Jurnal Kepastian Hukum dan Keadilan
P-ISSN: 2721-0545, E-ISSN: 2722-3604 Volume 2 Nomor 1, Desember 2020

PERLINDUNGAN DATA PRIVASI DI INDONESIA DAN SINGAPURA TERKAIT PENERAPAN DIGITAL CONTACT TRACING SEBAGAI UPAYA PENCEGAHAN COVID-19 SERTA TANGGUNG JAWABNYA

Tiara Almira Raila*

Sinta Dewi Rosadi

Rika Ratna Permata

Fakultas Hukum Universitas Padjadjaran

tiaralmirail@gmail.com, sinta@unpad.ac.id, permata_rika@yahoo.com

ABSTRACT

COVID-19 has hit the world and Indonesia is one of the countries affected. Regarding the prevention of the spread of the virus, Indonesian Government has made efforts, one of which is by implementing digital contact tracing using mobile applications. In practice, the mobile contact tracing app collects a person's personal data (such as person's full name, Identity Number (NIK), personal phone number and personal e-mail), against these collected datas, there is a potential that these datas can be used improperly and that there is an offence against the personal data itself. Through this paper, using the normative juridical method, the author will look for Indonesian positive legal provisions that foster matters relating to personal data that will be applied with the application of digital contact tracing, one of which uses the application and this paper will also conduct a similar study in Singapore as the first country to implement digital contact tracing through the application and as a neighboring country to Indonesia. In this examination, we will first see whether the application of digital contact tracing in Indonesia using existing applications is in accordance with the principles regarding personal data. Based on the research results, the application of digital contact tracing in Indonesia which uses applications, violate the principles related to personal data. Regarding the regulation of personal data in Indonesia in particular, it is still limited to a ministerial regulation. Unlike Singapore, it has guaranteed the protection of people's personal data through the Personal Data Protection Act and the Public Sector Governance Act 2018 and regarding the responsibility for personal data, in Indonesia, it is still limited to administrative sanctions, while in Singapore, it is up to criminal liability.

***Keywords**: Data Privacy; Contact Tracing Apps; Digital Contact Tracing; COVID-19*

ABSTRAK

Virus COVID-19 sedang menjadi perhatian utama dunia hingga saat ini. Terkait pencegahan penyebarannya, Pemerintah Indonesia melakukan beberapa upaya, salah satunya dengan menerapkan *digital contact tracing* menggunakan aplikasi pelacakan. Pada pelaksanaannya, aplikasi pelacakan (*contact tracing)* mengumpulkan data pribadi seseorang (seperti nama lengkap, NIK, nomor telepon pribadi dan e-mail pribadi), yang sangat berpotensi akan terjadinya pelanggaran data pribadi. Selain menggunakan aplikasi pelacakan, metode *digital contact tracing*

juga kerap dilakukan oleh pihak swasta dengan penginputan data pengunjung pada *public places*. Melalui tulisan dengan metode yuridis normatif ini, penulis akan membahas ketentuan hukum perihal data pribadi yang akan dihubungkan dengan penerapan *digital contact tracing*. Penulis juga akan melakukan kajian serupa pada negara Singapura, sebagai negara pertama yang menerapkan *digital contact tracing* melalui aplikasi pelacakan dan sebagai negara tetangga Indonesia. Penulisan ini terlebih dahulu akan melihat apakah penerapan *digital contact tracing* di Indonesia dengan aplikasi pelacakan yang ada, telah sesuai dengan prinsip-prinsip perlindungan data pribadi. Berdasarkan hasil penelitian, penerapan *digital contact tracing* di Indonesia dengan aplikasi pelacakan melanggar beberapa prinsip terkait data pribadi. Peraturan data pribadi di Indonesia sendiri secara khusus masih sebatas peraturan menteri. Berbeda dengan Singapura, telah menjamin perlindungan data pribadi masyarakatnya melalui Personal Data Protection Act dan Public Sector Governance Act 2018, dan mengenai tanggung jawab pada data pribadi, di Indonesia masih sebatas sanksi administratif, sementara di Singapura, sampai pada pertanggungjawaban pidana.

Kata Kunci: Data Privasi; Aplikasi *Contact Tracing*; Digital *Contact Tracing*; COVID-19

A. PENDAHULUAN

Saat ini dunia sedang mengalami pandemi global *(global pandemic)* dari *the novel coronavirus* (COVID-19). Indonesia menjadi salah satu yang ikut terdampak pandemi ini dan akan mengalami pandemi ini dalam jangka waktu yang lebih lama, karena penduduknya yang padat.[1] Karena itulah, seperti disebutkan sebelumnya, penting untuk mengatasi penyebaran virus COVID-19 ini.

Pemerintah Indonesia sendiri telah melakukan beberapa upaya. Salah satunya mengembangkan aplikasi seluler "PeduliLindungi" yang dikeluarkan oleh Kementerian Komunikasi dan Informasi bekerja sama dengan Kementerian Badan Usaha Milik Negara (BUMN). Aplikasi lokal ini membantu upaya pemerintah dalam melacak kasus pasien yang telah dikonfirmasi terinfeksi COVID-19 sekaligus orang-orang yang dicurigai terinfeksi di seluruh negeri. Penggunaan aplikasi ini bersifat suka rela. Selain dengan aplikasi, *digital contact tracing* juga dilakukan dengan penginputan data pengunjung di tempat-tempat umum, seperti di mal, restoran, dan perkantoran oleh perusahaan atau swasta yang bersangkutan. *Contact Tracing* itu sendiri diartikan sebagai proses pelacakan kontak dengan mengevaluasi riwayat lokasi pengguna.[2]

