PERLINDUNGAN DATA PRIBADI SEBAGAI BENTUK PERWUJUDAN CYBER SECURITY
(Studi Komparatif Indonesia dan Singapura)

Sylvia Faradina Amandasari Arthaputri,[1] Ahmad Syaifudin,[2] M. Fahrudin Andriyansyah[3]

Fakultas Hukum Universitas Islam Malang
Jalan Mayjen Haryono No 193 Malang 65144, Telepon (0341) 551932, Fax (0341) 552249
E-mail: sylvfaradina@gmail.com

ABSTRACT

The development of technology is increasing every year, in line with that the impact caused is the emergence of cybercrime such as hacking so that a legal umbrella is needed that can protect personal data. Departing from this issue, the problem formulations studied are as follows: 1) How is the protection of personal data according to Law No. 27 of 2022 on the protection of personal data as a form of realization of cyber security in Indonesia? and 2) How is the comparison of personal data protection arrangements in Indonesia and Singapore? This research uses normative legal research through 3 approaches, namely the legislative approach, concept approach, and comparative approach. The results show that Law No. 27 of 2022 on Personal Data Protection has realized 3 indicators of cyber security namely Confidentiality, Integrity, and Availability so that it has protected the personal data of the Indonesian people. The comparison with Singapore's Personal Data Protection Act 2012 is the difference in the scope of regulation, the definition of personal data, and the sanctions imposed.
Keywords**:** *Personal Data Protection, Cyber Security, Singapore*

ABSTRAK

Perkembangan teknologi semakin tahun semakin meningkat, sejalan dengan itu dampak yang ditimbulkan adalah munculnya kejahatan di dunia maya seperti peretasan ehingga dibutuhkan payung hukum yang dapat melindungi data pribadi. Berangkat dari isu tersebut rumusan masalah yang diteliti adalah sebagai berikut Bagaimana perlindungan data pribadi menurut UU Nomor 27 tahun 2022 tentang perlindungan data pribadi sebagai bentuk perwujudan cyber security di Indonesia? dan Bagaimana perbandingan pengaturan perlindungan data pribadi di Indonesia dan Singapura?. Penelitian ini menggunakan jenis penelitian hukum normatif melalui 3 pendekatan yakni pendekatan perundang-undangan, pendekatan konsep, dan pendekatan perbandingan. Hasil penelitian menunjukkan bahwa Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mewujudkan 3 indikator *cyber security* yakni *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) sehingga telah melindungi data pribadi masyarakat Indonesia. Adapun perbandingannya dengan Personal Data Protection Act 2012 milik negara Singapura adalah perbedaan dalam lingkup regulasi, definisi data pribadi, dan sanksi yang dikenakan.
Kata Kunci: Perlindungan Data Pribadi, *Cyber Security,* Singapura

[1] Mahasiswa Fakultas Hukum Universitas Islam Malang
[2] Dosen Fakultas Hukum Universitas Islam Malang
[3] Dosen Fakultas Hukum Universitas Islam Malang

PENDAHULUAN

Perkembangan teknologi yang semakin hari semakin pesat, memunculkan banyak inovasi baru dari teknologi.[4] Sejalan dengan itu dampak yang ditimbulkan salah satunya adalah munculnya kejahatan di dunia maya atau dikenal juga istilah kejahatan siber contohnya adalah peretasan data yang marak terjadi dalam beberapa tahun terakhir. Hal ini memunculkan ancaman terhadap keamanan siber (*cyber security*) yang salah satunya berkaitan dengan perlindungan terhadap data-data pribadi yang tadinya hanya bersifat konvensional mengalami masa transisi melalui perkembangan teknologi yang maju sehingga diintegrasikan dalam suatu sistem komputer sebagai alat dan jaringan internet sebagai media penyimpanannya. Oleh karena itu dibutuhkan sebuah payung hukum yang dapat melindungi data pribadi untuk mengurangi risiko tersebut dengan mewujudkan sistem perlindungan dari serangan digital melalui *cyber security*.

Dalam konteks kemajuan teknologi informasi, Indonesia dan Singapura merupakan dua negara yang memiliki perhatian serius terhadap perlindungan data pribadi sebagai bagian dari upaya menjaga *cyber security*. Namun, meskipun memiliki tujuan yang sama, implementasi dan kerangka hukum yang digunakan oleh tiap negara mungkin berbeda.[5] Setiap negara dengan tingkat pemerintahan serta otoritas yang berbeda membuat masing-masing tingkat pemerintahan tersebut mempunyai masalah-masalahnya sendiri.[6] Oleh karena itu, penelitian ini bertujuan untuk melakukan studi komparatif antara Indonesia dan Singapura dalam hal perlindungan data pribadi, dengan fokus pada regulasi pengaturan yang berlaku di kedua negara tersebut. Hal ini dapat membantu dalam mengidentifikasi kekuatan dan kelemahan dalam upaya meningkatkan *cyber security* dan perlindungan data pribadi di masing-masing negara. Oleh karena ini penting untuk melindungi individu, perusahaan, dan masyarakat secara keseluruhan, karena salah satu masalah utama kita sekarang ini adalah bagaimana caranya pemerintah Indonesia dalam bekerja melindungi data masyarakatnya dengan lebih cepat dan efisien namun dengan kualitas yang makin baik.[7]

