SANKSI TERHADAP PENYELENGGARA E-COMMERCE APABILA GAGAL DALAM MELINDUNGI DATA PRIBADI PENGGUNA

Achmad Rafli Hidayah[1]

Fakultas Hukum

Universitas 17 Agustus 1945 Surabaya

Jalan Semolowaru Nomor 45, Surabaya 60118, Indonesia

raflivinci@gmail.com

Abstract

This study focuses on imposing sanctions on e-commerce providers if they fail to protect their users' personal data. The purpose of this study is to find out the sanctions given to e-commerce providers if they fail to protect the personal data of their users based on the legal basis in force in Indonesia. The method used is a normative juridical research method, which means that the approach used in conducting this research is by approaching, examining, concepts and related theories to examine the Perpu that can answer the legal issues in this research. This type of research is a study of legal systematics by conducting research that has the aim of identifying the meaning and basis of the existing law. The results of the study indicate that there is a legal basis that can ensnare e-commerce providers if they fail to protect their users' personal data.

Keywords: *Sanctions, E-Commerce Operator, Personal Data*

Abstrak

Penelitian ini berfokus pada pemberian sanksi terhadap penyelenggara e-commerce apabila gagal dalam melindungi data pribadi penggunanya. Tujuan dari penelitian ini untuk mengetahui sanksi yang diberikan terhadap penyelenggara e-commerce apabila gagal dalam melindungi data pribadi penggunanya yang berdasarkan pada dasar hukum yang berlaku di Indonesia. Metode yang digunakan adalah metode penelitian yuridis normatif yang artinya bahwa pendekatan yang digunakan dalam melakukan penelitian ini yaitu dengan cara melakukan pendekatan, menelaah, konsep-konsep serta teori-teori yang berkaitan untuk mengkaji Perpu yang dapat menjawab isu hukum dalam penelitian ini. Jenis penelitian ini merupakan penelitian terhadap sistematika hukum dengan cara melakukan penelitian yang mempunyai tujuan untuk mengidentifikasi pengertian dan dasar hukum yang ada. Hasil penelitian menunjukkan bahwa terdapat dasar hukum yang dapat menjerat penyelenggara e-commerce apabila gagal dalam melindungi data pribadi penggunanya.

Kata Kunci: Sanksi, Penyelenggara E-Commerce, Data Pribadi

Pendahuluan

Internet merupakan salah satu bentuk dari adanya perkembangan teknologi dan informasi. Internet yang pada dasarnya digunakan untuk mengakses suatu informasi secara cepat beralih menjadi fasilitas yang dapat digunakan untuk melakukan transaksi jual-beli online sehingga hal tersebut membuat internet menjadi suatu pola yang dapat mempermudah perkerjaan manusia. Dengan adanya perkembangan dari dunia teknologi, internet yang semakin cepat maka suatu informasi yang diperoleh juga dapat dengan mudah untuk dicari dan dapat dimungkinannya

[1] Fakultas Hukum Universitas 17 Agustus 1945 Surabaya, Jl. Semolowaru No. 45, Menur Pumpungan, Kec. Sukolilo, Kota Surabaya, Jawa Timur 60118 | https://orcid.org/0000-0002-2169-3630 | https://publons.com/researcher/5293084/achmad-rafli-hidayah/ |raflivinci@gmail.com

melakukan pertukaran informasi dengan melewati batas teritorial suatu negara (*cross border*) (Makarim 2014).

Dengan berkembangnya internet tidak terlepas dengan berkembangnya suatu data pribadi terhadap penggunanya. Penggunaan internet yang sangat masif dengan cepat merubah internet menjadi suatu kecanggihan teknologi yang mempunyai fleksibilitas dengan biaya yang rendah serta dapat digunakan untuk segala bidang seperti untuk hiburan, berkomunikasi, informasi dan sebagainya. Semakin berkembangnya teknologi membuat internet juga mengalami perubahan yang signifikan sehingga hal tersebut mendorong peradaban manusia menuju kearah yang lebih modern sehingga dapat menuju kepada perdagangan bebas. Perdagangan bebas merupakan suatu keadaan yang dimana proses dari perdagangan tersebut tidak mempunyai batas terhadap ruang dan waktu. Sehingga perdagangan bebas timbul akibat dari pemanfaatan yang diperoleh melalui perkembangan dari teknologi dan internet. Perkembangan teknologi membuat awal mula terbentuknya *Electronic Commerce* (Hanim 2014).