Mengenai aplikasi yang diluncurkan Pemerintah Indonesia, yakni PeduliLindungi, cara kerjanya yaitu dengan melakukan referensi silang data yang tersimpan di perangkat

[1] Zhang Jane, "ADB approves $3 million grant to support Indonesia's fight against COVID-19",https://www.adb.org/news/adb-approves-3-million-grant-support-indonesias-fight-against-covid-19, diakses pada 9 September 2020

[2] European Centre for Disease Prevention and Control, *Mobile applications in support of contact tracing for COVID-19 – A guidance for EU/EEA Member States*, Stockholm: ECDC; 2020.

seluler penggunanya melalui koneksi *bluetooth.* Ketika pengguna berada di sekitar pengguna lain yang datanya telah diunggah ke PeduliLindungi, aplikasi memungkinkan pertukaran identitas secara anonim. Jika pengguna ditemukan berada di dekat kasus dugaan yang dikonfirmasi dalam pengawasan, aplikasi akan mengidentifikasi mereka. Fitur seperti ini diharapkan dapat membantu pelacakan kontak dan pelacakan kasus.[3]

Penggunaan aplikasi seperti ini sebenarnya dapat membantu upaya pencegahan penyebaran virus COVID-19, sekaligus membantu pemerintah dalam mengidentifikasi orang-orang yang punya kemungkinan terjangkit virus tersebut. Namun di sisi lain, muncul pertanyaan bagaimanakah jaminan keamanan data-data pengguna aplikasi di atas. Secara khusus, terdapat risiko sistem disalahgunakan atau adanya potensi serangan oleh peretas yang memiliki kemampuan tertentu untuk menyalahgunakan data-data pribadi tersebut.[4]

Secara umum data pribadi diartikan sebagai informasi yang sangat pribadi yang disimpan untuk diri sendiri, atau setidaknya hanya diketahui oleh orang-orang secara terbatas. Data pribadi itu sendiri adalah bagian dari hak seseorang dalam mengawasi akses informasi tentang kehidupan pribadi dan data miliknya.[5] Sangatlah esensial dan krusial untuk suatu data pribadi itu dijaga kerahasiaannya. Permasalahan terhadap data pribadi akan muncul saat kerahasiaan suatu data pribadi tidak dapat terlindungi sehingga rentan disalahgunakan secara melawan hukum[6]. Alasan krusial lain mengapa data pribadi harus dijaga dan dilindungi karena data pribadi merupakan bagian dari aspek privasi seseorang.

Perihal hak privasi sebenarnya telah dicantumkan dalam beberapa peraturan di Indonesia. Terutama dalam Undang-Undang Dasar 1945, pada Pasal 28 G ayat (1) yang walaupun tidak secara eksplisit menjelaskan mengenai data privasi, namun pasal ini tetap menyangkut kebebasan individu untuk menyimpan informasi dan pelindungan data dan informasi yang melekat pada dirinya.

Untuk konsep dasar dari perlindungan data privasi itu sendiri disajikan pada tahun 1890 dalam *the right to* privacy yang diperkenalkan oleh Samuel D. Warren dan Brandeis dalam *Harvard Law Review*. Privasi merupakan sesuatu yang melekat pada diri manusia

[3] Aplikasi PeduliLindungi untuk Melacak COVID-19 Sudah Bisa Diunduh, https://tekno.kompas.com/read/2020/03/29/18020057/aplikasi-peduli-lindungi-untuk-melacak-covid-19-sudah-bisa-diunduh?page=all, diakses pada 9 September 2020

[4] Koustubh "K.J." Bagchi, et.al. Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns, COVID-19 Rapid Response Impact Initiative, *White Paper 22*, hlm. 30

[5] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Penjelasan Pasal 26 ayat (1) huruf a, b, dan c

[6] Sinta Dewi Rosadi, Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia, *Jurnal Yustisia*. Vol.5 No.1 Januari - April 2016, hlm.26

sebagai individu. Privasi pun juga bisa berarti hak seseorang untuk memiliki *space* di mana ia dapat dibiarkan sendiri, di mana tidak ada orang lain yang memiliki akses kecuali mereka diizinkan untuk mengaksesnya. Frasa "dibiarkan sendiri" dimaksudkan untuk tidak disentuh dan dalam konteks privasi berarti tidak untuk dilihat dengan cara apapun. Privasi adalah kemampuan untuk menjadi diri sendiri.[7] Privasi adalah bagian dari Hak Asasi Manusia (HAM).

Mengenai penggunaan aplikasi pelacakan dalam upaya pencegahan COVID-19, ada beberapa negara lain yang menggunakan aplikasi pelacakan sejenis, salah satunya Singapura. Singapura merupakan negara pertama yang menerapkan *digital contact tracing* menggunakan aplikasi pelacakan. The GovTech Singapore, bersama dengan Kementerian Kesehatan Singapura, telah meluncurkan aplikasi seluler "TraceTogether". Aplikasi PeduliLindungi yang diluncurkan oleh pemerintah Indonesia sebenarnya banyak mengadopsi fitur-fitur dari aplikasi TraceTogether dari Negeri Singa ini. Aplikasi TraceTogether itu sendiri bekerja saat para pengguna ponsel (yang mengunduh aplikasi ini) berdekatan satu sama lain. Pada saat itulah mereka akan bertukar informasi menggunakan *bluetooth s*ecara anonim. Informasi ini disimpan di ponsel, dan hanya dibagikan pada kementerian Kesehatan (MOH) jika pengguna dinyatakan positif COVID-19. Aplikasi akan menghentikan fungsionalitasnya pada akhir wabah.[8] Salah satu fitur aplikasi TraceTogether juga termasuk SafeEntry yang digunakan ketika pengunjung hendak mengunjungi *public places* di Singapura, di mana data-data pada aplikasi TraceTogether akan ter-*transfer* secara otomatis ketika pengunjung men-*scan barcode* dari aplikasi tersebut pada SafeEntry. Sebenarnya tidak hanya dengan SafeEntry, perusahaan dapat memilih platform lain juga untuk upaya *digital contact tracing,* sama seperti halnya di Indonesia.

