Jurnal Ilmu Hukum Sui Generis
Volume 4 Nomor 3, Juli 2024
E-ISSN : 2964-2337

PERLINDUNGAN HUKUM BAGI KONSUMEN TERHADAP KEBOCORAN DATA PRIBADI BERDASARKAN PASAL 16 AYAT 2 HURUF E UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI

Kadek Nova Adistiya[1], Si Ngurah Ardhya[2], Putu Riski Ananda Kusuma[3]
Muhamad Jodi Setianto [4]

Program Studi Ilmu Hukum
Universitas Pendidikan Ganesha
Singaraja, Indonesia
e-mail: {nova.adistiya@undiksha.ac.id, ngurah.ardhya@undiksha.ac.id, pkusuma@undiksha.ac.id, jodi.setianto@undiksha.ac.id}

Abstrak

Penelitian ini bertujuan (1) untuk mengetahui bagaiman perlindungan hukum terhadap konsumen terkait kebocoran data pribadi dalam prespektif perbandingan, (2) mengetahui bagaiman upaya hukum bagi konsumen yang mengalami kerugian akibat kebocoran data pribadi. Jenis Penlitain yang digunakan oleh peneliti adalah penelitian hukum normatif, yakni melalui pendekatan peraturan perundang – undangan, pendekatan konseptual, dan pendekatan komfaratif. Penelitian ini didukung dengan bahan hukum yang terdiri dari peraturan perundang-undangan, jurnal, artikel, literatur-literatur serta karya tulis ilmiah yang relevan dengan dengan pokok permasalahan yang dikaji. Hasil penelitian menunjukkan bahwa (1) adanya perbandingan antara *Personal Data Protection Act 2020* (PDPA) milik negara Singapura dengan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (UU PDP) adalah dalam lingkup regulasi, tujuan pengaturan, definisi data pribadi, ruang lingkup perlindungan, aspek lembaga, dan sanksi yang dikenakan. (2) UU PDP telah mewujudkan 3 indikator *cyber security* yakni *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) sehingga telah melindungi data pribadi masyarakat Indonesia namun perlu adanya amandemen pada UU PDP dikarenaka masih adanya beberapa pasal yang dapat mengurangi atau malah menghilangkan perlindungan hukum bagi konsumen, Lalu pemerintah juga harus membuat lembaga yang khusus untuk menangani kebocoran data pribadi di Indonesia seperti yang sudah dilakukan oleh Singapura, hal tersebut dapat membantu masyarakat untuk mempermudah pelaporan dan penanganan jika terjadi kebocoran data pribadi. Adanya upaya hukum yang dapat dilakukan bagi konsumen yang mengalami kerugian akibat kebocoran data untuk menjamin hak dari konsumen.

Kata Kunci: Kebocoran Data Pribadi, UU PDP, *Personal Data Protection Act 2020*

Abstract

This research aims (1) to find out how legal protection is for consumers regarding personal data leaks in a comparative perspective, (2) to find out what legal

remedies are for consumers who experience losses due to personal data leaks. The type of research used by researchers is normative legal research, namely through a statutory and regulatory approach, a conceptual approach and a comparative approach. This research is supported by legal materials consisting of statutory regulations, journals, articles, literature and scientific papers that are relevant to the subject matter being studied. The results of the research show that (1) there is a comparison between the Personal Data Protection Act 2020 (PDPA) belonging to the Singapore state and Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) within the scope of regulation, regulatory objectives, definition of personal data, scope scope of protection, institutional aspects, and sanctions imposed. (2) The PDP Law has created 3 cyber security indicators, namely Confidentiality, Integrity, and Availability so that it has protected the personal data of the Indonesian people, but there needs to be an amendment to the PDP Law because there are still several articles that can reduce or instead eliminating legal protection for consumers, the government must also create a special institution to handle personal data leaks in Indonesia as has been done by Singapore, this can help the public to make reporting and handling easier if personal data leaks occur. Then there are legal remedies that can be taken for consumers who experience losses due to data leaks to guarantee consumer rights.
Keywords: *Personal Data Leak, Article 16 Paragraph 2 Letter E PDP Law, Personal Data Protection Act 2020*