Electronic Commerce mempunyai arti yakni suatu perdagangan yang dilakukan tanpa bertemunya antara penjual dan pembeli dengan menitikberatkan kepada sistem berupa pertukaran terhadap barang atau jasa dengan melalui sistem yang berupa elektronik yaitu internet. *Electronic Commerce* menjadi dipandang oleh masyarakat karena sistem yang diberikan membuat masyarakat menjadi mudah dalam melakukan perdagangan tanpa terhalang oleh jarak dan waktu. Transaksi yang digunakan dapat dilakukan dengan cara mengirim surat elektronik, fax dan banyak lagi. Metode yang digunakan untuk pembayaran yaitu dengan cara menggunakan internet sehingga hal tersebut merupakan suatu sistem yang dapat memberikan efisiensi terhadap masyarakat yang mengaksesnya.

Dalam mengkases suatu *Electronic Commerce* masyarakat atau pengguna dituntut untuk memberikan data pribadinya yang berupa nomor rekening bank, *e-mail*, nomor telepon, identitas sesuai KTP dan sebagainya. Hal tersebut membuat *Electronic Commerce* dapat menyimpan suatu informasi dari data pribadi penggunanya yang disimpan kedalam suatu sistem yang dimiliki oleh PSE. Dengan sistem tersebut membuat adanya bentuk tindak kejahatan yang dimana tindak kejahatan tersebut dapat dilakukan dengan cara membobol terhadap suatu sistem penyimpanan data pribadi pengguna yang telah dikelola oleh PSE. Dengan adanya tindak kejahatan seperti itu, PSE dituntut untuk memberikan jaminan keamanan terhadap data pribadi penggunanya yang telah disimpannya, apabila data pribadi pengguna yang telah disimpan tersebut telah bocor atau disebarluaskan maka PSE dapat dimintai pertanggungjawaban terhadap tindak kejahatan tersebut (Rosadi 2017).

Hukum di Indonesia sampai saat ini belum memberikan kepastian dan perlindungan terhadap data pribadi warganya, hal tersebut diakibatkan karena belum adanya instansi penegak hukum yang secara khusus menangani tentang kejahatan data pribadi dan memberikan perlindungan terhadap data pribadi masyarakatnya. Kurangnya kesiapan dari hukum Indonesia dalam memberikan antisipasi terhadap perkembangan dari teknologi dapat berakibat fatal bahkan dapat mengancam warganya. UU PDP di jaman modern harus memenuhi setidaknya 3 persyaratan: (1) adalah sesuatu yang mengikat individu dan komunitas ekonomi; (2) bersifat internasional; (3) masyarakat didorong untuk menjadi bagian dari komunitas terhadap ekonomi digital (Dewi Rosadi and Gumelar Pratama 2018).

Hukum di Indonesia belum ada yang secara khusus memberikan aturan terhadap perlindungan data pribadi di tingkat UU. Menurut penelitian yang dilakukan oleh ELSAM, hukum di Indonesia mempunyai 30 ketentuan Perpu yang mengatur mengenai kewajiban negara dalam memberikan suatu bentuk perlindungan terhadap data pribadi warganya (Djafar 2019). Kekurangan dari UU 23/2006 jo. UU 24/2013 yaitu tidak memberikan penjelasan secara rinci mengenai perincian dari perolehan, pengolahan, dan penyimpanan terhadap data pribadi. Menurut Permenkominfo 20/2016 telah mengatur mengenai perlindungan data pribadi yang mencakup perlindungan terhadap perolehan, pengumpulan, penyimpanan, pengiriman, penganalisisan, penyebarluasan, penampilan, pemusnahan terhadap data pribadi.

Meskipun pengguna memiliki hak untuk menggugat jika terjadi suatu kebocoran terhadap data pribadinya dan adanya suatu tujuan dari hukum yang mendasari kasus yang terjadi tersebut, tetapi hal tersebut tidak dapat serta merta dapat membuka jalan terhadap pemilik untuk mempertahankan haknya. Bukti kehilangan karena kebocoran data pribadi harus dibuat oleh pengguna selama masa percobaan terlebih lagi tidak adanya Perpu yang secara khusus yang mengatur mengenai perlindungan data pribadi yang membuat pengguna kesulitan untuk meminta pertanggung jawaban terhadap PSE atas kebocoran data pribadi yang telah terjadi.

Metode Penelitian

Metode yang digunakan adalah metode penelitian yuridis normatif yang artinya bahwa pendekatan yang digunakan dalam melakukan penelitian ini yaitu dengan cara melakukan pendekatan, menelaah, konsep-konsep serta teori-teori yang berkaitan untuk mengkaji Perpu yang dapat menjawab isu hukum dalam penelitian ini. Jenis penelitian ini merupakan penelitian terhadap sistematika hukum dengan cara melakukan penelitian yang mempunyai tujuan untuk mengidentifikasi pengertian dan dasar hukum yang ada.