Jadi, berkenaan dengan penerapan *digital contact tracing,* selain menggunakan aplikasi, pemerintah di banyak negara, termasuk di Indonesia dan Singapura, telah menginstruksikan perusahaan untuk mencatat detail kontak pengunjung (seperti di restoran, hotel. kedai kopi, pub, dan klub malam) untuk upaya pengujian dan penelusuran kasus COVID-19 seperti yang telah dijelaskan sebelumnya. Pencatatan ini dilakukan dengan meng-input data pribadi para pengunjung pada suatu aplikasi atau *platform* yang digunakan oleh perusahaan itu.[9]

---

[7] Warren dan Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review, Vol. IV, No. 5,* Desember 1890, hlm. 193

[8] "How Does The Trace Together App Work", https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473-How-does-the-TraceTogether-App-work-, diakses 26 September 2020

[9] "Contact Tracing: Why Some People Are Giving False Contact Details To Bars and Restaurants"https://theconversation.com/contact-tracing-why-some-people-are-giving-false-contact-details-to-bars-and-restaurants-143390, diakses pada 16 November 2020.

Kembali pada penerapan *digital contact tracing* dengan aplikasi pelacakan, dalam penggunaan aplikasi pelacakan di Indonesia (PeduliLindungi) harus diperhatikan kesesuaian dengan prinsip-prinsip penggunaan data pribadi itu sendiri. Perlu juga dilihat bagaimana perlindungan dan tanggung jawab yang dapat diberikan manakala terjadi pelanggaran terhadap data pribadi tersebut. Pengkajian mengenai perlindungan dan tanggung jawab ini akan dilakukan pada kedua negara yaitu Indonesia dan Singapura sebagai negara tetangga Indonesia.

Di Indonesia, regulasi terkait data pribadi dan hak privasi seseorang terdapat pada konstitusi Indonesia seperti yang telah dicantumkan sebelumnya, dan diatur juga dalam 1 pasal pada Undang-Undang Nomor 19 tahun 2016 yang berisi Perubahan Atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 26. Pasal 26 UU ITE ini mengatur bagaimana setiap informasi elektronik yang mengandung data pribadi itu hanya boleh digunakan atas seizin orang tersebut. Terdapat juga Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Untuk pengaturan khususnya masih sampai pada Peraturan Menteri saja yakni Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Privasi dalam Sistem Elektronik. Sementara, di Singapura, mengenai Perlindungan Data Pribadi telah diberikan jaminan pada Undang-Undang yaitu Personal Data Protection Act 2012 yang baru saja diamandemen pada 2020, serta Public Sector Governance Act 2018.

Di Indonesia, hingga kini belum ada hukum spesifik tentang perlindungan privasi dan data pribadi.Karena itu, seiring teknologi yang berkembang pesat saat ini, hukum untuk perlindungan privasi dan data pribadi menjadi semakin urgen dibutuhkan. Hukum yang ada dinilai belum efektif, terutama dalam mengikuti perkembangan pemanfataan teknologi itu sendiri.[10] Untuk melihat sampai manakah perlindungan data privasi di Indonesia, tulisan ini akan mencoba mengkaji peraturan-peraturan yang sudah ada. Sebagai *benchmark,* akan juga dilihat Singapura, bagaimana Negeri Singa itu memberi jaminan perlindungan data privasi pada masyarakatnya, terutama dikaitkan dengan penerapan *digital contact tracing* dalam pencegahan COVID-19 serta anggung jawab seperti apa yang diberikan manakala terjadi pelanggaran data pribadi pada penerapan *digital contact tracing*. Sebelumnya juga akan dikaji tentang kesesuaian penggunaan aplikasi pelacakan di Indonesia (PeduliLindungi) dengan prinsip-prinsip data pribadi yang ada.

[10] Sinta Dewi Rosadi, Op.Cit., hlm. 27

Rumusan Masalah

Berdasarkan uraian latar belakang masalah, berikut beberapa identifikasi masalah yang diangkat dalam penelitian ini:

1. Apakah penerapan *digital contact tracing*, khususnya pada aplikasi pelacakan di Indonesia, telah memenuhi prinsip-prinsip perlindungan data pribadi?
2. Bagaimana perlindungan data privasi di Indonesia dan Singapura terkait Penerapan Digital Contact Tracing sebagai upaya pencegahan Covid-19 serta tanggung jawabnya?

Metode Penelitian

Pendekatan tulisan ini adalah yuridis normatif. Dikenal juga sebagai *doctrinal research*, pendekatan jenis ini dilakukan dengan menelaah teori-teori, prinsip-prinsip, serta peraturan perundang-undangan, seperti UU ITE, PP No. 71 Tahun 2019 tentang PSTE, Permenkominfo, dan untuk yang di Singapura yaitu Personal Data Protection Act 2020 dan Public Sector Governance Act 2018.

B. PEMBAHASAN

1) Kesesuaian Penerapan *Digital Contact Tracing* sebagai Upaya Pencegahan COVID-19 Khususnya dengan Menggunakan Aplikasi Pelacakan (PeduliLindungi) dengan Prinsip-Prinsip Data Pribadi.

Pada penggunaan aplikasi pelacakan di Indonesia (PeduliLindungi), sebelum menjadi partisipan pada aplikasi tersebut, pengguna diharuskan melakukan registrasi dengan memasukan nama lengkap dan nomor telepon pribadi. Setelah pengguna melakukan registrasi, akan muncul "Syarat dan Ketentuan" yang meliputi definisi dari Peduli Lindungi, cara kerja PeduliLindungi, sampai dengan kebijakan kerahasiaan data Peduli Lindungi.