PENDAHULUAN

Perkembangan Zaman yang semakin maju seperti saat ini membuat segala sesuatu bisa diakses hanya dengan internet, dengan kebebasan yang ada sekarang dan didukung oleh perangkat elektronik yang praktis seperti komputer, smartphone sampai dengan jaringan yang bagus, memudahkan orang untuk bisa mengakses segala hal termasuk data pribadi orang lain (Kautsar, 2023). Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah orang yang terhubung dengan internet di Indonesia sudah mencapai 78,19 persen pada tahun 2023 atau sekitar 215.626.156 orang dari total penduduk yang berjumlah 275.773.901 orang. Pada tahun ini, penetrasi internet di Indonesia naik sebesar 1,17 persen (APJII, 2023). Kenaikan penetrasi ini masih dipengaruhi oleh penggunaan internet yang semakin jadi keperluan masyarakat, terutama sejak pandemi Covid-19 pada tahun 2020.

Dengan meningkatnya pengguna internet di Indonesia itu juga berdampak pada privasi data pribadi dari pengguna internet di Indonesia. Seperti kasus yang terjadi pada aplikasi Tokopedia dimana mengalami kebocoran data, kebocoran data adalah suatu kondisi dimana data sensitif secara sengaja atau tidak sengaja terexpose atau terakses oleh pihak tidak sah. Pada bulan maret 2020 tokopedia mengalami kebocoran data yang menyebabkan 91 juta akun pengguna Tokopedia dan 7 juta akun pedagang mengalai kebocoran yang diakibaktan serangan peratas yang selanjutnya dijual di website darkweb, data yang bocor dan dijual adalah data nama, user id, password, nomer hp, jenis kelamin, dan juga tanggal lahir (CNN Indonesia, 2020).

Tidak hanya kasus tersebut, pada tahun 2020 sampai dengan 2023 sering terjadi kebocoran data akibat serangan dari peretas, salah satu peretas yang terkenal bernama Bjorka, pada tahun 2022 Bjorka telah meretas history browsing pelanggan Indihome, data yang bocor sebanyak 26 juta data dimulai dari nama, jenis kelamin, keyword, serta Nomor Induk Kependudukan (NIK) para pelanggan Indihome. Selanjutnya kebocoran data Kementerian Komunikasi dan Informatika (Kominfo) yaitu registrasi SIM Card sebanyak 1,3 miliar data. Pada tanggal 6 september 2022, 105 juta data pemilih bocor yang berasal dari Komisi Pemilihan Umum (KPU), bahkan dokumen rahasia milik Presiden Jokowi juga bocor, dokumen tersebut didapat dari Badan Intelijen Negara (BIN).

Ada beberapa faktor yang menyebabkan data pribadi bocor di Indonesia, namun ada 3 faktor yang paling utama, yaitu: pertama, faktor Standar Operasional Prosedur (SOP), kedua, faktor Sumber Daya Manusia (SDM) dan ketiga, faktor Teknologi (Lahur, 2022).

Faktor Standar Operasional Prosedur (SOP):

1. Ketidaksesuaian SOP: Banyak organisasi atau lembaga di Indonesia mungkin memiliki SOP yang tidak memadai atau tidak diterapkan dengan benar. Misalnya, dalam perusahaan yang tidak memiliki SOP yang ketat dalam mengelola dan melindungi data pribadi, risiko kebocoran data menjadi lebih besar.
2. Ketidaktransparan dan lemahnya regulasi: Kurangnya regulasi yang ketat dan transparan dalam mengatur perlindungan data pribadi dapat menyebabkan SOP yang lemah. Organisasi mungkin tidak merasa terdorong untuk mengimplementasikan langkah-langkah yang memadai untuk melindungi data pribadi.

Faktor Sumber Daya Manusia (SDM):

1. Pelatihan yang kurang: Kurangnya pelatihan bagi petugas mengenai pentingnya keamanan data dan tindakan yang harus diambil dalam melindungi data pribadi dapat menyebabkan kesalahan manusia yang mengarah pada kebocoran data.
2. Penyusupan atau kolusi: Beberapa kasus kebocoran data yang disebabkan oleh petugas yang dengan sengaja atau tidak sengaja membagikan data pribadi dengan pihak ketiga atau melibatkan diri dalam tindakan yang merugikan perusahaan.