[4] Abdul Rokhim dan Sri Ayu Lestari. Implementasi Media Visualisasi 360 Pada Platform Android Untuk Promosi Penjualan Kendaraan Bekas. *Jurnal Teknika.* Vol.11 (No.2) Tahun 2019. hlm.1127

[5] Ananthia Ayu D., Titis Anindyajati, dan Abdul Ghoffar. 2019. *Perlindungan Hak Privasi Data Diri di Era Ekonomi Digital.* Jakarta*:* Pusat Penelitian dan Pengkajian Perkara Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi. hlm 11.

[6] M. Fahrudin Andriyansyah. Peran Partai Politik Lokal dalam Penyelenggaraan Otonomi Khusus di Provinsi Aceh. *Yurispruden.* Vol.3 (No.1) Tahun 2020. hlm.25

[7] Ahmad Syaifudin. Standar Profesi Hukum dan Kontribusi Pendidikan Tinggi dalam Mewujudkan Profesi Hukum yang Profesional di Era Disruptif. *Yurispruden.* Vol.4 (No.1) Tahun 2021. hlm. 103

Beberapa contoh kasus peretasan data pribadi yang terjadi di Indonesia dalam 3 tahun terakhir ini yakni pada bulan Mei 2020, terjadi insiden kebocoran data pengguna Tokopedia yang kemudian dijual secara ilegal di *platform* gelap yang dikenal sebagai *dark web*. Akibatnya, Tokopedia diberikan sanksi tertulis oleh Kementerian Komunikasi dan Informatika (Kemenkominfo).[8] Selain itu, terdapat juga kebocoran data sebanyak 230 ribu kasus terkait COVID-19 yang melibatkan penduduk Indonesia. Kemudian, pada tahun 2021, dilaporkan bahwa seseorang telah melakukan penjualan informasi pribadi yang meliputi Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk (KTP), data gaji, nomor ponsel, alamat, dan alamat surel (*e-mail*) yang berasal dari situs *bpjs-kesehatan.go.id* yang telah mengalami peretasan.[9] Dilaporkan pula bahwa terjadi pelanggaran keamanan yang mengakibatkan kebocoran data pribadi di antara nasabah asuransi BRI Life. Dalam kejadian ini, sebanyak 1,3 juta data pengguna aplikasi *Electronic Health Alert Card* (E-HAC) Indonesia yang dimiliki oleh Kementerian Kesehatan RI dan data pengaduan daring yang dimiliki oleh Komisi Perlindungan Anak Indonesia (KPAI) juga dilaporkan telah bocor.[10]

Sebagai upaya dalam menanggulangi kejahatan terhadap data pribadi yang marak terjadi, dibutuhkan suatu sistem yang mampu mengimbangi dan menanggulanginya. *Cyber security* merupakan kombinasi alat, kebijakan, konsep keamanan, upaya perlindungan keamanan, pedoman, teknik manajemen risiko, aktivitas pelatihan, praktik terbaik, jaminan, dan teknologi. Singkatnya *cyber security* ini merupakan bentuk keamanan di dunia maya, sehingga dapat dikatakan sebagai upaya dalam memastikan perlindungan terhadap setiap aktivitas yang menggunakan internet. Dari latar belakang tersebut selanjutnya muncul pertanyaan berupa rumusan masalah yakni Bagaimana perlindungan data pribadi menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai bentuk perwujudan *cyber security* di Indonesia? Dan Bagaimana perbandingan pengaturan perlindungan data pribadi di Indonesia dan Singapura?

---

[8] Wahyunanda Kusuma Pertiwi dan Yudha Pratomo. "*Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di Dark Web*". Kompas.com. Diakses 8 Januari 2024. https://tekno.kompas.com/read/2020/05/03/10203107/data-91-juta-pengguna-tokopedia-dan-7-juta-merchant-dilaporkan-dijual-di-dark.

[9] Ayomi Amindoni. "*BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor, Otomatis yang Dirugikan Masyarakat*". BBC News Indonesia. Diakses pada 8 Januari 2024. https://www.bbc.com/indonesia/indonesia-57196905

[10] Antara, Andi Firdausi, dan Pri. "*Data eHAC milik 1,3 Juta penggunanya dilaporkan bocor, Keamanan Data Tidak Prioritas".* BBC News Indonesia. Diakses 8 Januari 2024. https://www.bbc.com/indonesia/indonesia-58393345

Dalam penulisan hukum ini, jenis penelitian hukum yang digunakan adalah Yuridis-Normatif dengan menggunakan tiga jenis pendekatan yakni, pendekatan perundang-undangan, pendekatan konsep, dan pendekatan perbandingan. Adapun teknik pengumpulan bahan hukumnya adalah menggunakan studi kepustakaan yang mana mengkaji literatur-literatur yang berhubungan dengan isu hukum yang diteliti.