Pada bagian ketentuan mengenai Kebijakan Kerahasiaan Data PeduliLindungi, disebutkan bahwa data yang disimpan pada penyimpanan data meliputi nomor HP, user ID dan lokasi dan waktu saat terjadi pertukaran data. Data-data ini disebutkan disimpan secara aman dan tidak dibagikan ke publik. Namun, informasi pada aplikasi PeduliLindungi tidak menjelaskan siapa pihak yang dapat mengakses dan mengolah data yang bersangkutan. Dan sebenarnya, seaman-amannya sistem elektronik, tidak ada yang 100% aman. [11] Pada bagian

[11] Eugene H. Spafford, Security models for web-based applications, *Communications of the ACM*, Volume 44 , Issue 2 , 2001, hlm. 38.

P-ISSN: 2721-0545, E-ISSN: 2722-3604 Volume 2 Nomor 1, Desember 2020

"Kebijakan" PeduliLindungi dijelaskan bahwa aplikasi ini mengumpulkan data dari perangkat *(storage)* pengguna, seperti dijelaskan sebelumnya pada pendahuluan.

Lebih lanjut, saat pengguna telah menyetujui untuk menggunakan aplikasi dan telah melakukan registrasi, baru didapati bahwa ada keharusan untuk meng-*input* data pribadi lainnya, seperti Nomor Induk Kependudukan (NIK) dan *e-mail* pribadi untuk keperluan *contact tracing*. Jadi bukan hanya nomor telepon dan nama lengkap. Untuk hal ini, akan dilakukan analisis terkait kesesuaian penerapan aplikasi ini dengan prinsip-prinsip data pribadi, seperti yang ada pada GDPR, Pasal 5, sebagai berikut:[12]

a) Keabsahan, Keadilan, dan Transparansi

   Data harus diolah secara sah, adil, dan transparan.

b) Pembatasan Tujuan

   Setiap pengumpulan data pribadi harus memiliki tujuan yang jelas, eksplisit, dan sah dengan penggunaan terbatas.

c) Minimalisasi Data

   Penggunaan data pribadi harus relevan dan terbatas yang diperlukan sesuai dengan tujuannya.

d) Akurasi

   Setiap data harus akurat. Ini berarti setiap data yang sudah usang perlu segera dihapus atau diperbaiki.

e) Pembatasan Penyimpanan

   Penyimpanan data harus dalam mudah diakses oleh pemilik data.

f) Integritas dan Kerahasiaan

   Data pribadi harus dijamin keamanannya dan dilindungi oleh hukum ketika terjadi kehilangan, penghancuran, atau kerusakan yang tidak disengaja.

Jika dilihat, pengguna PeduliLindungi sebenarnya tidak menerima informasi mengenai data-data yang akan diproses ataupun diolah pada aplikasi. Untuk itu, dapat dikatakan bahwa aplikasi ini telah melanggar prinsip transparansi pengolahan data pribadi dikarenakan pengguna tidak menerima informasi secara eksplisit mengenai data-data yang digunakan ataupun dikumpulkan dan cara pengolahannya. Seharusnya aplikasi ini transparan kepada penggunanya.

Dengan dikumpulkannya data dari *storage* HP pengguna, prinsip minimalisasi data serta prinsip pembatasan tujuan juga telah dilanggar. Karena sebenarnya tidak terdapat

[12] General Data Protection Regulation, Pasal 5

urgensi dan tujuan yang jelas untuk melakukan pengumpulan data tersebut. Fungsi dari aplikasi ini untuk membantu pemerintah melakukan *contact tracing* yang sebenarnya tidak memerlukan pengumpulan data dari *storage* HP pengguna. Dengan cara ini terdapat risiko sangat besar pengguna dirugikan. Contoh, bila terjadi kebocoran data ataupun kegagalan dalam proteksi data pribadi pada aplikasi atau pada HP pengguna. Terdapat juga ancaman akses illegal oleh *hacker* untuk menyalahgunakan data pribadi tersebut. Mengingat banyaknya data pribadi pada HP pengguna yang bila bocor pada publik, akan sangat merugikan. Berdasarkan rekapitulasi dari Lembaga Riset Siber Indonesia (CISSRec), kondisi keamanan siber Indonesia pun masih relatif memprihatinkan. Pada 2019, mereka mencatat ada 88 juta serangan terhadap sistem keamanan di Indonesia. Jumlah ini meningkat belasan kali lipat ketimbang tahun sebelumnya.[13] Jadi perlu diingat sebenarnya tidak ada yang bisa betul menjamin keamanan data itu sendiri.

Kembali pada masalah keamanan data pengguna PeduliLindungi, dijelaskan bahwa data yang disimpan aman dalam format terenkripsi itu tidak akan dibagikan kepada orang lain dan hanya akan diakses apabila pengguna dalam risiko tertular Covid-19 dan perlu segera dihubungi oleh petugas kesehatan."[14] Kembali lagi, aplikasi PeduliLindungi sebenarnya tidak menjelaskan siapa pihak yang mengakses dan mengolah data para pengguna. Pada aplikasi juga sebenarnya dikatakan bahwa Pemerintah berjanji akan menghapus data jika sudah tidak digunakan. Namun, beberapa pakar siber menilai bahwa data pribadi yang dikumpulkan PeduliLindungi memliliki dua kemungkinan. Pertama, data itu bisa saja dihapus pada saat tidak digunakan lagi. Kedua, data dibiarkan begitu saja, disimpan sekian lama lalu tinggal menunggu bobol saja. Karena sebenarnya tidak ada yang mengawasi bahwa data ini benar-benar dihapus.[15]

2) Perlindungan Data Privasi di Indonesia dan Singapura terkait Penerapan *Digital Contact Tracing,* Khususnya dalam penggunaan Aplikasi Pelacakan sebagai Upaya Pencegahan COVID-19 dan Tanggung Jawabnya.