Pembahasan

Sanksi Bagi Penyelenggara E-Commerce Menurut Hukum Pidana

UUD NRI 1945 dalam Pasal 28G ayat (1) telah menyebutkan bahwa warga negara mempunyai hak untuk mendapatkan perlindungan baik untuk diri sendiri maupun keluarga. Perlindungan yang dimaksud berarti sangat luas tidak hanya untuk perlindungan terhadap diri sendiri saja melainkan dapat digunakan untuk melindungi privasi setiap warga negaranya (Saragih and others 2020). Dalam pasal tersebut telah menjelaskan bahwa perlindungan data pribadi merupakan suatu bentuk perlindungan dari negara terhadap hak privasi setiap warga negaranya untuk dapat menikmati hidup mereka tanpa harus ada ancaman terhadap mereka. Hal tersebut mempunyai tujuan yaitu hak privasi merupakan bentuk dari hak dari warga negara yang harus dihormati (Rumlus and Hartadi 2020). Pasal tersebut memberi isyarat bahwa undang-undang dan peraturan lain perlu diberlakukan agar perlindungan data pribadi dapat berfungsi dengan baik.

Ketentuan yang mengatur tentang kewajiban PSE untuk mengamankan pribadi terdapat dalam UU 11/2008 jo UU 19/2016 dan peraturan pelaksananya adalah PP 71/2019 dan Permenkominfo 20/2016. UU 11/2008 menyiratkan persetujuan pihak yang berkepentingan untuk menggunakan sistem informasi dan dalam hal hal yang tidak diinginkan, PSE wajib menghapus informasi/dokumen elektronik. Selain itu, Pasal 12 PP 71/2019 mengatur mengenai implementasi bahwa PSE wajib menerapkan manajemen risiko atas kerugian yang mungkin terjadi untuk menghindari penyalahgunaan data. Manajemen risiko ini harus dilakukan oleh operator sistem elektronik, yang menganalisis risiko dan mengatasi ancaman atau kerugian yang akan terjadi.

Upaya pencegahan juga dapat dilakukan dengan kewajiban penyelenggara sistem informasi untuk melatih pengguna sistem elektronik. Salah satu pelatihan yang perlu dilakukan adalah tidak membagikan data pribadi yang sangat penting bagi mereka dan berhati-hati dengan klasifikasi data yang mereka bagikan. Kesadaran juga dapat berhubungan dengan berbagai jenis kejahatan di dunia maya ketika mereka menyebarkan informasi pribadi mereka dengan cara yang tidak aman. Kewajiban ini diatur dalam Pasal 28 PP 71/2019. Klarifikasi tersebut meliputi hak, kewajiban dan tanggung jawab semua pihak terkait serta tata cara pengajuan pengaduan.

Kewajiban penyelenggara sistem sebagaimana dimaksud dalam Pasal 30 ayat (1) PP 71/2019 adalah kewajiban untuk menyelenggarakan fungsi sesuai dengan karakteristik sistem elektronik dalam rangka melindungi hak atau kepentingan pengguna sistem elektronik. Selain itu, ciri-ciri tersebut dimaksudkan untuk menerapkan sekurang-kurangnya relief-relief yang terdapat pada ayat (2), salah satunya melakukan koreksi. Tidak hanya pencegahan, tetapi ada juga aturan untuk pencegahan. Pasal 14 juga mengatakan PSE memiliki kewajiban dalam mematuhi prinsip perlindungan data pribadi, yang meliputi pengolahan data pribadi dengan melindungi keamanan data dari penyalahgunaan data pribadi.

PP 71/2019 mengatur bahwa PSE wajib menghapus dan menghapusnya dari mesin pencari jika informasi/dokumen elektronik tidak relevan. Ketidakrelevanan yang dimaksud adalah ketika dikumpulkan/diproses tanpa persetujuan pemiliknya, diperoleh secara melawan hukum dan dilaporkan oleh PSE yang merugikan pemilik data pribadi tersebut. Ini mungkin kasus yang sedang berlangsung bahwa diperoleh secara ilegal oleh pihak ketiga yang mencuri informasi pribadi seseorang.

Dalam hal terjadi pelanggaran data pribadi, UU 11/2008 memberikan beberapa opsi penegakan hukum. Beberapa ketentuan sanksi pidana dijelaskan di bawah ini:

a. Hukuman pidana untuk akses tidak sah atau ilegal ke perangkat elektronik tertentu untuk mendapatkan suatu informasi yang berupa elektronik;
b. Hukuman pidana untuk perbuatan melawan hukum atau melawan hukum yang mengubah, menghancurkan, mencuri, mengirimkan, mengungkapkan atau menutupi suatu informasi yang berupa elektronik maupun dokumen yang berbentuk elektronik;