PEMBAHASAN

A. Perlindungan Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi sebagai Bentuk Perwujudan *Cyber Security* di Indonesia

Bentuk perlindungan hukum yang diberikan oleh suatu negara memiliki dua sifat, yaitu bersifat preventif dan represif.[11] Preventif berarti pencegahan yakni salah satu sifat perlindungan hukum yang bertujuan untuk mencegah terjadinya pelanggaran hukum atau tindakan yang melanggar aturan yang telah ditetapkan. Sedangkan represif berarti pemberian sanksi yakni sifat perlindungan hukum yang berarti bahwa negara memberikan konsekuensi atau hukuman kepada mereka yang melanggar hukum.[12] Dalam hal ini perlindungan hukum yang kaitannya dengan data pribadi di Indonesia telah diwujudkan secara preventif dan represif dalam produk hukum yakni Undang-Undang Nomor 27 Tahun 2022 tentang Perlidungan Data Pribadi.

Adapun beberapa usaha dan upaya yang telah diatur dalam peraturan tentang perlindungan data pribadi tersebut adalah sebagai berikut:

1. Pengumpulan informasi pribadi. Setiap individu mempunyai hak untuk diberitahu dan mempunyai kendali atas pengumpulan informasi pribadi tentang mereka. Data pribadi hanya dapat dikumpulkan dengan izin yang sah dan secara transparan.
2. Informasi pribadi hanya dapat digunakan sesuai dengan alasan perolehannya; hal ini berarti data tersebut tidak boleh digunakan untuk tujuan tambahan tanpa alasan yang sah.
3. Keamanan data pribadi perlu dilindungi dari akses yang melanggar hukum, penggunaan yang tidak patut, dan manipulasi yang tidak disengaja atau disengaja.
4. Wewenang untuk mengungkapkan dan mengelola informasi pribadi. Setiap orang berhak melihat dan mengelola informasi pribadinya. Seseorang berhak meminta agar data pribadinya diperbaiki atau dihapus jika terdapat kesalahan atau ketidakakuratan.

[11] Fitria Dewi Navisa, Hukum Kenotariatan Indonesia Jilid I, Media Sains Indonesia (2022)
[12] Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, Surakarta: magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, 2003), hlm.20

5. Pemindahan informasi pribadi. Setiap orang berhak jika memungkinkan, agar data pribadinya ditransfer ke lokasi atau penyedia layanan lain.

Sehubungan dengan itu korelasi antara perlindungan data pribadi terhadap perwujudan *cyber security* didasarkan pada kasus-kasus peretasan data yang terjadi beberapa tahun ke belakang. Hal ini menjadi bukti bahwa Indonesia masih lemah terhadap *cyber security*-nya sehingga serangan-serangan siber seperti peretasan data masih sering terjadi, sedangkan kasus-kasus yang sama kedepannya tidak dapat dihindari bahkan dapat berkembang pesat sesuai dengan perkembangan zaman.

Dengan demikian acuan yang dilakukan sebagai indikator perwujudan *cyber security* dalam menganalisis regulasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi ini menggunakan konsep CIA Triad atau dikenal dengan *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan informasi) yang berperan sebagai tiga aspek penting dalam indikator keamanan.[13] Ketiga konsep ini merupakan panduan dalam membentuk sistem, prosedur, ataupun kebijakan yang berhubungan dengan keamanan informasi. [14] Keamanan informasi merupakan anak bagian dari payung *cyber security*, sehingga untuk meminimalisasi ruang lingkup yang luas dari *cyber security* diambil konsep CIA Triad ini sebagai tiga aspek yang penting dalam menciptakan sebuah keamanan informasi yang kuat dan efektif. Sehingga dengan terselenggaranya ketiga aspek ini maka *cyber security* dapat diwujudkan dengan optimal, karena konsep ini biasanya digunakan dalam mengantisipasi terjadinya kejahatan siber. Adapun penjelasan mengenai ketiga konsep tersebut jika dilihat perwujudannya didalam pengaturan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi diuraikan sebagai berikut:[15]

a. Confidentiality

Confidentiality atau kerahasiaan bertujuan untuk mencegah informasi diungkapkan tanpa izin atau dapat diungkapkan secara tidak sengaja karena kelalaian pihak yang mengelolanya. Prinsip ini memberikan jaminan terhadap kerahasiaan data atau informasi dengan menjaga kerahasiaan suatu informasi dari pihak yang tidak berwenang. Dengan kata lain prinsip ini berupa pengelolaan dari pembatasan hak terhadap informasi.