Menurut Laurence Lessig, hukum memberikan batasan antara yang boleh dan tidak, karena itulah hukum dapat menjadi alternatif perlindungan untuk berbagai permasalahan

[13] Herdanang Ahmad Fauzan, "PeduliLindungi, Antara Covid-19 dan Perlindungan Data Pribadi",https://teknologi.bisnis.com/read/20200624/84/1257107/pedulilindungi-antara-covid-19-dan-perlindungan-data-pribadi#, diakses 19 September 2020

[14] Tentang PeduliLindungi, https://www.pedulilindungi.id/#tentang, diakses pada 14 September 2020

[15] Arif Rahman, "Aplikasi PeduliLindungi Bisa Tak Berguna Bagi User", https://cyberthreat.id/read/6233/Aplikasi-PeduliLindungi-Bisa-Tak-Berguna-bagi-User, diakses 19 September 2020

pelanggaran data privasi. Hukum juga dapat memberlakukan sanksi yang sah pada para pelanggar.[16] Oleh karena itu, untuk mencegah pelanggaran terhadap data privasi yang semakin marak, banyak negara di dunia mulai menerapkan norma hukum, karena hukum dianggap dapat menciptakan keteraturan dan ketertiban di dalam masyarakat demi tujuan keadilan

Terkait upaya pencegahan penyebaran COVID-19, Indonesia menerapkan *digital contact tracing* dengan menggunakan aplikasi pelacakan PeduliLindungi. Aplikasi ini menggunakan data pribadi pengguna untuk keperluan *contact tracing*. Selain *digital contact tracing*, juga dilakukan metode penginputan data oleh pengunjung ketika memasuki *public places*, seperti mal, restoran, tempat hiburan, dan lain sebagainya. Dalam pengumpulan data pribadi untuk keperluan *contact tracing*, baik melalui aplikasi pelacakan maupun metode penginputan data pengunjung, dibutuhkan jaminan keamanan dan kejelasan tanggung jawab yang dapat diberikan jika terjadi pelanggaran atas data-data pribadi tersebut. Setelah ditelusuri, data-data pribadi yang dikumpulkan pada aplikasi, meliputi nama lengkap, NIK, email serta nomor telepon. Sementara, penginputan data oleh pengunjung pada *public places* biasanya hanya nama lengkap dan nomor telepon pribadi saja. Terkait ini, banyak pakar hukum memperingatkan tentang "krisis privasi" karena perusahaan dapat mengeksploitasi data-data tersebut sebelum meneruskannya ke pemasar atau pihak ketiga lainnya.[17]

Secara umum data pribadi merupakan informasi yang sangat pribadi yang disimpan untuk diri sendiri, atau setidaknya hanya diketahui oleh orang-orang terbatas.[18] Data pribadi sangat berkaitan dengan privasi karena privasi menyangkut informasi yang bersifat pribadi. Karena itulah, penyalahgunaan data peribadi dapat menyebabkan pelanggaran privasi.

Seperti yang dikatakan oleh Thomas J. Smedingho, informasi seseorang yang dikumpulkan dan digunakan oleh orang lain juga termasuk dalam hak atas privasi. Penyalahgunaan data tersebut merupakan pelanggaran hak atas privasi seseorang.[19] Seiring perkembangan teknologi informasi, perlindungan data pribadi sekarang telah diperlakukan sebagai bagian dari perlindungan privasi. Sebab, data pribadi seseorang pasti mengandung informasi--informasi pribadi orang tersebut *(information privacy).*[20]

---

[16] Lawrence Lessig, *Code Version 2.0,* New York: Basic Books Publishing, 2006, hlm. 223.

[17] Shanti Das, "Contact Tracing Data Harvested From Pubs and Restaurants", https://www.thetimes.co.uk/article/contact-tracing-data-harvested-from-pubs-and-restaurants-being-sold-on-s0d85mkrr

[18] Penjelasan Pasal 26 ayat (1) huruf a, b, dan c Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[19] Thomas J. Smedinghodd, (ed.), *Online Law: The SPA's Legal Guide to Doing Business on the Internet*, Kanada: Addison Wesley Developers Press, 1996, hlm. 269-273

[20] Alan Westin, Privacy and Freedom, London, 1967, hlm. 7, dalam Sinta Dewi, Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional Dewi, S. Bandung, PT Refika Aditama, 2015, hlm.28

Di Indonesia saat ini, pengaturan mengenai perlindungan data pribadi dapat ditemukan dalam 1 Pasal dalam Undang-Undang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE) yaitu pada Pasal 26 yang merupakan salah satu bentuk pengejawatahan Pasal 28 G ayat (1) Undang-Undang Dasar 1945 (UUD 1945).

Dari Pasal 26 UU ITE, Pasal tersebut mengandung beberapa pokok pemikiran. Pertama, setiap data pribadi yang dikumpulkan atau digunakan dalam media apapun harus selalu atas dasar persetujuan *(consent)* pemilik data yang bersangkutan. Kedua, undang-undang memberikan sarana kepada pemilik data pribadi untuk dapat mengajukan gugatan atas kerugian jika terjadi kebocoran data. Yang terakhir yakni yang ketiga, the *right to be forgotten* atau hak untuk dilupakan.

Dari aturan UU ITE di atas diturunkan ke dalam peraturan pemerintah yakni Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disebut PP PSTE). PP PSTE mengharuskan seluruh penyelenggara sistem elekronik untuk turut serta menjaga data privasi yang dikelolanya sebagaimana tercantum pada Pasal 15.