Pencurian data pribadi berkaitan dengan ketentuan penegakan hukum UU 11/2008 yang berkaitan dengan perbuatan yang dilarang yaitu Pasal 30 ayat (2) UU 11/2008, menyebut bahwa setiap orang dapat dengan sengaja mengakses sistem elektronik dengan tidak memiliki hak dan melawan hukum dengan tujuan memperoleh informasi/dokumen elektronik. Melihat pasal ini, pelaku pencurian data pribadi telah memenuhi unsur Pasal 30 ayat (2) UU 11/2008. Frasa "dengan cara apa pun" dapat berarti menggunakan sistem elektronik , baik menggunakan perangkat lunak tertentu maupun tidak, yang tujuannya untuk mencuri data atau informasi dari seseorang. Hal ini sejalan dengan ketentuan Pasal 46 (2) bahwa pelaku dipidana dengan kurungan penjara paling lama tujuh tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah). Pelaku tindak pidana pencurian data siber seharusnya dituntut untuk memberikan ganti rugi dan ganti rugi kepada korban sebagai bentuk pertanggungjawaban.

Secara umum bocornya suatu data dapat terjadi melalui penyusupan akses dari luar yang mana akses tersebut menuju kedalam sistem. Tetapi, bisa jadi suatu pelanggaran tersebut telah diakibatkan oleh tindakan pelanggaran oleh orang yang memiliki kontrol khusus terhadap tersebut lalu mengirim data tersebut keluar dari sistem, dengan orang dalam tersebut diharuskan untuk

menjamin perlindungan terhadap kerahasiaan dari data milik pengguna. Sebagai pengontrol dan pemroses data, perusahaan harus bertanggung jawab secara fisik dan logis atas sistem keamanan. Setidaknya perbuatan peretasan untuk mencuri data secara mendasar dapat mengefisienkan ketentuan Pasal 30 dan 32 UU 11/2008 tentang akses tanpa izin dan penyusupan data.

Selanjutnya, pertanggung jawaban pidana, termasuk terhadap penyelenggara situs deepweb yang menjadi pasar gelap, tidak boleh dibebaskan dari tanggung jawab pidana. Pasal 480 KUHP menjelaskan bahwa KUHP melarang adanya suatu tindakan seperti memberikan data pribadi yang didapat melalui suatu kejahatan seperti memperjual belikan barang hasil curian kedalam *black market*. Selain pemain utama, tentu saja ada tindakan penyertaan yang perlu dilakukan oleh pengguna legal seperti perusahaan dan otoritas yang disengaja untuk tidak mempunyai atau merawat sistem keamanan elektronik miliknya dengan tujuan agar menangani data pribadi yang tepat. Dengan kata lain bahwa mereka mempunyai tanggungjawab dalam memfasilitasi sarana bagi publik untuk melakukan suatu tindak kejahatan. Selain itu, Pasal 65 ayat (2) KUHP telah memuat ketentuan terhadap perbuatan pidana yang dilakukan oleh Korporasi apabila Perdagangan melalui sistem elektronik melakukan perdagangan yang tidak searah dengan peraturan yang telah ditetapkan.

Peraturan tersebut mungkin terkait sudut pandang terhadap perlindungan data pribadi dari pernyataan privasi yang dikirimkan oleh PSE. Pengenaan white collar crime sangat diperlukan dalam penerapannya, agar setiap PSE sadar akan kewajiban hukumnya. Apabila berdasarkan karena rumitnya sistem elektronik, PSE cenderung mengelabui pengguna yang mengkases sistem tersebut melalui serangkaian trik melalui kode dalam sistem elektronik, atau tidak memperdulikan pembobolan dan pencurian terhadap data pengguna yang dimana hal tersebut dilakukan secara jelas. Dengan melakukan hal tersebut ada kemungkinan bahwa pihak asuransi akan mendapat keuntungan dari klaim terhadap asuransinya.

Peraturan perundang-undangan telah menjamin bahwa terdapat pengaturan mengenai data pribadi, yaitu Pasal 26 ayat (1) UU 11/2008 jo. UU 19/2016 bahwa, kecuali undang-undang dan peraturan menentukan lain, penggunaan informasi tentang data pribadi seseorang dengan sarana elektronik harus dilakukan dengan persetujuan subjek data (Saleh 2021). PP 20/2016, perlindungan data pribadi meliputi perlindungan terhadap pengumpulan, pengumpulan, pemrosesan, dan analisis, penyimpanan, tampilan, publikasi, transmisi, penyebaran, dan pemusnahan data pribadi.

Menurut Permenkominfo 20/2016, untuk menggunakan suatu sistem elektronik perlunya sertifikat dan memiliki peraturan secara internal dengan tujuan untuk melindungi data pribadi. Adapun aspek yang harus diperhatikan dalam melindungi data pribadi seperti aspek dalam penerapan teknologinya, aspek biaya dan aspek metode yang digunakan.