[13] Yusnita Sari, I., Muttaqin, Jamaludin, Simarmata, J., Rahman, M. A., Iskandar, A., Fernando, A., Sugianto, Giap, Y. C., & Hazriani. Keamanan Data Dan Informasi. (2020)

[14] Pitra Winarianto, Daniel Eduardo Daud, CIA Triad, https://student-activity.binus.ac.id/csc/2022/08/cia-triad/, diakses pada 15 Januari 2024 pukul 00.33 wib

[15] D. Junian, Pengembangan Kebijakan Keamanan Informasi pada Perusahaan Jasa Layanan Kurir, Jakarta: Universitas Indonesia, (2008), hlm 7-10

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9495-9509

Perwujudan konsep ini dalam Undang-Undang Nomor 27 Tahun 2022 tercantum dalam BAB IV Kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi Dalam Pemrosesan Data Pribadi. Hal ini diatur dalam Pasal 36 yang menyatakan bahwa pengendali data pribadi wajib menjaga kerahasiaan data pribadi yang dimilikinya. Selain itu, Pasal 37 juga mengatur bahwa pengendali data pribadi wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi. Tujuannya adalah untuk memastikan bahwa data pribadi tidak diakses atau diungkapkan oleh pihak yang tidak berwenang. Contohnya, jika suatu perusahaan memiliki data pribadi pelanggan seperti nomor telepon atau alamat email, maka perusahaan tersebut harus memastikan bahwa data tersebut hanya diakses oleh pihak yang berwenang seperti karyawan yang bertanggung jawab dalam pemrosesan data tersebut.

Dengan demikian konsep *confidentiality* (kerahasiaan) telah terwujud sesuai dengan pasal-pasal yang telah diuraikan, yang mana dalam hal ini bentuk *cyber security* terhadap data pribadi adalah bahwa pengendali data pribadi memiliki kewajiban dalam mencegah informasi data diungkapkan tanpa izin karena sifatnya rahasia yang mana hal ini didasari sebagai prinsip perlindungan data pribadi dalam Pasal 16 ayat (2) huruf e yang berbunyi:

> "pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, penyalahgunaan, perusakan, dan atau penghilangan data pribadi."

b. Integrity

Dalam hal keamanan informasi, integritas mengacu pada gagasan bahwa data tidak dapat ditambahkan, diubah, atau dihapus tanpa izin terlebih dahulu. Atau dengan kata lain, integritas adalah sebuah konsep yang berusaha menjaga kebenaran informasi. Prinsip ini berhubungan dengan integritas atau keutuhan suatu data dalam menjaga aslinya suatu data dari aktivitas modifikasi. Adapun aktivitas modifikasi yang dimaksud disini ialah data tersebut tidak dapat ditambahkan, diubah, atau dihapus tanpa izin terlebih dahulu dari pemilik data.

Perwujudan konsep ini dalam Undang-Undang Nomor 27 Tahun 2022 diwujudkan dalam BAB IV Kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi Dalam Pemrosesan Data Pribadi. Hal ini diatur dalam Pasal 18 ayat (1) yang menyatakan bahwa pengendali data pribadi atau prosesor data pribadi wajib memperoleh persetujuan dari pemilik data pribadi sebelum melakukan pemrosesan data pribadi. Selain itu, Pasal 20 ayat (1) juga mengatur bahwa pemilik data pribadi berhak untuk meminta pengendali data pribadi atau prosesor data pribadi untuk menghapus data pribadi yang dimilikinya jika data tersebut tidak lagi diperlukan atau jika

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9495-9509

pemilik data pribadi mencabut persetujuannya. Contohnya, jika seseorang memberikan data pribadi seperti nomor telepon atau alamat email kepada suatu perusahaan, maka perusahaan tersebut tidak dapat menambahkan, mengubah, atau menghapus data pribadi tersebut tanpa persetujuan dari orang tersebut. Jika perusahaan ingin melakukan perubahan atau penghapusan data pribadi, maka perusahaan harus meminta persetujuan terlebih dahulu dari orang tersebut.

Selain daripada itu pada Pasal 30 berbunyi sebagai berikut:

"(1) Pengendali data pribadi wajib memperbarui dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi paling lambat 3x24 jam terhitung sejak pengendali data pribadi menerima permintaan pembaruan dan/atau perbaikan data pribadi

(2) pengendali data pribadi wajib memberitahukan hasil pembaruan dan/atau perbaikan data pribadi kepada subjek data pribadi."