Terkait dengan penerapan *digital contact tracing* pada aplikasi pelacakan, perlu diperhatikan bahwa data pribadi yang dikumpulkan pada penggunaan aplikasi itu harus dijaga kerahasiaannya, keutuhannya, juga ketersediaannya. Selain itu perlu ada jaminan bahwa penggunaan atau pengungkapan data dilakukan atas *consent* dari pemilik data pribadi pada saat perolehan data.

Seperti yang dijelaskan, penerapan *digital contact tracing* tidak hanya menggunakan aplikasi pelacakan, namun juga penginputan data pengunjung di *public places* seperti mal, restoran ataupun perkantoran. Untuk keperluan *contact tracing* ini, banyak perusahaan menggunakan *platform* tertentu untuk pengumpulan data. Biasanya, data-data dari pengunjung hampir sama dengan data yang dikumpulkan dengan aplikasi PeduliLindungi. Perusahaan-perusahaan yang mengumpulkan data pribadi para pengunjung ini harus memperhatikan peraturan yang berlaku terkait data pribadi individu dalam menyelenggarakan upaya *contact tracing* ini.

Sebagaimana tercantum pada Pasal 15 ayat (3) PP PSTE, PP PSTE mendelegasikan kepada Menteri Komunikasi dan Informatika untuk mengeluarkan peraturan menteri sebagai peraturan turunannya. Dengan itu, dikeluarkanlah Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (selanjutnya disebut Permenkominfo 20/2016). Peraturan ini lebih

komprehensif mengatur perlindungan data privasi, seperti dalam hal persetujuan pemilik data (terdapat pada Pasal 9), tujuan pengumpulan data (terdapat pada Pasal 7), pembatasan (terdapat pada Pasal 7 Jo. Pasal 12), pencegahan (terdapat pada Pasal 5), pilihan (terdapat pada Pasal 8), penyimpanan data (terdapat pada Pasal 15), pengungkapan data (terdapat pada Pasal 21 Jo. Pasal 23), transfer data (terdapat pada Pasal 22), serta pemberitahuan (terdapat pada Pasal 28).

Mengenai peraturan, seperti diketahui, peraturan menteri merupakan peraturan teknis dan peraturan pendelegasian dari peraturan yang lebih tinggi, yakni peraturan pemerintah. Dengan begitu, manakala terjadi pelanggaran terhadap data pribadi ataupun kegagalan dalam perlindungan data pribadi, seperti dalam penerapan *digital contact tracing* melalui penggunaan aplikasi pelacakan, sanksi yang dapat diterapkan paling tinggi pada sanksi administratif saja. Jika melihat tataran hierarkis peraturan perundang-undangan pun, seperti yang tercantum dalam Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan, seperti dalam Pasal 7, tidak secara jelas menerangkan posisi peraturan menteri. Akhirnya, dapat dikatakan, terdapat ketidakjelasan aturan terkait perlindungan data privasi di Indonesia karena bentuk aturan tersebut sebatas peraturan Menteri itu sendiri.

Dalam aturan-aturan di atas, seperti dalam Permenkominfo, pelanggaran data privasi tidaklah diikuti dengan sanksi pidana atau sanksi lainnya. Akibatnya tidak ada ketakutan yang dirasakan pengelola data bila terjadi penyalahgunaan data. Sanksi tersebut dinilai tidak menimbulkan efek jera bagi pelaku. Dengan kata lain, pengaturan khusus mengenai perlindungan data pribadi yang hanya pada sebatas Peraturan Menteri kurang dapat mengakomodir permasalahan menyangkut data pribadi yang demikian kompleks.

Beralih ke Singapura, seperti di Indonesia, negara tetangga ini juga menggunakan aplikasi pelacakan untuk keperluan *contact tracing* sebagai salah satu upaya pencegahan penyebaran COVID-19. Aplikasi ini dinamakan TraceTogether. Data-data pada aplikasi tersebut disimpan dalam sektor public (Pemerintah Singapura). Di Singapura, perlindungan data pribadi pada sektor public dan swasta dibedakan.[21]

Data-data pengguna yang dikumpulkan dari aplikasi TraceTogether di atas dilindungi oleh Public Sector Governance Act 2018 (selanjutnya disebut PSGA) dimana ketentuan keamanan data dimasukkan dalam Undang-Undang tersebut. Lahirnya PSGA ini ditujukan

[21] Findlay, Mark. et.al. Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-Crisis. *Singapore Management University (SMU) Centre for AI & Data Governance Research Paper No. 2020/02*. hlm.17

untuk lebih memperkuat tata kelola data sektor publik sambil memfasilitasi berbagi data antar-lembaga untuk meningkatkan pembuatan kebijakan dan pemberian layanan. [22]

PSGA itu sendiri menetapkan tentang kriteria data yang bisa dibagikan ke seluruh badan publik. PSGA juga memberlakukan hukuman pidana kepada pejabat publik yang secara sembrono atau sengaja mengungkapkan data tanpa izin, menyalahgunakan data untuk keuntungan, atau mengidentifikasi ulang data yang dianonimkan seperti pada Section 7 PSGA.

Dalam penjelasan section 7 pada PSGA, dikatakan bahwa seorang individu yang menyebabkan *disclosure of data* (kebocoran data), secara sengaja maupun tidak sengaja, dibawah kontrol sektor public Singapura, dapat dikenakan hukuman penjara sampai dengan 2 tahun atau denda sebesar $5000 (lima ribu dollar singapura).