Pemilik data pribadi berhak atas kerahasiaan datanya, sesuai dengan menurut Permenkominfo 20/2016; Pemilik data pribadi mempunyai hak untuk mengajukan keluhan terkait penyelesaian sengketa terhadap data pribadinya; Pemilik data pribadi mempunyai hak untuk mengkases riwayat dari data pribadinya; dan Pemilik data pribadi mempunyai hak untuk penghancuran terhadap suatu data pribadinya yang telah tersimpan didalam suatu sistem secara elektronik. Hal yang telah disebutkan diatas telah terkandung dalam Pasal 26 Permenkominfo 20/2016.

Menurut UU 11/2008 jo. UU 19/2016, apabila terbukti telah terjadi tindak pidana terhadap data pribadi dengan melakukan penyalahgunaan yang dilakukan pihak ketiga dan

penyalahgunaan tersebut telah memenuhi unsur pidana dan merugikan kerugian terhadap pemilik data pribadi, maka pihak ketiga tersebut dapat dikenakan berupa kurungan penjara paling lama 12 tahun dan/atau denda paling banyak 12 miliar rupiah.

Sanksi Bagi Penyelenggara E-Commerce Menurut Hukum Perdata

Pasal 26 UU 11/2008 menetapkan bahwa siapapun yang melakukan tindakan mengenai perolehan data pribadi tanpa persetujuan mereka (Rosalinda Elsina Latumahina 2014). Sekurang-kurangnya pelanggaran terhadap PDP dapat dijerat dengan perbuatan melawan hukum karena kesalahan berdasarkan ketentuan hukum dalam Pasal 1365 KUHPerdata atau Pasal 1366 KUHPerdata tentang ketidakpatutan atau kelalaian. Pasal 3 UU 11/2008 memiliki prinsip yaitu hati-hati dan mempunyai kewajiban untuk bertanggungjawab terhadap semua PSE, baik dari perusahaan maupun dari pemerintahan, untuk mempertanggungjawabkan sistem elektronik yang harus mempunyai tingkat keamanan yang tinggi dan bertanggungjawab. Tentu lebih ideal jika tetap mengesahkan fungsi dan peran kejaksaan sebagai penuntut umum dalam perlindungan data pribadi.

Pada UU 8/1999, Pasal 15 UU 11/2008 memuat asas praduga tanggung jawab, dimana setiap PSE akan selalu dipertanggungjawabkan perbuatannya berdasarkan hukum yang berlaku, tidak berlaku apabila kegagalan itu terjadi diluar dari perbuatan PSE melainkan diakibatkan dari kesalahan dari pengguna sendiri dikarenakan sebab-sebab secara alamiah. Beban dari pembuktian tersebut tetunya berada di PSE, jika ternyata PSE tidak memberikan pernyataan yang sesungguhnya mengenai insiden terhadap terjadinya suatu kebocoran terhadap data pribadi pengguna akan menimbulkan masalah selanjutnya yang akan muncul yakni adanya suatu pembohongan terhadap publik serta pelanggaran terhadap hak dari publik agar mendapatkan suatu informasi yang jelas bagi pengguna atau konsumen sebagai pemilik dari data pribadinya (Maharani 2018).

Pasal 14 sampai Pasal 18 PP 71/2019 mengatur setidaknya mengenai aturan perlindungan data yang harus diterapkan oleh PSE. Jika terjadi pelanggaran data, PSE memiliki kewajiban untuk melaporkan. Namun, dengan melakukan konferensi pers saja tidak cukup, tetapi dengan membuat surat tertulis yang dibuat langsung terhadap pemilik data. Selanjutnya, PP 80/2019 juga mengatur perlindungan data pribadi yang relatif lebih lengkap, hal ini terlihat pada ketentuan perlindungan data pribadi pada bab tersendiri dibandingkan dengan PP 71/2019. Selain itu, PP 80/2019 memberikan suatu bentuk kewajiban terhadap setiap Perdagangan Melalui Sistem Elektronik untuk melindungi data sesuai aturan yang diatur dalam Peraturan Pemerintah, dengan mengacu pada best practice atau praktik yang berlaku.

Seperti dijelaskan di atas, setiap pengguna dapat meminta kompensasi dari perusahaan dan/atau lembaga pemerintah yang lalai dalam merahasiakan data data. Hanya saja membuktikan kerugian yang berupa non-uang tidaklah mudah. Selain itu, setiap pengguna tentunya memiliki keterbatasan waktu dan biaya dalam menuntut haknya, sehingga pengetahuan pemilik data sangat diperlukan untuk mengajukan tuntutan baik perorangan maupun bersama-sama tentunya dibutuhkan dengan gugatan perwakilan kelompok. Tentunya upaya ini akan sangat memakan biaya secara administratif, baik dari segi waktu maupun tenaga baik pengguna maupun kuasa hukumnya. Oleh karena itu, dukungan pengacara yang bertanggung jawab atas kepentingan konsumen sangat dibutuhkan untuk mengajukan gugatan agar kebocoran data menjadi kebiasaan baik bagi penyelenggara swasta maupun pemerintah.

