevant data to confirm the user's health condition and location. The guidelines issued by the European Data Protection Board provide that contact tracing apps must not collect data that is irrelevant to the prevention of virus transmission, such as citizenship status, communication identifiers, device identifiers, equipment directory items, messages, and others.[156]

Under the GDPR, pseudonymization is an important aspect of increasing the security in data processing.[157] Pseudonymization makes it so that data cannot be used to identify individuals by replacing identifiable parameters with randomly generated identifiers.[158] In addition to pseudonymization, encryption and anonymization methods can also be used to prevent data from being identified.[159]

The decision to keep data on a centralized or decentralized server also needs to be considered when implementing contact tracing apps. The decentralization approach is considered to be the best way to fulfill the principle of data minimization compared to the centralized approach.[160] This approach allows users to have more control over their information by leaving it in their respective devices, whereas a central server where all the data is stored would be more susceptible to breaches. Vietnam and Malaysia have seemingly adopted the decentralized approach, stating that the data will be stored on user devices, not in a central database.[161]

4. Accuracy

Organizations must store and process data that is accurate and clear.[162] Data can be categorized as inaccurate if it is 'incorrect or misleading' to a fact.[163] This obligation requires giving an individual the right to rectify any incorrect data. Organizations must carry out reviews to ensure the accuracy of the data stored, and update it periodically.[164]

The accuracy of the data will have an impact on the effectiveness of contact tracing apps. Inaccurate data that shows a small number of infections will render these apps useless. Conversely, inflated numbers stemming from false positives could cause distrust of the effectiveness of contact tracing apps.

A research conducted by Nancy Ayer Fairbank and others provide that accuracy can be guaranteed by following two steps. First, data must be obtained by official health

156 'Guidelines 04/2020' (n 148), p. 9.

157 GDPR, art. 32(1) (a).

158 Nils Gruschka et al., 'Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR', *2018 IEEE International Conference on Big Data (Big Data)*, Institute for Electrical and Electronics Engineers, Seattle, December 2018, p. 2.

159 Ibid.

160 'COVID-19 Contact tracing: data protection expectations on app development', *International Commissioner's Office,* 2020, available at https://ico.org.uk/media/for-organisations/documents/2617676/ico-contact-tracing-recommendations.pdf, accessed on 26 July 2020.

161 Thuy (n 76).

162 GDPR, art. 5(1)(d).

163 Sumroy & Donovan (n 138), p. 5.

164 'Guide to the General Data Protection Regulation' (n147), p. 32.

sources and must be unique so that the data cannot be reused and modified.[165] The recommended design in this case is what has been used by Singapore's TraceTogether, which is to use authentication methods such as the QR Tag generator which can help health officials confirm the accuracy of data gathered. Second, users can reconfirm the accuracy of the data gathered by health officials, as is the case in Brunei's BruHealth.[166]

5. Storage limitation

Organizations are only allowed to store data for as long as the data is needed.[167] The organization that stores the data must also be able to justify storing the data. This principle also relates to an individual's right to delete data if the storing organization no longer requires the said data.[168]

Data gathered by contact tracing apps must only be used during the COVID-19 pandemic. The use of non-identifiable data may be stored for historical and research purposes, but must still pay attention to the rights of individuals concerned to ensure that information cannot be re-identified.[169] Indonesia, for example, has stated that user data will immediately be deleted once the pandemic is over.[170]

6. Integrity and confidentiality

Personal data must be processed in a manner that can guarantee its security. Safeguards must be in place to protect against, among others, unauthorized or unlawful processing, loss or damage to personal data.[171] To fulfill this principle, organizations must have adequate information governance and security policies and always review the latest security guidelines.[172] Data cannot be used for other processes or be shared with other parties without the data owner's knowledge.

An example of a violation of this principle is the sale of user data in the case of the *Office of the Privacy Commissioner for Personal Data v. Octopus* (Hong Kong, 2010).[173] Octopus, a provider of electronic payment smart cards in Hong Kong, was proven to

---

165 Nancy Ayer Fairbank et al., 'There's an App for That: Digital Contact Tracing and Its Role in Mitigating a Second Wave', *Berkman Klein Center for Internet & Society*, 2020, p. 25, available at https://cyber.harvard.edu/sites/default/files/2020-05/Contact_Tracing_Report_Final.pdf, accessed on 24 July 2020.