Pemberlakuan hukuman pidana di Singapura jika terjadi kebocoran data, khususnya pada sektor public (pemerintah), dapat dikatakan lebih efektif, setidaknya bila dibandingkan dengan aturan di Indonesia yang hanya menerapkan sanksi administratif dan masih sebatas peraturan menteri. Meskipun pidana merupakan *ultimum remedium* namun dapat dipandang cukup efektif untuk memberikan efek jera terhadap pelaku penyalahgunaan data privasi.

Perlindungan data pribadi di Singapura juga terdapat pada Personal Data Protection Act (PDPA) yang baru saja diamandemen pada tahun 2020. Undang-undang dibuat sebagai standar dasar untuk perlindungan data di sektor swasta. Tujuannya untuk meningkatkan kepercayaan dalam pengelolaan dan pemrosesan data. Namun badan public dalam hal ini Pemerintah Singapura tidak terikat oleh PDPA, tetapi di bawah PSGA.

Dalam penerapan *digital contact tracing* di Singapura terdapat organisasi atau pihak swasta yang terlibat. Telah dijelaskan sebelumnya bahwa dalam aplikasi TraceTogether memiliki salah satu fitur SafeEntry. Fitur ini digunakan ketika pengunjung *public places* menginput datanya melalui *scan barcode* pada aplikasi SafeEntry yang digunakan oleh organisasi/pihak swasta melalui aplikasi TraceTogether.

Seperti halnya di Indonesia, perusahaan/organisasi di Indonesia juga mengumpulkan data pribadi untuk keperluan *contact tracing* dengan menggunakan suatu *platform* tersendiri. Terkait ini, organisasi atau pihak swasta di Singapura juga diwajibkan untuk memberikan jaminan keamanan data yang tersimpan di bawah kontrolnya maupun pada aplikasi SafeEntry. Dalam PDPA, berkaitan dengan penggunaan SafeEntry, terdapat aturan yang jelas mengenai kewajiban organisasi atau pihak swasta untuk melindungi data pada perangkat atau *device*

[22] *Ibid.*

P-ISSN: 2721-0545, E-ISSN: 2722-3604 Volume 2 Nomor 1, Desember 2020

yang digunakannya untuk mengumpulkan data pribadi individu, seperti yang diatur pada section 24 PDPA.

Section tersebut mewajibkan organisasi untuk melindungi data pribadi dengan aman dan melakukan pencegahan terhadap akses, pengumpulan, penggunaan, pengungkapan yang tidak sah, dan hilangnya media atau perangkat penyimpanan data pribadi. Dalam hal terjadi *disclosure of data* secara tidak sah di bawah organisasi itu yang sangat mungkin terjadi, *section* 48 mengatur mengenai hal tersebut berikut dengan sanksinya.

Manakala terjadi *unauthorized disclosure of data,* individu di bawah organisasi tersebut dapat dikenakan pidana penjara sampai dengan 2 tahun ataupun dikenakan denda sebesar $5,000 dollar Singapura ataupun dikenakan keduanya. Hal ini sama penerapannya dengan peraturan pada sektor publik yang ada pada Public Sector Governance Act 2018 (PSGA).

Secara umum, ketika organisasi sektor swasta mengumpulkan, menggunakan dan / atau mengungkapkan data pribadi seseorang, mereka diwajibkan untuk memberi tahu individu tentang tujuan mereka (PDPA, pasal 20 (1)) dan untuk mendapatkan persetujuan dari individu (PDPA, pasal 13) Namun, PDPA menyediakan "Pengecualian Tanggap Darurat", di mana organisasi tidak perlu memberikan pemberitahuan atau mendapatkan persetujuan jika pengumpulan, penggunaan, atau pengungkapan data pribadi diperlukan dalam keadaan darurat. Yang dimaksud dengan keadaan darurat adalah keadaan yang mengancam kehidupan, kesehatan atau keselamatan individu atau individu lain. Disebutkan bahwa pengumpulan, penggunaan, dan pengungkapan data pribadi "untuk melakukan pelacakan kontak dan tindakan respons COVID-19" termasuk dalam Pengecualian Tanggap Darurat.

Namun, organisasi yang telah mengumpulkan data pribadi dengan mengandalkan Pengecualian Tanggap Darurat, tetap harus berhati-hati untuk tidak menggunakan atau mengungkapkan data pribadi untuk tujuan lain, kecuali mereka telah memperoleh persetujuan untuk tujuan lain tersebut. Jadi organisasi tidak boleh mengumpulkan, menggunakan, atau mengungkapkan data pribadi daripada yang diperlukan untuk tujuan tindakan respons terhadap COVID-19 yang dimaksud.

Organisasi/swasta juga harus mengingat bahwa Pengecualian Tanggap Darurat tidak membebaskan mereka dari kewajiban perlindungan data dalam PDPA. Ini termasuk, kewajiban untuk melindungi data pribadi dengan membuat "pengaturan keamanan yang wajar" seperti yang telah dijelaskan sebelumnya, dan kewajiban untuk menghapus data pribadi setelah tujuan awal pengumpulan data pribadi telah kedaluwarsa dan tidak ada tujuan

hukum yang memerlukan penyimpanan data pribadi lagi. Langkah-langkah tanggapan COVID-19 ini memang sangat melibatkan pengorbanan privasi yang diperlukan demi kesehatan masyarakat. Tetap saja, privasi tetap menjadi nilai penting bahkan dalam menghadapi pandemi.

Untuk praktik perlindungan data privasi di Singapura itu sendiri, dalam melakukan penegakan dan efektifitas berlakunya aturan ini, dihadirkan *Personal Data Protection Commission (PDPC)*. Tugas utama komisi ini setidaknya sebagai pemantau kepatuhan dalam pelaksanaan aturan ini, selain sebagai yang berwenang menerima pengaduan dari masyarakat umum dan sebagai fasilitator dalam penyelesaian sengketa alternatif. Setiap individu yang mengalami kerugian atas adanya penyalahgunaan data privasi oleh organisasi yang memiliki kewajiban untuk melindungi data privasi, seperti dalam halnya penerapan *digital contact tracing*, dapat mengajukan gugatan kepada organisasi yang bertanggung jawab secara perdata. Lebih lanjut, setiap yang mengalami kerugian dapat melakukan pengaduan kepada PDPC Singapore juga atas dugaan adanya penyalahgunaan data privasinya oleh organisasi. PDPC Singapore juga dapat melakukan penyidikan setelah mendapat aduan dan memungkinkan untuk menjatuhkan sanksi berupa denda sampai dengan S$1 Juta bilamana terdapat cukup bukti yang menyatakan organisasi tersebut telah melanggar aturan pada PDPA. Sanksi yang dapat dijatuhkan selain denda, yakni sanksi berupa pidana penjara maksimal tiga tahun sebagaimana diatur dalam Section 56 PDPA.[23]

C. PENUTUP

Dalam penerapannya, aplikasi yang diluncurkan Pemerintah Indonesia telah melanggar prinsip transparansi, prinsip pembatasan tujuan, dan prinsip minimalisasi data. Jika dibandingan dengan Singapura, negara tetangga ini sudah memiliki bentuk perlindungan yang tertuang dalam *Personal Data Protection Act* maupun *Public Sector Governance Act.* Pemerintah Singapura menerapkan sanksi pidana dan denda maupun keduanya terhadap pelanggaran data pribadi, seperti jika terjadi *disclosure of data* secara tidak sah. Sementara di Indonesia, sanksi untuk hal tersebut masih sebatas sanksi adminsitratif yang kurang memiliki efek jera bagi penyalahguna data, hal ini sendiri berkaitan dengan tanggung jawab atas data pribadi. Untuk peraturan secara khusus perihal perlindungan data pribadi, di Indonesia masih sebatas pada peraturan Menteri dan tersebar di peraturan-peraturan lain yang kurang cukup mengakomodir. Mengenai praktik perlindungan data privasi di Singapura pun cukup baik

[23] Personal Data Protection Act, Singapore, Section 56,

untuk dijadikan *benchmark* bagi Indonesia, terutama dengan adanya Personal Data Protection Commission (PDPC). Sungguh mendesak bagi Indonesia untuk segera memiliki peraturan secara khusus yang mengatur mengenai perlindungan data pribadi warga negaranya. Terlebih pada kasus pemanfaatan data pribadi untuk upaya pencegahan COVID-19. Indonesia diharapkan dapat mencontoh Singapura yang telah memberi jaminan perlindungan data pribadi yang telah dituangkan dalam undang-undang Negeri Singa tersebut, yaitu PDPA dan PSGA.

DAFTAR PUSTAKA

Buku

Lawrence Lessig, *Code Version 2.0,* New York: Basic Books Publishing, 2006

Sinta Dewi, Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional, Bandung, PT Refika Aditama, 2015

Thomas J. Smedinghodd, (ed.). *Online Law: The SPA's Legal Guide to Doing Business on the Internet*, Kanada: Addison Wesley Developers Press, 1996

Jurnal

Eugene H. Spafford, Security models for web-based applications, *Communications of the ACM*, Volume 44 , Issue 2 , 2001

Findlay, Mark. et.al., Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-Crisis. *Singapore Management University (SMU) Centre for AI & Data Governance Research Paper No. 2020/02*. 2020.

Koustubh "K.J." Bagchi, et.al, Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns, COVID-19 Rapid Response Impact Initiative, *White Paper 22, 2020.*

Sinta Dewi Rosadi, Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing di Indonesia, *Jurnal Yustisia*. Vol.5 No.1 Januari - April 2016, hlm.26

Warren dan Louis D. Brandeis, The Right to Privacy, *Harvard Law Review, Vol. IV, No. 5,* Desember 1890

Website

Arif Rahman, "Aplikasi PeduliLindungi Bisa Tak Berguna Bagi User", https://cyberthreat.id/read/6233/Aplikasi-PeduliLindungi-Bisa-Tak-Berguna-bagi-User, diakses 19 September 2020

Herdanang Ahmad Fauzan, "PeduliLindungi, Antara Covid-19 dan Perlindungan Data Pribadi",https://teknologi.bisnis.com/read/20200624/84/1257107/pedulilindungi-antara-covid-19-dan-perlindungan-data-pribadi#, diakses 19 September 2020

Zhang Jane.

"ADB approves $3 million grant to support Indonesia's fight against COVID-19",https://www.adb.org/news/adb-approves-3-million-grant-support-indonesias-fight-against-covid-19, diakses pada 9 September 2020

"Aplikasi PeduliLindungi untuk Melacak COVID-19 Sudah Bisa Diunduh", https://tekno.kompas.com/read/2020/03/29/18020057/aplikasi-peduli-lindungi-untuk-melacak-covid-19-sudah-bisa-diunduh?page=all, diakses pada 9 September 2020

"Are Asean Contact Tracing Apps Following Privacy and Data Compliance Laws", https://hrasiamedia.com/featured/2020/are-asean-contact-tracing-apps-following-privacy-and-data-compliance-laws/, diakses pada 14 September 2020

"How Does The Trace Together App Work", https://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473-How-does-the-TraceTogether-App-work-, diakses 26 September 2020

"Tentang PeduliLindungi", https://www.pedulilindungi.id/#tentang, diakses pada 14 September 2020

Peraturan Perundang-Undangan

Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik LN Nomor 5952.

Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Privasi dalam Sistem Elektronik

Singapore Personal Data Protection Act Amendment Bill 2020

Singapore Public Sector Governance Act 2018