Kewajiban pelaku agar selalu beritikad baik dalam mengembangkan kegiatannya diatur dalam Pasal 7 ayat 1 UU 8/1999, di mana pelaku usaha mempunyai suatu kewajiban dalam bertanggungjawab untuk menciptakan persaingan usaha yang sehat dengan tujuan untuk mendukung pembangunan secara nasional. Terdapat banyak dari ketentuan UU 8/1999 yang mewajibkan pelaku perdagangan untuk berperilaku yang berkontribusi terhadap keberhasilan pembangunan ekonomi berskala nasional, khususnya di sektor korporasi. Untuk setiap pelanggaran yang dilakukan oleh pelaku usaha akan dikenakan sanksi hukum. Pengenaan sanksi tersebut penting mengingat untuk membuat persaingan usaha lebih sehat memerlukan keseriusan dan tekad yang kuat. Pelaku usaha dalam hal ini penyelenggara e-commerce berkewajiban memberikan ganti rugi kepada konsumen atas kerugian atau ganti rugi yang dalam hal ini merupakan kerugian akibat hilangnya data pribadi konsumen.

Sanksi Bagi Penyelenggara E-Commerce Menurut Hukum Administrasi

Menurut UU 23/2006, negara memiliki kewajiban dalam menjaga dan mengamankan data pribadi yang dimiliki oleh penduduknya. Oleh karena itu, untuk menjaga kerahasiaan informasi terhadap data tersebut diperlukan hak akses dari penyelenggara dan badan pelaksana pendataan kependudukan yang pengaturannya telah diatur dalam Perpres 67/2011. Kekurangan dari aturan tersebut adalah belum adanya pasal yang mengatur mengenai perlindungan terhadap data pribadi warga negara dengan menyimpan dan menggunakan yang terkait dalam pemindaian dan pendaftaran terhadap sidik jari dan retina warga negara selanjutnya. Muncul permasalahan terhadap adanya suatu perbedaan dalam penjelasan mengenai data kependudukan yang bersifat dirahasiakan. Terdapat perbedaan secara mendasar terhadap UU 23/2006 dengan perubahannya. Dalam situasi ini memiliki pemikiran yang berbeda dalam mengelompokkan jenis data pribadi yang dilindungi di Indonesia.

Walaupun berkaitan dengan kearsipan, namun hal tersebut memiliki keterkaitan terhadap proses dalam kegiatan penyelenggaraan pemerintahan, salah satunya berkaitan dengan penyelenggaraan pemerintahan dengan sistem kearsipan dan seringkali data atau informasi data secara pribadi seperti kependudukan, guru dan mahasiswa. Pasal 3 huruf (f) UU 43/2009 menyebutkan yaitu tujuan arsip adalah untuk memberikan rasa aman terhadap pemiliknya sebagai bentuk bukti dari tanggung jawab pemerintah dalam melindungi masyarakat (Primanta 2020). Selanjutnya, peraturan perundang-undangan tersebut telah mengatur tentang jangka waktu terhadap penyimpanan data atau informasi yaitu antara 10 tahun hingga 25 tahun. Setelah mencapai penyimpanan sampai 25 tahun maka masa penyimpanan terhadap data tersebut dapat diperpanjang atau dapat dihapus atau juga dapat dipublikasikan kepada umum selama salah satunya tidak mengungkapkan hal-hal yang bersifat sensitif atau data pribadi.

Dalam Pasal 1 angka 22 UU 23/2014 mengakui bahwa data pribadi merupakan data individu yang harus diamankan, dirawat, dan dipelihata dengan cermat yang harus dijaga kerahasiaannya. Kemudian Pasal 85 UU 23/2006 mengatur bahwa negara memiliki kewajiban untuk melindungi dan menyimpan data pribadi milik warga negaranya. Pasal 79 juga mengatakan bahwa negara memiliki kewajiban dalam melindungi dan memberi menteri tugas agar dapat bertanggungjawab terhadap hak terhadap mengakses data pribadi milik warga negara (Kusnadi 2021).

Tugas administratif kementerian/lembaga yang bertanggung jawab atas perlindungan data pribadi yaitu Kementerian Komunikasi dan Informatika, Kemendag dan BPKN, karena tentunya pemilik data pribadi adalah pengguna sistem sebagai konsumen. Sesuai dengan bidangnya masing-

masing mempunyai wewenang, tugas dan fungsi pokok untuk melaksanakan orientasi, pengawasan, pencegahan dan penindakan.

Perusahaan yang berada di bawah PP 71/2019 mewajibkan terhadap pengenaan sanksi berupa denda administrasi yang diberikan oleh Kementrian Informatika selain itu dapat juga dilaporkan oleh BPKN melalui Mendag agar dapat dimasukkan kedalam daftar hitam berdasarkan mekanisme dari Peraturan PP 80/2019 atas dasar tidak menghormati hak dari konsumen terhadap kenyamanan serta keamanan. Selain itu, Kementrian Informatika juga memiliki akses terhadap sistem dengan cara mengunci dengan tujuan mencegah perusahaan agar hal tersebut terulang kembali terhadap pengguna lainnya. Kondisi tersebut dengan tujuan untuk memulihkan atau menormalisasi agar dapat keluar dari *black list* harus diperbolehkan apabila tentang semua kebocoran datanya bersama dengan solusi atau pengananan insiden memiliki fakta yang jelas dan hak dari konsumen yang merasa dirugikan telah dipulihkan.

Selanjutnya, untuk perlindungan terhadap data pribadi merupakan bentuk dari keamanan *cyber*, tidak terlepas dari wewenang otoritas yang berwenang, yang meliputi: Kepolisian, Kemhan, Badan Intelejen Negara. Dengan menggunakan sumber dana dari negara, yakni sumber dana tersebut merupakan uang yang berasal dari rakyat dengan tujuan untuk membeli peralatan dan perlengkapan untuk keamanan serta pelatihan alat tersebut tentu saja tidak murah. Sehingga timbul pemikiran dari publik tentang apa manfaat yang diberikan oleh alat tersebut untuk kepentingan publik.

Publik mempunyai hak untuk menuntut mendapatkan informasi secara jelas dan kredibel selama proses dari pencegahan dan tindakan dari aparat penegak hukum serta mempertanyakan mengenai situasi terhadap kebocoran data pribadi yang sering kali terjadi dan terulang. Apakah kejadian itu sering terjadi dikarenakan semua pihak yang terkait seolah sudah melupakannya, ataukah terlalu sulit berkoordinasi untuk melindungi kepentingan publik. Setiap warga negara mempunyai hak untuk menggugat PMH di hadapan pejabat yang berwenang atas pelaksanaan kewenangannya yang tidak semestinya apabila merasa dirugikan. Ini bisa dianggap sebagai pembiaran yang merugikan masyarakat. Tentunya akan lebih ideal jika ditambah dengan penguatan fungsi dan peran kejaksaan sebagai penuntut umum dalam perlindungan data pribadi.

Dalam negara dengan hukum yang maju, pemberian kekuasaan dan menggunakan dana negara serta pelaksanaan fungsi dan tugas dari perlindungan rakyat dan negara tidak diberikan tanpa tanggung jawab administratif yang bertanggungjawab. Tampaknya masyarakat perlu lebih proaktif mengenai masalah ini, salah satunya dipaksa untuk menuntut administrasi pemerintah yang mengabaikan wewenang dan tanggung jawab yang telah diberikan.

Dalam Pasal 1 PP 71/2019, PSE adalah setiap orang, penyelenggara pemerintah, badan usaha, dan masyarakat yang secara sendiri-sendiri atau bersama-sama menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik. pengguna sistem elektronik untuk keperluan sendiri dan/atau kebutuhan pihak ketiga.

Selain itu, dalam Pasal 100 ayat (2) PP 71/2019, terdapat sanksi administratif atas berbagai pelanggaran perlindungan data pribadi, yaitu:

1. Berupa teguran secara tertulis;
2. Berupa ganti rugi secara administratif;
3. Berupa diberhentikan secara sementara;

4. Berupa pemutusan terhadap akses;
5. Berupa dicoret dari daftar PSE.

Bentuk dari sanksi diatas merupakan sanksi yang diberikan oleh Keminfo yang merujuk kepada Perpu yang berlaku.

Ketentuan terkait tanggung jawab PSE diatur tidak hanya dalam peraturan pemerintah, tetapi juga dalam Pasal 36 Permenkominfo 20/2016, sebagai berikut:

Setiap orang yang menghimpun, merubah, memperoleh, menyimpulkan, menyimpan, mempublikasikan, mengkomunikasikan, mengirim dan/atau menyebarkan data pribadi tanpa mempunyai hak untuk menyebarkan atau bertentangan dengan ketentuan dalam Permen ini atau peraturan perundang-undangan lainnya dapat dikenakan sanksi administratif yang merujuk pada ketentuan dalam suatu perundang-undangan berupa:

1. Berupa teguran secara lisan;
2. Berupa teguran secara tertulis;
3. Berupa kegiatan dapat diberhentikan secara sementara; dan/atau
4. Berupa diumumkan melalui website online.

Kesimpulan

Meskipun hukum di Indonesia belum ada yang secara khusus memberikan aturan mengenai data pribadi tetapi setidaknya ada beberapa dasar hukum yang dapat dijadikan sebagai dasar dalam melindungi data pribadi pengguna. Adapun beberapa dasar hukum yang dapat digunakan dalam melindungi data pribadi seperti KUHP, KUHPerdata, UU 8/1999, UU 23/2006 jo. UU 24/2013 dan UU 11/2008 jo. UU 19/2016. Selain itu terdapat dasar hukum yang menjadi landasan terhadap PSE yang dimana mempunyai peran terhadap menyimpan data pribadi pengguna seperti PP 20/2016, PP 71/2019 dan Permenkominfo 20/2016. Dengan berdasarkan UUD NRI 1945 Pasal 28G ayat (1) yang dimana menjelaskan mengenai hak dari warga negara yaitu mendapatkan perlindungan terhadap diri sendiri, keluarga, kehormatan, martabat, dan harta benda. Tidak sampai disitu, pasal tersebut juga mengatur terkait privasi setiap warga negaranya sebagai suatu hak yang harus dihormati. Maka dari itu, pasal tersebut telah memberi isyarat bahwa negara wajib memberikan perlindungan terhadap data pribadi warga negaranya.

Daftar Pustaka

Dewi Rosadi, Sinta, and Garry Gumelar Pratama. 2018. 'URGENSI PERLINDUNGANDATA PRIVASIDALAM ERA EKONOMI DIGITAL DI INDONESIA', *Veritas et Justitia*, 4.1 <https://doi.org/10.25123/vej.2916>

Djafar, Wahyudi. 2019. 'Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan', *Jurnal Becoss*, 1.1

Hanim, Lathifah. 2014. 'PERLINDUNGAN HUKUM BAGI PARA PIHAK DALAM E-COMMERCE SEBAGAI AKIBAT DARI GLOBALISASI EKONOMI.', *Jurnal Pembaharuan Hukum*, 1.2 <https://doi.org/10.26532/jph.v1i2.1476>

Kusnadi, Sekaring Ayumeida. 2021. 'PERLINDUNGAN HUKUM DATA PRIBADI SEBAGAI HAK PRIVASI', *AL WASATH Jurnal Ilmu Hukum*, 2.1 <https://doi.org/10.47776/alwasath.v2i1.127>

Maharani, Resna Pratiwi. 2018. 'TANGGUNG JAWAB PENYELENGGARA TRANSAKSI ELEKTRONIK DALAM MELINDUNGI HAK KONSUMEN', *SUPREMASI Jurnal Hukum*, 1.1 <https://doi.org/10.36441/supremasi.v1i1.158>

Makarim, Edmon. 2014. 'KERANGKA KEBIJAKAN DAN REFORMASI HUKUM UNTUK KELANCARAN PERDAGANGAN SECARA ELEKTRONIK (E-COMMERCE) DI INDONESIA', *Jurnal Hukum & Pembangunan*, 44.3 <https://doi.org/10.21143/jhp.vol44.no3.25>

Primanta, Asa Intan. 2020. 'Pertanggungjawaban Pidana Pada Penyalahgunaan Data Pribadi', *Jurist-Diction*, 3.4 <https://doi.org/10.20473/jd.v3i4.20214>

Rosadi, Sinta Dewi. 2017. 'Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya', *Sosiohumaniora*, 19.3

Rosalinda Elsina Latumahina. 2014. 'Aspek Hukum Pelindungan Data Pribadi Di Dunia Maya', *GEMA AKTUALITA*, Vol. 3 No. <http://dspace.uphsurabaya.ac.id:8080/xmlui/bitstream/handle/123456789/92/Aspek Hukum Perlindungan Data Pribadi di Dunia Maya.pdf?sequence=1>

Rumlus, Muhamad Hasan, and Hanif Hartadi. 2020. 'Kebijakan Penanggulangan Pencurian Data Pribadi Dalam Media Elektronik', *Jurnal HAM*, 11.2 <https://doi.org/10.30641/ham.2020.11.285-299>

Saleh, Abd. Rahman. 2021. 'Perlindungan Data Pribadi Dalam Perspektif Kebijakan Hukum Pidana', *HUKMY : Jurnal Hukum*, 1.1 <https://doi.org/10.35316/hukmy.2021.v1i1.91-108>

Saragih, Lydia Kharista, Danrivanto Budhijanto, and Somawijaya Somawijaya. 2020. 'Perlindungan Hukum Data Pribadi Terhadap Penyalahgunaan Data Pribadi Pada Platform Media Sosial', *De Rechtsstaat*, 6.2