Faktor Teknologi:

1. Keamanan TI yang lemah: Jika sistem dan perangkat lunak yang digunakan oleh sebuah organisasi memiliki keamanan yang lemah, maka data pribadi dapat lebih mudah diakses oleh pihak yang tidak berwenang. Contoh-contoh termasuk kekurangan pembaruan perangkat lunak, konfigurasi yang buruk, dan ketidakmampuan untuk mendeteksi serangan siber.
2. Serangan siber: Penyusupan oleh peretas atau serangan siber dapat menjadi penyebab kebocoran data. Penyerang dapat mencuri data pribadi atau merusak sistem, yang dapat mengakibatkan kebocoran data.

Saat ini peraturan mengenai perlindungan data pribadi sudah secara terperinci diatur dalam Undang-Undang Perlindungan Data Pribadi yang disahkan pada September 2022, yang mana sudah dirancang dari tahun 2019 oleh Kementerian

Komunikasi dan Informatika Republik Indonesia. Di Undang- Undang ini mengatur bahwa tidak hanya pemerintah yang menjadi prosesor dan pengendali data pribadi namun, setiap orang hingga organisasi/institusi (Kautsar, 2023). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) adalah undang-undang yang mengatur mengenai hak dan kewajiban subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi dalam pemrosesan data pribadi, baik secara elektronik maupun nonelektronik. UU PDP bertujuan untuk melindungi data pribadi sebagai salah satu hak asasi manusia yang merupakan bagian dari pelindungan diri pribadi, sesuai dengan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. UU PDP juga dimaksudkan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya pelindungan data pribadi.

UU PDP mengatur mengenai asas, jenis, hak, pemrosesan, transfer, sanksi, kelembagaan, kerja sama internasional, partisipasi masyarakat, penyelesaian sengketa dan hukum acara, larangan, dan ketentuan pidana terkait pelindungan data pribadi. Undang-Undang bertujuan untuk mengurangi terjadinya kebocoran data masyarakat. UU PDP membuat system pemerintahan yang lebih efektif dan efesien dalam memberikan bantuan pelayanan terhadap masyarakat, Undang-Undang ini diharapkan mampu menjamin perlindungan hukum bagi data pribadi konsumen. Dalam pasal 16 ayat 2 huruf E UU PDP menyatakan 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 namun masih ada pasal dalam UU PDP yang belum secara jelas mengatur mengenai perlindungan data pribadi.

Contohnya pada pasal 2 ayat 2 UU PDP yang menyatakan Undang-Undang ini tidak berlaku untuk pemrosesan data pribadi oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga. Pasal ini tidak jelas mengatur bagaimana batasan kegiatan pribadi atau rumah tangga yang dikecualikan dari perlindungan data pribadi. Pasal ini juga bisa menimbulkan multitafsir dalam praktiknya, misalnya apakah data pribadi yang diproses oleh orang perseorangan untuk kepentingan bisnis atau pekerjaan masih termasuk kegiatan pribadi atau tidak.

Berdasarkan latar belakang diatas mengenai masih banyaknya hal yang perlu dianalisa dengan mendalam mengenai perlindungan hukum bagi konsumen yang mengalami kebocoran data, maka peneliti tertarik untuk melakukan penelitian yang dituangkan dengan judul ***"PERLINDUNGAN HUKUM BAGI KONSUMEN TERHADAP KEBOCORAN DATA PRIBADI BERDASARKAN PASAL 16 AYAT 2 HURUF E UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI"***

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif dikarenakan di dalam Undang-Undang Perlindungan Data Pribadi masih adanya beberapa pasal yang dapat mengurangin atau malah menghilangkan perlindungan hukum bagi konsumen yang menjadikan UU PDP ini tidak sesuai dengan tujuannya untuk melindungin data pribad, dalam pelaksanaannya masih ada kekaburan hukum

dalam pengaturan perlindungan data pribadi. Penelitian ini menggunakan sumber bahan hukum primer dan bahan hukum sekunder bahan hukum primer terdiri peraturan perundang-undangan, catatan-catatan resmi, atau risalah dalam pembuatan peraturan perundang-undangan dan putusan-putusan hakim dan sekunder yang di gunakan dalam penelitian ini bersumber dari bahan-bahan kepustakaan, buku-buku literatur hukum, jurnal, pendapat para ahli yang berkaitan dengan pokok bahasan di penelitian ini. Selanjutnya data yang diperoleh akan dianalisis dan disajikan dalam bentuk kualitatif.