Dengan demikian konsep *integrity* (integritas) diwujudkan telah terwujud sesuai dengan pasal-pasal yang telah diuraikan, yang mana dalam hal ini bentuk *cyber security* terhadap data pribadi adalah bahwa pengendali data pribadi memiliki kewajiban tidak dapat menambahkan, mengubah, atau menghapus data tanpa izin terlebih dahulu dari pemilik data.

c. Availability

Aspek ketiga yakni *availability* atau ketersediaan, aspek ini penting karena tanpa ketersediaan maka data menjadi tidak berarti meskipun kerahasiaan dan integritas terjamin. *Availability* atau ketersediaan menunjukkan kemampuan pengguna data untuk mengakses data mereka dalam suatu sistem atau jaringan ketika subjek data membutuhkan. Prinsip ini berarti bahwa pemilik data berhak memiliki akses kapanpun dan dimanapun terhadap data yang telah tersimpan dalam suatu sistem dan/atau jaringan. Dengan kata lain prinsip ini berhubungan dengan ketersediaan informasi saat dibutuhkan.

Perwujudan konsep ini dalam Undang-Undang Nomor 27 Tahun 2022 tercantum dalam BAB IV Kewajiban Pengendali Data Pribadi dan Prosesor Data Pribadi Dalam Pemrosesan Data Pribadi. Hal ini diatur dalam Pasal 19 ayat (1) yang menyatakan bahwa pemilik data pribadi berhak untuk memperoleh akses terhadap data pribadi yang dimilikinya yang telah tersimpan oleh pengendali data pribadi atau prosesor data pribadi. Pemilik data pribadi juga berhak untuk memperoleh salinan data pribadi yang dimilikinya dan meminta pengendali data pribadi atau prosesor data pribadi untuk mengirimkan salinan data pribadi tersebut ke alamat yang telah ditentukan oleh pemilik data pribadi. Contohnya, jika seseorang ingin mengetahui data pribadi yang dimiliki oleh suatu perusahaan, maka orang tersebut berhak untuk meminta

akses terhadap data pribadi tersebut dan meminta perusahaan untuk mengirimkan salinan data pribadi tersebut ke alamat yang telah ditentukan.

Selain daripada itu, pada pasal 32 berbunyi sebagai berikut:

"(1) pengendali data pribadi wajib memberikan akses kepada subjek data pribadi terhadap data pribadi yang diproses beserta rekam jejak pemrosesan data pribadi sesuai dengan jangka waktu penyimpanan data pribadi

(2) akses sebagaimana dimaksud pada ayat (1) diberikan paling lambat 3x24 jam terhitung sejak pengendali data pribadi menerima permintaan akses"

Dengan demikian konsep *Availability* (ketersediaan) sudah terwujud sesuai dengan bunyi pasal yang penulis telah uraikan, yang mana dalam hal ini bentuk *cyber security* terhadap data pribadi adalah bahwa pengendali data pribadi memiliki kewajiban untuk memberikan akses kepada subjek data pribadi kapanpun ingin mengakses datanya.

Berdasarkan uraian diatas maka konsep *cyber security* yang diwakili oleh *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan) telah terwujud dalam kebijakan dan regulasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Adapun jika dilihat secara keseluruhan undang-undang ini telah menjadi salah satu pondasi benteng ketahanan *cyber security* di era digital saat ini, dikarenakan diatur ketentuan mengenai hak dan kewajiban terhadap pengendali data yang terbukti mengalami kebocoran data pribadi.[16]

B. Perbandingan Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Singapura

1. Pengaturan Perlindungan Data Pribadi Di Indonesia

Perlindungan hukum terhadap data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 memiliki dua elemen penting, yaitu subjek data pribadi dan pengendali data pribadi. Orang perseorangan yang dilampirkan data pribadinya disebut sebagai subjek data pribadi. Di sisi lain, setiap individu, badan publik, termasuk organisasi internasional, yang bertindak sendiri atau bersama-sama untuk menentukan tujuan dan melakukan kontrol atas pemrosesan data pribadi adalah pengontrol data pribadi.

Undang-undang yang disahkan pada 17 Oktober 2022 ini berlandaskan bahwa hak atas data pribadi merupakan hak milik yang melekat pada setiap individu sebagai subyek data pribadi. Perlindungan data pribadi ini berlaku bagi siapa saja baik individu warga negara

[16] Fitria Dewi Navisa, Perlindungan Hukum Atas Kebocoran Data Dan Informasi Pribadi Pada Penumpang Transportasi Udara, Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang Vol. 5 No. 1 (2022), Hlm 125-140

ISSN (*Print*) : 0854-7254 | ISSN (*Online*) : 2745-9829
Volume 30 Nomor 1 Bulan Januari Tahun 2024, 9495-9509

Indonesia maupun warga negara asing yang berada di Indonesia, kaitannya dengan seluruh pemrosesan data pribadi yang meliputi pengumpulan, penggunaan, pengungkapan, penyimpanan, pengiriman, hingga penghapusan data.