166 Ibid.

167 GDPR, art. 5(1) (e).

168 'Guide to the General Data Protection Regulation (GDPR)' (n 147), p. 40.

169 'Recommendations on Privacy and Data Protection in the Fight against COVID-19', *AccessNow*, 31 March 2020, available at https://www.accessnow.org/releases-recommendations-on-privacy-data-protection-covid-19/, accessed on 26 July 2020.

170 Cindy Mutia Annur, 'Kominfo Pantau Pasien Covid-19 Lewat 2 Aplikasi, Langgar Aturan Data?', *KataData*, 7 April 2020, available at https://katadata.co.id/desysetyowati/digital/5e9a41f600b4d/kominfo-pantau-pasien-covid-19-lewat-2-aplikasi-langgar-aturan-data, accessed on 24 July 2020.

171 GDPR, art. 5(1) (f).

172 Sumroy & Donovan (n 143), p. 6.

173 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (n 134), p. 17.

sell user data without approval.[174] This type of misconduct is a serious violation, and governments must ensure that the same mistakes do not occur when using contact tracing apps.

7. Accountability

Under this principle, the data controller must be responsible and must be able to demonstrate compliance with the other six principles.[175] Organizational accountability can be demonstrated in several ways, such as by record keeping, appointing data protection officers, and carrying out a Data Protection Impact Assessment or Privacy Impact Assessment (PIA).[176]

When processing data on the reason of public interest, it is strongly recommended that a PIA is conducted.[177] A PIA is a process in which an organization or government identifies the risk of processing user data so that later it can minimize adverse impacts to the user's privacy.[178] Under the PIA, the government not only evaluates the application system, but must also consult with relevant internal and external stakeholders.[179]

In countries such as the Philippines where several COVID-19 mitigation apps are available, the government is required to take appropriate actions to be able to control user data. Using a single app managed by the government would more easily guarantee accountability since there would be less apps to manage.[180] This single app system will also have an impact on the app's effectiveness, given that governments have more influence than private developers.[181]

D. Recommendations

While contact tracing apps may become a useful tool to assist efforts to contain the COVID-19 pandemic, countries should be aware of how the technology may impact human rights and personal data protection.

From the explanation provided in the above sections, it seems that most ASEAN member states have not met the international standards for the protection of the right

174 'Octopus sold personal data of customers for HK$44m', *South China Morning Post*, 27 July 2010, available at https://www.scmp.com/article/720620/octopus-sold-personal-data-customers-hk44m, accessed on 26 July 2020.

175 GDPR, art. 2.

176 Sumroy & Donovan (n 143), p. 6.

177 Ibid.

178 'Conducting privacy impact assessments code of practice', *International Association of Privacy Professionals*, 2014, p. 4, available at https://iapp.org/media/pdf/resource_center/ICO_pia-code-of-practice.pdf,accessed on 26 July 2020.

179 David Wright, 'A Comparative Analysis of Privacy Impact Assessment in Six Countries', *Journal of Contemporary European Research* p. 161, volume 9:1, 2013, pp. 161-163.

180 'Guidelines 04/2020' (n 151), p. 9.

181 Fairbank et al. (n 165), pp. 35-37.

to privacy and personal data when implementing contact tracing apps. For countries to rectify these missteps and adhere towards their obligations, or for those countries planning to implement contact tracing apps in the future, the following conditions must be met:

1. Based on law: The use of contact tracing apps must be authorized by laws that are specific and foreseeable.[182] Said authorization must be based on the State's legislation to ensure legal clarity and certainty as to what data is gathered, as well as how the data could be used and where it is stored.[183]

2. Voluntariness: The implementation of contact tracing apps must not be mandated by the Government and must be voluntary. States must ensure that individuals are not denied access to services or benefits for refusing to use contact tracing apps, including access to health services or economic aid during the pandemic.[184]

3. Limitation: The collection and storage of user data must be limited by the need to control the COVID-19 pandemic. The data that is collected must be limited in scope, its storage time-bound in relation to the pandemic and the data must not be repurposed for means other than protecting public health.[185] Access to user data must be limited to health officials only, and the data must be deleted immediately once the COVID-19 pandemic has been contained.[186]

4. Safeguards: States must put in place safeguards to ensure that the data collected by contact tracing apps is not abused and/or appropriated for any uses other than controlling the spread of COVID-19. User data must not fall into the hands of public or private entities that would use the data for surveillance/commercial purposes.[187]

5. Transparency: States must guarantee that sufficient information is provided so that individuals are able to fully comprehend the scope, nature and application of contact tracing apps.[188] This could include releasing the source code of the contact tracing apps as well as publishing reviews regarding the effectiveness of contact tracing apps in combating the spread of COVID-19.[189]

6. Oversight: States must establish an independent body to oversee multiple aspects of the implementation of contact tracing apps, including its effectiveness and

---

182 'Human Rights and the Government's Response to Covid-19: Digital Contact Tracing', *United Kingdom Parliament Joint Committee on Human Rights*, 6 May 2020, United Kingdom, para. 21(a).

183 Mark J. Taylor & Tess Whitton, 'Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data', *Laws*, volume 9:1, 2020, p. 2.

184 'Ethical considerations' (n 7), p. 3.

185 'Joint civil society statement' (n 8).

186 'Guide to the General Data Protection Regulation (GDPR)' (n 147), p. 40.

187 'Recommendations on Privacy and Data Protection in the Fight against COVID-19' (n 169).

188 'Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance', *Electronic Frontier Foundation*, May 2014, available at https://necessaryandproportionate.org/principles/, accessed on 2 August 2020.

189 Open Letter to KOMINFO (n 38).

privacy protections.[190] The independent body must be provided with sufficient resources along with the necessary enforcing powers to effectively carry out their functions.

7. Remedy: States must provide the opportunity and mechanism for individuals to challenge measures related to contact tracing apps that are inconsistent with the right to privacy and the principles of personal data protection.[191]

8. Non-discrimination: States must ensure that contact tracing apps do not further exacerbate existing inequalities by guaranteeing that the implementation of these apps does not impact vulnerable or disadvantaged groups disproportionately.[192]

III. Conclusion

The COVID-19 pandemic warrants a swift and effective response by governmental authorities if they hope to contain its spread and reduce its drastic socio-economic impacts. Contact tracing has proven in many different countries to become a crucial method in stopping the spread of COVID-19. These efforts have been supported by the implementation of contact tracing apps. This technology has been proven to be popular among countries, with 7 out of 10 ASEAN countries having their own contact tracing app available for its citizens.

While contact tracing apps may be useful, we must not let the COVID-19 pandemic become a turning point leading towards unlimited government surveillance and the degradation of the right to privacy. In light of such concerns, countries must adhere to the standards of lawfulness and non-arbitrariness imposed by international human rights law when implementing contact tracing apps. Furthermore, user data must at all times be protected in accordance with the widely known general data principles. This can be done through the enactment and effective enforcement of a comprehensive domestic personal data protection act.

The implementation of contact tracing apps has ignited a much-needed debate on the data protection framework within ASEAN. As previously mentioned, currently there exists no binding regulatory framework within ASEAN that guarantees the right to privacy and guarantees the protection of personal data. This has resulted in the high variance of the degree of personal data protection within ASEAN member countries, which has far-reaching implications towards the protection of the right to privacy. It is highly desirable that a binding ASEAN General Data Protection Regulation is created similar to the EU GDPR. The urgency is clear, as countries are increasingly reliant upon digital technology to provide innovative solutions for different pressing matters such as the COVID-19 pandemic.

---

190 United Kingdom Parliament Joint Committee on Human Rights (n 182), para. 21(b).

191 Madan Lal Bhasin, 'Challenge of Guarding Online Privacy: Role of Privacy Seals and Government Regulations', *Palgo Journal of Business Management* p. 59, volume 3:2, 2016, pp. 67-69.

192 'Mobile Location Data and Covid-19: Q&A' (n 32). See also *Privacy in the Digital Age* (n 113), para. 28.