HASIL DAN PEMBAHASAN

Perlindungan Hukum Terhadap Konsumen Terkait Kebocoran Data Pribadi Dalam Prespektif Perbandingan

Perlindungan data pribadi di Indonesia.

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 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.

Pada pasal 16 ayat (2) huruf e UU PDP 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."

Bisa dikatakan pada pasal 16 ayat (2) huruf e menyatakan hak subjek data pribadi dimana menyebutkan melindungi keamanan data pribadi, namun pada UU PDP ini masih memiliki beberapa kekurangan. Misalnya pada pasal 2 ayat (2) disebutkan "Undang-undang ini tidak berlaku terhadap pengolahan data pribadi yang dilakukan oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga" kalimat ini bisa dikatakan lemah dan dapat menimbulkan istilah negatif dalam penafsirannya karena pasal ini tidak secara jelas mengatur mengenai pengecualian pada kalimat "orang perseorangan dalam kegiatan pribadi" yang dapat mengakibatkan tidak berlakunya undang-undang ini dalam mengatasi pembobolan data yang dilakukan oleh peratas yang pada dasarnya hanya untuk kepentingan pribadi, padahal dalam pasal 18 ayat (1) disebutkan bahwa pengolahan data pribadi dapat dilakukan oleh 2 (dua) orang atau lebih pengontrol data" maka dapat diartikan jika seseorang menggunakan data orang lain secara pribadi atau rumah tangga, aturan ini tidak dapat digunakan karena tidak ada hubungannya dengan kegiatan profesional atau komersial.

Pasal 56 ayat (1) Bab VII menyatakan bahwa pengendali data pribadi dapat mentransfer data pribadi kepada pengendali data pribadi dan/atau pengolah data pribadi di luar wilayah hukum Negara Republik Indonesia sesuai dengan ketentuan yang diatur dalam Undang-Undang ini, namun dalam ayat (1) hal ini tidak menjelaskan tidak adanya frasa "dengan persetujuan pemilik data pribadi" maka hal tersebut merupakan kelemahan mutlak sehingga bertentangan dengan tujuan utama dibentuknya Undang-Undang Perlindungan Data Pribadi, sehingga dalam pasal 56 tidak memberikan nilai tambah terhadap perlindungan data pribadi di dalam dan luar negeri. Oleh karena itu perlu adanya perbandingan dengan undang-undang tentang perlindungan data pribadi dari negara lain untuk memperbaiki kekurangan-kekurangan pada UU PDP di Indonesia.

Perlindungan data Pribadi di Singapura.

Di negara Singapura, perlindungan terhadap data pribadi diatur dalam Personal Data Protection Act 2012 yang sudah diamandemen menjadi Personal Data Protection (Amendment) Act 2020 (yang 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 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.

Dalam Pasal 322 PDPA disebutkan bahwa:

"Tujuan dari Undang-undang ini adalah untuk mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi dengan cara yang mengakui baik hak individu untuk melindungi data pribadi mereka dan kebutuhan organisasi untuk mengumpulkan, menggunakan atau mengungkapkan data pribadi untuk tujuan yang masuk akal akan menganggapnya tepat dalam situasi tersebut."

Perbandingan perlindungan data

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 (Amendment) Act 2020 (PDPA) :

1. 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.
2. Tujuan Pengaturan

   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.
3. Definisi Data Pribadi

   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. Maksud dari informasi yang dapat diindetifikasi secara langsung atau tidak langsung adalah :

   a. Identifikasi Secara Langsung: Ini merujuk pada informasi yang dengan jelas mengidentifikasi seseorang. Contohnya termasuk nama lengkap, nomor identifikasi (seperti KTP atau paspor), alamat rumah, nomor telepon, dan alamat email. Informasi ini dapat langsung menghubungkan data dengan individu tertentu.
   b. Identifikasi Tidak Langsung: Ini melibatkan informasi yang, meskipun tidak langsung mengidentifikasi seseorang, masih dapat digunakan untuk mengidentifikasi mereka jika dikombinasikan dengan data lain. Contohnya

termasuk alamat IP, alamat MAC, nomor rekening bank, dan data geografis. Meskipun ini tidak langsung mengungkap identitas, tetapi dapat membantu mengidentifikasi individu jika dikaitkan dengan informasi lain.