Perlindungan data pribadi didefinisikan sebagai langkah-langkah komprehensif untuk menjaga Data Pribadi selama pemrosesannya guna menegakkan hak konstitusional setiap individu yang memiliki data tersebut. Dengan kata lain peraturan ini berisi perlindungan terhadap setiap aktivitas pemrosesan data pribadi yang mana aktivitas tersebut berupa pengumpulan, penggunaan, maupun pengungkapan data pribadi. Undang-undang ini berasaskan perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan.

Undang-Undang Perlindungan Data Pribadi mengatur upaya perlindungan data pribadi melalui beberapa hal, seperti penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan, serta penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi. Hal ini bertujuan untuk memberikan perlindungan yang memadai atas data pribadi sehingga masyarakat dapat memberikan data pribadi untuk kepentingan masyarakat yang lebih besar tanpa disalahgunakan atau melanggar hak pribadinya.[17]

2. Pengaturan Perlindungan Data Pribadi di Singapura

Di negara Singapura, perlindungan terhadap data pribadi diatur dalam *The Personal Data Protection Act No. 26 of 2012* (selanjutnya disebut PDPA). Undang-undang ini mencantumkan prinsip-prinsip berikut sebagai bagian dari gagasannya untuk melindungi data pribadi warga negaranya:

a. Prinsip *Consent* (Persetujuan)

   Jika suatu organisasi mendapat persetujuan dari subjek data pribadi, organisasi tersebut dapat mengumpulkan, menggunakan, dan mengungkapkan informasi pribadi orang tersebut.

b. Prinsip *Purpose* (Tujuan)

   Organisasi dapat mencari, memperoleh, menggunakan, dan mengungkapkan informasi pribadi tentang seseorang dalam keadaan apa pun; terlebih lagi, asalkan

[17] Fitria Dewi Navisa, Perlindungan Hukum Atas Kebocoran Data Dan Informasi Pribadi Pada Penumpang Transportasi Udara, Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang Vol. 5 No. 1 (2022), Hlm 125-140

subjek data diberitahu tentang alasan permintaan atau pengumpulan, organisasi dapat menggunakan dan mengungkapkan informasi pribadi individu tersebut kepada yang bersangkutan.

c. Prinsip *Reasonableness* (Kewajaran)

Jika suatu organisasi memiliki alasan yang sah dan dapat diterima untuk mengumpulkan, menggunakan, atau menerbitkan informasi pribadi seseorang, maka hal tersebut diperbolehkan.

3. Perbandingan Pengaturan Perlindungan Data Pribadi Di Indonesia Dan Singapura

Selanjutnya agar lebih jelas dalam melihat perbedaan dan persamaan dari kedua undang-undang ini, berikut adalah perbandingan pengaturan perlindungan data pribadi di Indonesia dan Singapura antara Undang-Undang Nomor 27 Tahun 2022 (UU PDP) dan *Personal Data Protection Act* (PDPA) Tahun 2012:

a. Lingkup Regulasi

UU PDP milik Indonesia mencakup seluruh sektor dan aktivitas yang memproses data pribadi. Sedangkan PDPA milik Singapura lebih fokus pada perlindungan data pribadi dalam konteks bisnis dan perdagangan elektronik. Dengan kata lain UU PDP memberi pengaturan lebih luas dan komprehensif karena mencakup seluruh sektor dan setiap aktivitas yang menyimpan, menggunakan, serta mengungkapkan data pribadi. Sedangkan PDPA lebih berfokus kepada organisasi yang mengumpulkan, menggunakan, atau mengungkapkan data pribadi dalam konteks bisnis atau pekerjaan mereka. Hal ini dikarenakan organisasi seringkali memiliki akses ke data pribadi individunya, dan pengaturan ini bertujuan untuk memastikan bahwa organisasi tersebut memperlakukan data pribadi tersebut dengan benar dan sesuai hukumnya.

b. Tujuan Pengaturan

UU PDP milik Indonesia memberikan landasan hukum untuk keamanan atas data pribadi, menjamin hak warga negara atas perlindungan diri pribadi, dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Sedangkan PDPA Singapura mengatur pengumpulan, penggunaan dan pengungkapan data pribadi oleh organisasi dengan cara mengakui hak individu untuk melindungi data pribadi mereka dan kebutuhan organisasi untuk mengumpulkan, menggunakan, atau mengungkapkan data pribadi untuk tujuan yang sah oleh subjek data dalam data tersebut. Dengan demikian

penekanan regulasi dan kebijakan dalam UU PDP lebih kepada hak subjek data pribadi akan tetapi termasuk juga kepada kewajiban dari pengendali data pribadi. Sedangkan dalam PDPA Singapura regulasi dan kebijakan berdasar dari hak subjek data pribadi untuk merumuskan kebijakan terhadap pengendali data pribadinya yang dalam hal ini adalah organisasi.

c. Definisi Data Pribadi

"Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik." (Pasal 1 ayat (1) UU PDP). Sedangkan dalam PDPA didefinisikan yakni *"personal data" means data, whether true or not, about an individual who can be identified —*