4. 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. 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.

5. 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 maka lembaga yang berwenang belum diatur secara komprehensif.

6. Sanksi

UU PDP mengatur sanksi yang diberikan dapat berupa sanksi administratif dan sanksi pidana. Sanksi administratif pada pasal 57 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 pada pasal 67 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 diatur dalam pasal 67 yaitu dikenakan 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 pada pasal 21 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.

Upaya Hukum Bagi Konsumen Yang Mengalami Kerugian Akibat

Kebocoran Data Pribadi.

Perlindungan konsumen telah dibentuk dan dibuat beberapa puluhan tahun lalu diseluruh belahan dunia dan sampai saat ini sudah ada beberapa negara yang telah mempunyai norma khusus atau undang-undang yang mampu memberikan keamanan dan kepastian hukum terhadap konsumen, termasuk memfasilitasi sarana peradilannya. sejalan dengan adanya hal tersebut, berbagai belahan negara telah memastikan dan mengesahkan hak-hak konsumen yang digunakan sebagai pedoman dan landasan pengaturan perlindungan kepada konsumen (Wahyudi, 2023).

Dengan banyaknya kasus kebocoran data yang terjadi di Indonesia menyebabkan terjadinya ketakutan dimasyarakat terutama konsumen, karena hal tersebut perlu adanya tindakan pencegahan atau upaya apa yang dapat mereka lakukan jika data pribadi mereka mengalami kebocoran, oleh karena itu perlunya adanya upaya pencegahan baik dari pemerintah, dari prosesor data, dan juga masyarakat untuk melalukan pencegahan untuk mencegah atau mengurangi dampak dari kebocoran data bila terjadi kebocoran data. Lalu juga perlu untuk diketahui masyarakat sebagai konsumen dapat melakukan upaya hukum jika kebocoran data terjadi dan mengakibatkan kerugian baik secara materiil maupun immaterial.

Kebocoran yang sering terjadi di Indonesia disebabkan lemahnya cyber security di Indonesia, oleh karena itu perlu adanya cyber security di Indonesia, cyber security merupakan sebuah praktik untuk melindungi sistem teknologi dan perangkat seperti komputer, seluler, server, sistem elektronik dan data suatu perusahaan. Sehubungan dengan itu korelasi antara perlindungan data pribadi terhadap perwujudan cyber security didasarkan pada kasus-kasus peretasan data yang terjadi beberapa tahun ini, dari tahun 2019-2024. 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. Ketiga konsep ini merupakan panduan dalam membentuk sistem, prosedur, ataupun kebijakan yang berhubungan dengan keamanan informasi. 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 ketiga konsep tersebut sudah terwujud pada pasal-pasal Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Dalam upaya pencegahan pemerintah juga harus mengamandemen Undang-

Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dikarenaka masih adanya beberapa pasal yang dapat mengurangin atau malah menghilangkan perlindungan hukum bagi konsumen yang menjadikan UU PDP ini tidak sesuai dengan tujuannya untuk melindungin data pribadi dari masyarakat dalam hal ini konsumen. Lalu pemerintah juga harus membuat lembaga yang khusus untuk menangani kebocoran data pribadi di Indonesia seperti yang sudah dilakukan oleh Singapura, hal tersebut dapat membantu masyarakat untuk mempermudah pelaporan dan penanganan jika terjadi kebocoran data pribadi.

Upaya hukum yang dapat dilakukan konsumen yang mengalami kerugian akibat kebocoran data pribadi. Dengan banyaknya kasus kebocaran data pribadi hal tersebut menimbulkan ancaman yang lebih serius seiring dengan meningkatnya kemungkinan individu menderita kerugian sebagai akibat dari kebocoran data pribadi. Kebocoran data pribadi yang dikelola oleh suatu perusahaan, maka itu adalah tanggungjawab perusahaan tersebut baik diretas oleh pihak ketiga maupun sengaja dibocorkan. Perusahaan e-commerce digolongkan sebagai pengendali data pribadi yang berbentuk korporasi yang tunduk pada ketentuan pelindungan data pribadi dalam Undang-Undang Perlindungan Data Pribadi. Jual beli secara online atau pemindahan Kepemilikan dari pengusaha kepada konsumen, harus ada akad.

Transaksi E-Commerce hampir sama dengan transaksi yang dilakukan secara konvensional, tidak ada transaksi tanpa adanya perjanjian antar pihak dan sepakat dalam sebuah perikatan, dalam hal ini, perjanjian yang dilakukan oleh para pihak adalah perjanjian jual beli yang dikenal dengan kontrak elektronik. Kontrak elektronik atau electronic contract, merupakan perikatan ataupun hubungan hukum yang dilakukan secara elektronik dengan memadukan jaringan (networking) dari system informasi berbasiskan komputer (computer cased information system) (suadi, 2021). Setelah kita memasukkan data pribadi kita ke dalam aplikasi e-commerce, aplikasi belanja online biasanya menjelaskan kontrak antara pengguna/konsumen aplikasi di website, dalam kontrak yang dinyatakan oleh toko online itu sendiri atau secara sepihak, kita sebagai pengguna hanya disediakan sebuah kolom untuk dicentang sebagai persetujuan, apakah kita sepakat dengan perjanjian yang tertera atau tidak. Maka, tidak adanya peran kita sebagai konsumen untuk ikut andil dalam menyusun perjanjian.

Berdasarkan Pasal 46 ayat (1) Dalam hal terjadi kegagalan Pelindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3 x 24 (tiga kali dua puluh empat) jam kepada:

1. Subjek data pribadi
2. Lembaga

Pemberitahuan tersebut harus memuat data pribadi yang terungkap, kapan dan bagaimana data pribadi tersebut bocor, serta upaya penanganan serta pemulihan kebocoran data pribadi. Dan jika kebocoran data yang terjadi hingga menggagu kenyamanan publik atau berdampak serius terhadap masyarakat maka perusahaan wajib memberitahukan kepada masyarakat. Dalam Undang-Undang Perlindungan Data Pribadi, pengendali data pribadi yang tidak mengumumkan kebocoran data pribadi yang telah terjadi, dapat dikenai sanksi administratif berupa:

1. Peringatan tertulis;
2. Penghentian sementara semua kegiatan pemrosesan data pribadi;

3. Penghapusan atau pemusnahan data pribadi; dan/atau
4. Denda administratif dikenakan paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Dalam perkara ini, Selain sanksi administratif, pengguna yang dirugikan dapat menuntut secara perdata atas data pribadi yang diungkapkan. Hal ini tertuang dalam Pasal 12 ayat (1) Undang-Undang Perlindungan Data Pribadi, dimana individu yang memiliki data pribadi (pengguna) berhak mengajukan gugatan dan mendapatkan ganti rugi atas pelanggaran pengolahan data pribadi sesuai dengan undang-undang. Dan pengguna yang telah dirugikan dapat menggugat dengan Pasal 1365 KUHPerdata tentang perbuatan melawan hukum. Dalam kasus diatas pengguna (korban) dapat melaporkan dengan dasar wanprestasi dimana perusahaan telah lalai atas perjanjian yang dibuat pertama kali antara konsumen dengan perusahaan, maka korban dapat menggugat dengan dasar wanprestasi, sanksi hukum pelaku wanprestasi ada diataranya:

1. Membayar ganti rugi yang diderita kreditur berdasarkan Pasal 1243 KUHPerdata
2. Pembatalan perjanjian berdasarkan Pasal 1266 atau Pasal 138 ayat (2) KUHPerdata
3. Peralihhan risiko karena terjadinya Force Majure dan menyebabkan wanprestasi
4. Pembayaran biaya perkara yang hanya dapat dimintakan bila sudah terbukti di muka hakim dengan penetapan dari hakim.

Lalu berdasarkan Pasal 64 ayat (1), (2), (3), (4) Penyelesaian sengketa Perlindungan Data Pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan ketentuan peraturan perundang-undangan. Lalu proses peradilan Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan perundang-undangan. Dan persidangan dilakukan secara tertutup demi melindungi data pribadi.