(a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access.(Pasal 2 ayat (1) PDPA)

Terjemahan bebas:

"data pribadi" berarti data, baik benar atau tidak, tentang seorang individu yang dapat diidentifikasi –

(a) dari data tersebut; atau

(b) dari data dan informasi lain yang dapat diakses atau mungkin dapat diakses oleh organisasi;

Dengan demikian UU PDP memberikan definisi yang lebih luas mengenai data pribadi, mencakup informasi yang dapat diidentifikasi secara langsung atau tidak langsung, sedangkan PDPA Singapura lebih fokus pada informasi yang dapat diidentifikasi secara langsung.

d. Ruang Lingkup Perlindungan

UU PDP mengidentifikasikan bahwa perlindungan data merupakan keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. sedangkan PDPA mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi, dan termasuk menetapkan *Do Not Call Register* dan untuk menyediakan administrasinya, dan untuk hal-hal yang terkait dengannya. Dengan demikian kedua undang-undang memberikan hak kepada subjek data untuk mengakses, mengoreksi, dan menghapus data pribadi mereka. Namun, PDPA Singapura juga memberikan hak kepada subjek

data untuk menolak penggunaan data pribadi mereka untuk tujuan pemasaran melalui ketentuan *Do Not Call Register* yang merupakan kebijakan bahwa masyarakat memiliki hak untuk menerima maupun menolak pesan singkat (SMS atau MMS) dari pihak ataupun organsiasi marketing yang tidak diinginkan.

e. Aspek Lembaga Perlindungan Data Pribadi

Indonesia belum memiliki lembaga khusus yang menangani permasalahan data pribadi, adapun hal ini termasuk juga dengan peraturan turunan yang mengatur secara jelas mengenai aspek tersebut. Sedangkan Singapura dalam melakukan perlindungan data sebagai bentuk penegakan dan efektivitas berlakunya aturan PDPA dibentuk *Personal Data Protection Commission* (PDPC) yang bertugas sebagai pemantau dalam pelaksanaan aturan serta berwenang dalam menerima pengaduan dari masyarakat umum dan sebagai fasilitator dalam penyelesaian sengketa alternatif. Dengan demikian PDPA sudah tercantum lembaga otoritas yang menegakkan pengaturan ini yakni *Personal Data Protection Comission* (PDPC), sedangkan di Indonesia karena masih termasuk undang-undang baru dan masih masa transisi selama 2 tahun maka peraturan turunan dan lembaga yang berwenang belum diatur secara komprehensif.

f. Sanksi

UU PDP mengatur sanksi yang diberikan dapat berupa sanksi administratif dan sanksi pidana. Sanksi administratif yang dapat dikenakan berupa teguran tertulis, peringatan, pembatasan atau penghentian sementara kegiatan pengolahan data pribadi, pencabutan izin pengolahan data pribadi, dan/atau denda administratif. Besarnya denda administratif dapat mencapai maksimal 2% dari total omzet tahunan. Sementara itu, sanksi pidana yang dapat dikenakan berupa pidana penjara dan/atau denda. Pelanggar yang melakukan tindakan pidana dapat dikenakan hukuman penjara maksimal 5 tahun dan/atau denda maksimal 5 miliar rupiah. Sedangkan PDPA menetapkan sanksi bagi organisasi atau individu yang melanggar ketentuan UU ini. Sanksi tersebut termasuk denda hingga $1 juta atau 10% dari pendapatan tahunan organisasi, mana yang lebih tinggi, serta hukuman penjara hingga 3 tahun. Selain itu, individu yang melanggar UU ini dapat dikenakan denda hingga$5.000 atau hukuman penjara hingga 2 tahun atau keduanya. UU ini juga memberikan hak kepada individu untuk mengajukan tuntutan pribadi terhadap organisasi yang

melanggar UU ini. Dengan demikian PDPA Singapura memberikan sanksi yang lebih berat dibandingkan UU PDP.

KESIMPULAN

1) Perlindungan data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur mengenai beberapa hal yakni: pengumpulan data pribadi, informasi pribadi hanya dapat digunakan sesuai dengan alasan perolehannya, keamanan data pribadi perlu dilindungi dari akses yang melanggar hukum, wewenang untuk mengungkapkan dan mengelola informasi pribadi, termasuk juga pemindahan data pribadi. Adapun konsep cyber security yang diwakili oleh *Confidentiality* (Kerahasiaan), *Integrity* (Integritas), dan *Availability* (Ketersediaan) telah terwujud dalam kebijakan dan regulasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.
2) Perbandingan sistem perlindungan data pribadi di Indonesia dan Singapura kaitannya dengan regulasi dan kebijakan yang diterapkan dalam peraturan Singapura yakni *The Personal Data Protection Act No.26 of 2012 Singapore* (PDPA). Untuk praktik perlindungan data pribadi di Singapura itu sendiri, dalam melakukan penegakan dan efektifitas berlakunya aturan ini, dihadirkan *Personal Data Protection Commission* (PDPC) sedangkan Indonesia belum mengatur secara khusus mengenai lembaga yang berwenang dalam menegakkan perlindungan data masyarakatnya. Dalam hal kelebihan, kedua undang-undang tersebut memiliki tujuan yang sama yaitu melindungi data pribadi dan hak-hak subjek data. Selain itu, kedua undang-undang juga mengatur mengenai kewajiban pengendali data untuk memproses data pribadi dengan cara yang benar dan adil serta memberikan hak kepada subjek data untuk mengakses, mengoreksi, dan menghapus data pribadi mereka. Namun, dalam hal kekurangan, PDPA lebih fokus pada perlindungan data pribadi dalam konteks bisnis dan perdagangan elektronik, sedangkan Undang-Undang Nomor 27 Tahun 2022 mencakup semua sektor dan aktivitas yang memproses data pribadi. Dalam PDPA juga terdapat kebijakan *Do-Not Call Registry* yang merupakan kebijakan bahwa masyarakat memiliki hak untuk menerima maupun menolak pesan singkat (SMS atau MMS) dari pihak ataupun organsiasi marketing yang tidak diinginkan.

DAFTAR PUSTAKA

Abdul Rokhim, Sri Ayu Lestari, (2019). Implementasi Media Visualisasi 360 Pada Platform Android Untuk Promosi Penjualan Kendaraan Bekas, Jurnal Teknika, Vol.11 (No.2),

Ahmad Syaifudin, (2021). Standar Profesi Hukum dan Kontribusi Pendidikan Tinggi dalam Mewujudkan Profesi Hukum yang Profesional di Era Disruptif, Yurispruden, Vol.4 (No.1)

Ananthia Ayu D., Titis Anindyajati, dan Abdul Ghoffar. (2019). Perlindungan Hak Privasi Data Diri di Era Ekonomi Digital. Jakarta: Pusat Penelitian dan Pengkajian Perkara Perpustakaan Kepaniteraan dan Sekretariat Jenderal Mahkamah Konstitusi,

Antara, Andi Firdausi, dan Pri. "Data eHAC milik 1,3 Juta penggunanya dilaporkan bocor, Keamanan Data Tidak Prioritas". BBC News Indonesia. Diakses 8 Januari 2024. https://www.bbc.com/indonesia/indonesia-58393345

Ayomi Amindoni. "BPJS Kesehatan: Data Ratusan Juta Peserta Diduga Bocor, Otomatis yang Dirugikan Masyarakat". BBC News Indonesia. Diakses pada 8 Januari 2024. https://www.bbc.com/indonesia/indonesia-57196905

C.Junian, (2008). Pengembangan Kebijakan Keamanan Informasi pada Perusahaan Jasa Layanan Kurir, Jakarta: Universitas Indonesia

Fitria Dewi Navisa, Hukum Kenotariatan Indonesia Jilid I, Media Sains Indonesia (2022)

----------, Perlindungan Hukum Atas Kebocoran Data Dan Informasi Pribadi Pada Penumpang Transportasi Udara, Yurispruden: Jurnal Fakultas Hukum Universitas Islam Malang Vol. 5 No. 1 (2022)

M. Fahrudin Andriyansyah, (2020). Peran Partai Politik Lokal dalam Penyelenggaraan Otonomi Khusus di Provinsi Aceh, Yurispruden, Vol.3 (No.1)

Muchsin, (2003). Perlindungan dan Kepastian Hukum bagi Investor di Indonesia, (Surakarta: magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret

Personal Data Protection Act 2012

Pitra Winarianto, Daniel Eduardo Daud, CIA Triad, https://student-activity.binus.ac.id/csc/2022/08/cia-triad/, diakses pada 15 Januari 2024 pukul 00.33 wib

Satrio Pangarso Wisanggeni. "Data Pribadi 2,3 Juta Penduduk Indonesia Bocor". Kompas.id. Diakses 8 Januari 2024. https://www.kompas.id/baca/ilmu-pengetahuan-teknologi/2020/05/22/ data-pribadi-23-juta-penduduk-indonesia-bocor

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Wahyunanda Kusuma Pertiwi dan Yudha Pratomo. "Data 91 Juta Pengguna Tokopedia dan 7 Juta Merchant Dilaporkan Dijual di Dark Web". Kompas.com. Diakses 8 Januari 2024. https://tekno.kompas.com/read/2020/05/03/10203107/data-91-juta-pengguna-tokopedia-dan-7-juta-merchant-dilaporkan-dijual-di-dark.

Yusnita Sari, I., Muttaqin, Jamaludin, Simarmata, J., Rahman, M. A., Iskandar, A., Fernando, A., Sugianto, Giap, Y. C., & Hazriani. (2020). Keamanan Data Dan Informasi.