KESIMPULAN DAN SARAN

Berdasarkan uraian tersebut di atas, penulis mengemukakan kesimpulan sebagai berikut :

1. Perbandingan sistem perlindungan data pribadi di Indonesia dan Singapura kaitannya dengan regulasi dan kebijakan yang diterapkan dalam peraturan Singapura yakni Personal Data Protection (Amendment) Act 2020 Singapura (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.
2. Dengan berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dapat dikatakan sebagai solusi atas kebocoran data pribadi yang sudah menjadi hal umum saat ini. Undang-Undang Perlindungan Data Pribadi ini mentetapkan berdasarakan Pasal 35 bahwa pengendali data berkewajiban melakukan pengawasan lalu menjaga keamanan dari data pribadi

konsumen, maka jika terjadi kebocoran data baik oleh pihak ketiga maka yang bertanggung jawab tetap pengendali data. Dan jika terjadi kegagalan dalam penjagaan data pribadi maka pengendali data akan dikenakan sanksi administratif. Oleh karena itu Undang-Undang Perlindungan Data Pribadi menjadi payung hukum yang tepat saat dimana maraknya kebocoran data pribadi terjadi.

Adapun selanjutnya, berdasarkan pada penelitian ini, maka terdapat sejumlah saran yang dapat diusulkan kepada beberapa pihak terkait Perlindungan Data Pribadi, yakni sebagai berikut :

1. Peran pemerintah untuk melakukan amandemen pada pasal-pasal pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang masih memiliki kekurangan, lalu dapat juga melakukan pembinaan terhadap masyarakat terkait pentingnya melindungi data pribadi dengan cara iklan di televisi atau dengan memasang banner dijalanan, sebagaimana dimaksud dapat dilakukan melalui pendidikan, pelatihan, sosialisasi, dan atau pengawasan sesuai dengan ketentuan peraturan perundang-undangan. Pemerintah juga harus membentuk lembaga yang khusus untuk menangani kebocoran data pribadi di Indonesia seperti yang sudah dilakukan oleh Singapura, hal tersebut dapat membantu masyarakat untuk mempermudah pelaporan dan penanganan jika terjadi kebocoran data pribadi.
2. Peran penegak hukum, dikarenakan belum adanya lembaga yang secara khusus menangani kasus kebocoran data maka peran penegak hukum agar dapat membantu masyarakat dalam penyelesaian kasus kebocoran data pribadi yang terjadi kepada masyarakat.
3. Peran Penyedia layanan sebagai pemroses data juga harus meningkatkan standar operasional prosedur (SOP) yang ketat, meningkatkan sumber daya manusia (SDM) yang terlatih dalam keamanan data, dan meningkatkan penggunaan teknologi yang aman, untuk menunjang terlaskananya perlindungan data pribadi di oraganisasi yang memiliki data pribadi konsumen.
4. Peran masyarakat juga harus ditingkatkan dikarenakan Peran masyarakat begitu penting dalam mewujudkan berjalanya perlindungan data pribadi, karena jika masyarakat lebih teredukasi mengenai penting data pribadi itu, maka masyarakat akan lebih hati dalam menggunakan data pribadinya.

DAFTAR RUJUKAN

Kautsar, T. R. (2023). *Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi Dan Regulasi Perlindungan Data Pribadi*.

APJII. (2023). *Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang*. APJII. https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang

CNN Indonesia. (2020). *Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijual*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

Lahur, M. F. (2022). *Kominfo Sebut 3 Faktor Kebocoran Data Pribadi Terus Terjadi*. TEMPO. https://tekno.tempo.co/read/1555106/kominfo-sebut-3-faktor-kebocoran-data-pribadi-terus-terjadi

Suadi, I. P. M., Yuliartini, N. P. R., & Ardhya, S. N. (2021). Tinjauan Yuridis Subyek Hukum Dalam Transaksi Jual Beli Online / E-Commerce Ditinjau Dari Kitab Undang- Program Studi Ilmu Hukum Universitas Pendidikan Ganesha e-Journal Komunitas Yustisia Univer. *E-Journal Komunitas Yustisia Universitas Pendidikan Ganesha Program*, 4(2), 668–681.

Wahyudi, G. N., Ardhya, S. N., & Setianto, M. J. (2023). Implementasi Pasal 14 Ayat 3 Peraturan Gubernur Bali Nomor 1 Tahun 2020 Tentang Tata Kelola Minuman Fermentasi Dan / Atau Detilasi Khas Bali Terkait Peredaran Arak Bali Tanpa Label Di Kabupaten Buleleng. *Ilmu Hukum Sui Generis*, 3, 137–148.

Personal Data Protection (Amendment) Act 2020

Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi