Rio Law Jurnal
Volume. 6 Nomor. 1 2025 ISSN 2722-9602
http://dx.doi.org/10.36355/.v1i2
Open Access at: https://ojs.umb-bungo.ac.id/index.php/RIO/index

PROTEKSI HUKUM DALAM PERETASAN (PENCURIAN) DATA PRIBADI NASIONAL

Haris Dermawan[1], Junaidi Lubis[2], Muhammad Koginta Lubis[3]
Prodi Hukum
Universitas Battuta
Jl. Sekip Simpang Sikambing No. 1 Medan
junaidilubis67@yahoo.co.id

ABSTRACT

The incident of data theft or cyber attack (ransomware) some time ago taught us how important legal protection is as early as possible so that the same incident does not happen again in the future. That the law in this case must be able to protect as early as possible so that the same incident does not happen again and even if it does happen again, the law must be able to fully protect the data so that legal certainty is created in the protection of personal data nationally. What is protected by law is to protect important information and protect data from loss, damage to theft, how important the law is in protecting this kind of thing. The purpose of this study is to find out how important the law is in providing data protection from all forms of damage, loss to theft which can clearly harm many people and have an impact on the emergence of legal uncertainty in providing personal data nationally. The government in this case should create a clear and firm legal umbrella to provide security to every user of personal data so that hacked data can be protected by law and resolved in the best possible way, so that there is legal certainty for all users of personal data. The purpose of this study is to find out how the law provides national personal data protection. The method used in this case is by looking at various kinds of legal rules related to the protection of personal data normatively so that there is legal certainty from the side of the legal rules that have been determined by the provisions of the laws and regulations in force in Indonesia. The results of the study indicate that the legal rules are still weak so that the law has not been able to provide protection as early as possible for legal certainty in protecting all personal data nationally.

Keywords: Legal Protection, Hacking, National Personal Data.

ABSTRAK

Kejadian pencurian data atau serangan siber (ransomware) beberapa waktu yang lalu mengajarkan bahwa memang betapa pentingnya proteksi hukum sedini mungkin agar kejadian yang sama tidak lagi terulang dimasa yang akan datang. Bahwa hukum dalam hal ini harus mampu memproteksi sedini mungkin agar kejadian yang sama tidak lagi dan kalaupun sampai terjadi lagi maka hukum harus mampu melindungi data itu sepenuhnya sehingga terciptalah kepastian hukum dalam perlindungan data pribadi secara nasional. Yang diproteksi hukum adalah untuk melindungi informasi penting serta menjaga data dari kehilangan, kerusakan hingga terjadi pencurian, sungguh betapa pentingnya hukum dalam melindungi hal semacam ini. Tujuan dari penelitian ini adalah untuk mengetahui bahwa betapa pentingnya hukum dalam memberikan perlindungan data dari segala bentuk kerusakan, kehilangan hingga pencurian yang jelas bisa merugikan banyak orang dan membawa dampak munculnya ketidak pastian hukum dalam memberikan data pribadi secara nasional. Pemerintah dalam hal ini sudah sepatutnya membuat satu payung hukum yang jelas dan tegas untuk memberikan keamanan kepada setiap pengguna data pribadi agar data yang sudah dire

tas dapat dilindungi oleh hukum dan untuk diselesaikan dengan cara sebaik-baiknya, sehingga adanya kepastian hukum bagi semua pengguna data pribadi. Tujuan dari penelitian ini adalah untuk mengetahui bagaimana hukum memberikan perlindungan data pribadi secara nasional. Metode yang digunakan dalam hal ini yaitu dengan cara melihat berbagai macam aturan hukum yang berhubungan dengan perlindungan data pribadi secara normatif sehingga adanya kepastian hukum dari sisi aturan hukum yang sudah ditetapkan secara ketentuan peraturan perundang-undangan yang berlaku di Indonesia. Hasil penelitian menunjukkan bahwa masih lemahnya aturan hukum sehingga hukum belum mampu memberikan proteksi sedini mungkin untuk adanya kepastian hukum dalam melindungi semua data pribadi secara nasional.
Kata kunci: Proteksi Hukum, Peretasan, Data Pribadi Nasional.

PENDAHULUAN

Peretasan atau hacking data seperti contoh pengguna BPJS Kesehatan dan data COVID-19 adalah transaksional karena sudah ada penawaran transaksi yang dijual di forum internet Raid Forum yang dilakukan oleh akun bernama Kotz. Ini jelas merupakan globalisasi kejahatan ekonomi yang memanfaatkan keadaan untuk melakukan peretasan sistem dan hacker. Semuanya bergantung pada era globalisasi yang semakin meningkat bersama dengan era keterbukaan dan industri. Inilah hanyalah contoh lemahnya perlindungan data pribadi, yang memungkinkan bobol, pencurian, dan transaksi data pribadi.

Pencuri data menggunakan kelemahan hukum dan perlindungan hukum terhadap data pribadi. Negara bertanggung jawab untuk memastikan bahwa pemilik data pribadi dilindungi secara hukum. Negara harus membuat kebijakan hukum pidana yang mengatur tindakan apa yang dapat dipidana dan hukuman apa yang dapat diberikan kepada hacker dan pencuri data pribadi yang ditransaksikan. Dengan digitalisasi dan "*internetisasi*" aktivitas manusia melalui gagasan Internet of Things (IoT), peradaban manusia telah berubah secara dramatis. Konsep Internet of Things (IoT) bermaksud untuk memperluas manfaat dari konektivitas internet yang tersambung secara terus menerus.

Dalam kehidupan yang sudah digital dan "internetisasi", data dan informasi menjadi komponen penting untuk kelangsungan sistem. Banyak orang di zaman sekarang tidak menyadari bahwa konsep ini menghasilkan transaksi elektronik antara developer dan data atau informasi, yang merupakan perluasan fungsi internet. Semua perubahan ini berdampak pada globalisasi digital, yang meningkat karena batas negara semakin sedikit dan aliran data internasional yang lebih besar.

1. PENTINGNYA MEMAHAMAI PERLINDUNGAN DATA PRIBADI (PDP)

Untuk alasan apa data pribadi perlu dilindungi? Tentu ini merupakan pertanyaan mendasar yang ada dalam pikiran kita, sehingga diketahui bahwa data pribadi itu harus dilindungi oleh hukum sedemikian rupa agar jangan sampai

terkait data pribadi seseorang itu sampai kemana-mana. Hal ini disebabkan oleh fakta bahwa perlindungan data pribadi merupakan salah satu hak asasi manusia dan merupakan bagian dari perlindungan diri pribadi. [Diktum Menimbang Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi jo. Pasal 28G ayat (1), Pasal 28H ayat (4), dan Pasal 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 1]. Oleh karena itu, perlu ada undang-undang yang akan melindungi data pribadi sambil juga melindungi hak warga negara. Apa artinya data pribadi? Data pribadi dalam UU PDP didefinisikan sebagai data individu yang teridentifikasi atau dapat diidentifikasi secara terpisah atau yang dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Dalam hal ini bahwa data pribadi itu hanya milik pribadi seseorang bukan untuk dibagikan kepada siapaun kecuali ditentukan lain oleh kehedak hukum. [Pasal 1 angka 1 UU PDP 2].

Sekarang Indonesia memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, atau UU PDP. Menurut UU PDP, data pribadi adalah data tentang orang yang teridentifikasi atau dapat diidentifikasi secara terpisah atau yang dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik. [Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi 3]. Perihal apa saja yang masuk dalam kategori perlindungan data pribadi? [Pasal 4 UU PDP 4], antara lain:

a. Data pribadi yang spesifik termasuk informasi kesehatan, data biometrik, data genetika, catatan kriminal, data anak, data keuangan pribadi, dan/atau data lainnya yang diatur oleh undang-undang.
b. Data pribadi umum termasuk nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data yang digabungkan untuk mengidentifikasi seseorang.

Data pribadi adalah data individu tertentu yang disimpan, dirawat, dan dijamin benar dan rahasia. Salah satu hak asasi manusia adalah perlindungan data pribadi. Tujuan perlindungan data pribadi adalah untuk memastikan bahwa warga negara memiliki hak untuk melindungi data mereka sendiri dan meningkatkan kesadaran masyarakat tentang pentingnya melindungi data mereka. Pencurian data pribadi terutama di zaman modern seperti saat ini sering terjadi. Modus-modus pelaku untuk mendapatkan data pribadi seseorang sangat beragam. UU ITE telah mengatur hal terkait pencurian data pribadi dalam Pasal 32 Ayat 1, 2 dan 3 dengan ancaman pidana. [jdih.kominfo.go.id/infografis/view/21 5].

Hak konstitusional warga negara harus dilindungi dengan perlindungan data pribadi. Data pribadi adalah informasi tentang identitas seseorang, seperti Kartu Keluarga (KK), Nomor

induk kependudukan (NIK), dan sebagainya. Namun, sangat disayangkan bahwa spekulasi tentang kebocoran data pribadi semakin meningkat akhir-akhir ini. Bahkan, Indonesia menduduki peringkat ketiga di dunia dalam hal jumlah kasus kebocoran data terbanyak. [Indriana Firdaus, Bangka Belitung, Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan, Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia. DOI: https://doi.org/10.52005/rechten.v4i2.986].

Jumlah kasus ini menunjukkan bahwa sistem hukum dan keamanan Indonesia kurang kuat. Permasalahan ini menimbulkan risiko penyalahgunaan data pribadi seseorang. Pihak yang tidak bertanggung jawab akan menggunakan data tersebut untuk melakukan tindak kejahatannya, seperti penipuan, pembajakan, akses ilegal, dan manipulasi. [Fanny Priscyllia, Perlindungan Privasi Data Pribadi Dalam Perspektif Perbandingan Hukum, Jatiswara, 34.3 (2019) 1–5 https://doi.org/10.29303/jatiswara.v34i3.2187]. Dalam UU ITE Pasal 30 ayat (1) menjelaskan bahwa setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukuan intersepsi atau penyadapan atas sitem informasi elektronik dan/ atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain. Ada kemungkinan bahwa peretasan, sebagai tindakan melawan hukum, dapat diancam dengan pidana sesuai dengan undang-undang. Pelaku juga dapat diberi sanksi untuk memberikan efek jera atas tindakannya.

1.1. PELINDUNGAN DATA PRIBADI MASYARAKAT OLEH PEMERINTAH

UU PDP sendiri merupakan pengejewantahan dari Pasal 28G ayat (1) UUD 1945 yang berbunyi: "Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi". Pengertian pelindungan data pribadi berdasarkan Pasal 1 angka 2 UU PDP adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.

Menurut UU PDP, ada prosesor dan pengendali data pribadi. Pengendali data pribadi adalah setiap individu, badan publik, dan organisasi internasional yang bertindak sendiri atau bersama-sama untuk menetapkan tujuan dan mengawasi pemrosesan data pribadi. [Pasal 1 angka 4 UU PDP 8]. Namun, yang dimaksud dengan "prosesor data pribadi" adalah setiap individu, lembaga negara, dan organisasi internasional yang bertindak atas nama pengendali data pribadi dalam pemrosesan data. Semakin banyak pengguna internet, semakin banyak kejahatan digital yang terjadi. Karena itu, untuk menciptakan keamanan, payung hukum yang kuat sangat penting. The General

Declaration of Human Rights, pasal 12, mengatur hak setiap orang atas perlindungan hukum terhadap data pribadinya dalam hukum internasional.

Indonesia telah meratifikasi UDCHR, yang berarti bahwa pemerintah harus berkomitmen untuk menegakkan hukum mengenai hak privasi tersebut. Hukum ini diharapkan dapat memberikan keuntungan, kepastian hukum, perlindungan, dan keadilan bagi semua orang. [Hanifan Niffari, Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain Jurnal Hukum Dan Bisnis (Selisik), 6.1 (2020), 1–14Https://Doi.Org/10.35814/Selisik.Vol 6.1699 [9]. Saat ini pengaturan terhadap perlindungan data pribadi telah terbuat dalam peraturan perundang-undangan, yaitu:

a. Peraturan perundang-undang Nomor 27 tahun 2022 Tentang Perlindungan Data Pribadi

Pada 17 Oktober 2022, undang-undang ini disahkan. Ini dibuat karena penting bagi pemerintah untuk memberikan kepastian hukum kepada orang-orang tentang data pribadi mereka. Undang-undang ini juga dijadikan sebagai acuan utama, jika terjadi tindak pelanggaran terhadap data pribadi. dirancang untuk menghindari tumpang tindih peraturan dan memberikan perlindungan bagi masyarakat. Dalam Pasal 1, ketentuan umum tentang perlindungan data pribadi dijelaskan, dan Pasal 57, menjelaskan sanksi administratif yang akan diterapkan jika pelanggaran jenis ini terjadi. Pasal 67 juga membahas ketentuan pidana Tindakan tersebut.

b. Peraturan Perundang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Selain itu, UU ITE memiliki peraturan tentang perlindungan data pribadi. Peraturan ini dimaksudkan untuk menjadi alat hukum yang dapat mengatur segala macam pelanggaran dalam bidang informasi dan teknologi. Selain itu, peraturan ini mencakup ketentuan umum mengenai upaya untuk melindungi hak privasi seseorang dan sanksi yang akan diterima jika pelanggaran tersebut terus terjadi. [MRTR Herryani, 'Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace', Transparansi Hukum, 5.1 (2022), 110–33 http://ojs.unik-kediri.ac.id/index.php/transparansihukum/article/view/2274 10]. Dalam pasal 26 ayat (2) dijelaskan bahwa: "Setiap orang yang dilanggar haknya sebagaimana dimaksud dalam ayat (1) dapat mengajukan gugatan atas kerugian yang di timbulkan berdasarkan undang-undang ini."

Perlindungan data pribadi dalam setiap transaksi elektronik dibantu oleh peraturan yang disebutkan di atas. Sebagai pemilik data, kita harus berhati-hati dengan data pribadi kita

sendiri, meskipun ada payung hukum yang melindunginya.

c. Peraturan Pemerintah Nomor 71 tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Dalam PP PTSE ini, perlindungan data pribadi sangat penting. Pada pasal 8, PSE harus memastikan keamanan dan keandalan transakisi elektronik sebagai mana perlu. Selain itu, pasal 14 memberikan banyak penjelasan tentang prinsip dan tanggung jawab yang berkaitan dengan perlindungan data pribadi. Dalam pasal 100 ayat 2 dijelaskan jenis sanksi administratif yang dapat diterima jika hal tersebut tetap dilanggar. Sanksi ini termasuk teguran tertulis, denda, penghentian sementara, pemutusan akses, dan penghapusan dari daftar. [Peraturan Pemerintah Republik Indonesia Nomor 7l Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik Menimbang', Media Hukum, 7.2 (2012) 11].

d. Pihak yang Berperan dalam Menegakkan Hukum Perlindungan Data Pribadi Akibat Kejahatan Peretasan

Dengan kemajuan dalam teknologi dan informasi saat ini, kita harus selalu waspada terhadap kejahatan digital yang selalu terlihat di balik. Salah satu kejahatan yang tidak pandang bulu adalah kejahatan peretasan. Tindak pidana ini dapat melibatkan orang yang tidak bersalah. Oleh karena itu, untuk memastikan bahwa pilar hukum dilaksanakan dengan benar, diperlukan partisipasi aktif dari berbagai pihak.

1. Pemerintah

Pemerintah memiliki dua tanggung jawab utama untuk melindungi data pribadi dan informasi pribadi warganya. Membuat undang-undang yang mengatur perlindungan data pribadi sebagai hak privasi adalah tugas pertama. Tugas kedua adalah melakukan pengawasan dan penegakkan undang-undang tersebut. Ketika fungsi dan tanggung jawabnya berjalan dengan baik.

2. Pihak Pengontrol atau pemproses data

Pengotrol dan pemproses data harus berpartisipasi secara aktif dalam melindungi data setiap individu. Karena mereka bertanggung jawab sebagai pemegang kendali, mereka harus dapat mengatasi segala hambatan dan memilih strategi untuk mengurangi resiko jika terjadi kebocoran data pada sistem yang ada. Menurut Peraturan Badan Siber dan Sandi Negara (BSSN) No. 8 tahun 2020 tentang Sistem Pengaman dan Penyelenggaraan Sistem Elektronik, sertifikasi harus berdasarkan tingkat resiko tertinggi atau terendah.

3. Pemilik Data

Orang yang memiliki data adalah orang yang sangat penting untuk menjaga privasi mereka. Ketika kita menggunakan media sosial, kita harus tahu bagaimana berperilaku etis. Kita juga harus tahu apa yang tidak boleh dilakukan agar hal-hal yang tidak diinginkan tidak terjadi di masa depan. Jangan sampai pemilik data tidak mematuhi peraturan atau menggumbar data

pribadi mereka sendiri meskipun regulasi dan pihak lain sudah melakukan tugas mereka.

4. Penegak Hukum

Berbicara tentang penegakkan hukum selalu terkait dengan lembaga penegak hukum, seperti polisi, hakim, jaksa, dan BSSN, karena itu adalah tugas dan tanggung jawab mereka. Keterlibatan pihak-pihak ini menjadi salah satu faktor yang sangat penting untuk pelaksanaan hukum yang ada.

Dari penjelasan di atas, dapat disimpulkan bahwa pelanggaran seperti kejahatan peretasan tidak akan terjadi jika semua pihak melakukan tugas mereka dengan baik dan berhati-hati. Oleh karena itu, perlu ada hubungan dan kontribusi yang nyata agar penegakkan hukum ini dapat dilakukan secara maksimal dan optimal.

Pasal 20 hingga 50 UU PDP menetapkan tanggung jawab pengendali data pribadi, termasuk menjaga kerahasiaan dan keamanan data, menunjukkan bukti persetujuan subjek data saat pemrosesan, dan mencegah akses yang tidak sah ke data pribadi. Sementara itu, Pasal 51 s.d. Pasal 52 UU PDP menetapkan tanggung jawab prosesor data pribadi, termasuk, tetapi tidak terbatas pada, meminta persetujuan tertulis pengendali data pribadi sebelum melakukan pemrosesan data pribadi. Dalam hal ini, pengendali dan prosesor data pribadi harus menunjuk orang yang bertanggung jawab untuk melindungi data pribadi, yaitu: Pasal 53 ayat (1) UU PDP [12]

a) pemrosesan data pribadi untuk kepentingan pelayanan publik
b) Kegiatan utama pengendali data pribadi mencakup jenis, volume, dan/atau tujuan yang membutuhkan pengawasan rutin dan sistematis terhadap volume besar data
c) Kegiatan utama pengendali data pribadi terdiri dari pemrosesan data pribadi yang besar, khusus, atau terkait dengan tindak pidana.

Petugas atau pejabat yang bertanggung jawab atas perlindungan data pribadi dipilih berdasarkan profesionalitas, pengetahuan tentang hukum dan praktik perlindungan data pribadi, dan kemampuan untuk melaksanakan tugas. Menurut Satjipto Rahardjo, perlindungan hukum adalah upaya untuk mengatur berbagai kepentingan dalam masyarakat agar tidak terjadi tubrukan kepentingan dan setiap orang dapat menikmati semua hak yang diberikan oleh hukum. [Satjipto Rahardjo, 2000, Ilmu Hukum, PT Citra Aditya Bakti: Bandung 13]. Membatasi suatu kepentingan tertentu dan memberikan otoritas pada yang lainnya secara terstruktur adalah cara pengorganisasian dilakukan.

Pendapat Fitzgerald tentang tujuan hukum adalah untuk mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat dengan mengatur perlindungan dan pembatasan terhadap kepentingan tersebut. Pendapat ini menjadi inspirasi dari perlindungan hukum Satjipto Rahardjo. Perlindungan hukum

adalah hukum itu sendiri untuk memberikan keamanan, keuntungan, dan keadilan bagi masyarakat. Prinsip perlindungan hukum terhadap tindakan pemerintah berasal dari konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia. Tujuan dari pembentukan konsep-konsep tentang pengakuan dan perlindungan terhadap hak-hak asasi manusia adalah untuk membatasi dan meletakkan tanggung jawab kepada masyarakat dan pemerintah.

Prinsip negara hukum adalah prinsip kedua yang mendasari perlindungan hukum terhadap tindakan pemerintah. Dalam hal pengakuan dan perlindungan hak asasi manusia, pengakuan dan perlindungan hak asasi manusia sangat penting karena tujuan negara hukum. [Philipus M Hadjon, 1987, Perlindungan Bagi Rakyat Indonesia, Surabaya: PT Bina Ilmu, 1987 14].

1.2. PERKEMBANGAN PERLINDUNGAN DATA PRIBADI DI INDONESIA

Istilah "data pribadi" sering disamakan dengan istilah "personal data" (di Eropa) atau "personal information" (di AS). Malaysia menggunakan istilah "data peribadi", Singapura menggunakan "personal data", dan Philipina, bersama dengan Jepang dan Korea Selatan, menggunakan "informasi pribadi". Istilah yang digunakan di sini hampir sama. Menurut Kamus Besar Bahasa Indonesia, "Data pribadi" berarti informasi tentang karakteristik individu, seperti nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan keluarga. [Wahyudi Djafar dan M. Jodi Santoso, 2019, Perlidnungan Data Pribadi Konsep, Instrumen, dan Prinsipnya, Lembaga Studi dan Advokasi Masyarakat (ELSAM) 15].

Namun, Peraturan Data Pribadi Umum Uni Eropa (EU GDPR) mendefinisikan personal data sebagai berbagai informasi yang terkait dengan orang yang "diidentifikasi" atau dapat diidentifikasi. Definisi luas dari konsep "data pribadi" memungkinkan badan legislatif negara-negara Uni Eropa untuk mencakup semua data yang mungkin terkait dengan seorang individu. Orla Lynskey, “Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order”. International and Comparative Law Quarterly, (2014) 63 (3). pp. 569-597 [14].

Pada akhirnya, seseorang hanya dapat membatasi ruang lingkup informasi pribadi untuk yang berhubungan dengan seseorang. Menurut Richard Murphy, ruang lingkup informasi pribadi terdiri dari semua data tentang seseorang yang dapat diidentifikasi oleh individu tersebut. Namun demikian, karena ada banyak informasi yang dapat diidentifikasi tentang kita dan apa yang kita lakukan, definisi Murphy terlalu luas. Wahyudi Djafar dan M. Jodi Santoso, Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipny [15]. Sebagai bagian dari hak privacy, perlindungan data pribadi merupakan hak asasi manusia yang mendapatkan

perlindungan dari instrumen hukum internasional dan konstitusi negara.

Hak privasi ini dilindungi oleh konstitusi Indonesia, seperti yang ditunjukkan dalam Pasal 28G ayat (1) UUD NRI 1945, yang menyatakan bahwa: “Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.” Namun, dalam instrumen internasional lain, hak privasi juga diatur dalam Universal Declaration of Human Rights (1948), khususnya dalam Pasal 12, dan International Covenant on Civil and Political Rights (ICCPR) 1966, khususnya dalam Pasal 17.

Alan Wastin, yang pertama kali mendefinisikan data privasi atau "informasi privasi" sebagai hak individu, keluarga, atau kelompok untuk menentukan batas data privasi mereka. Kemudian dikembangkan oleh pakar hukum lainnya. Arthur Miller adalah salah satunya yang menggambarkan data privasi sebagai kemampuan seseorang untuk mengontrol informasi yang relevan. Begitu juga dengan kemajuan teknologi yang memungkinkan informasi individu dapat diakses, diproses, dikumpulkan, dan disimpan. Selain itu, perspektif Barat tentang hak privasi tidak selalu benar karena memiliki konsekuensi sosial yang mewajibkan orang untuk memperhatikan informasi pribadi mereka. [Wahyudi Djafar, Bernhard Ruben Fritz, dan Blandina Lintang, Perlindungan data Pribadi Usulan Pelembagaan Kebijakan dari Perspektif HAM, Jakarta: 2016) 16].

Istilah "privasi" dan "data pribadi" sebenarnya sudah lama ada. Meskipun International Covenant on Civil and Political Rights (ICCPR) tidak secara eksplisit menyebutkan istilah "data pribadi", perlindungan data pribadi adalah bagian penting dari kehidupan pribadi setiap orang. Konvensi regional Uni Eropa (General Data Protection Regulation/GDPR) dan konvensi regional lainnya, seperti Konvensi Uni Afrika (UNCRC), mengatur perlindungan data pribadi. [Edmon Makarim, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi, Kolom Hukumonline.com 17]. Beberapa negara memiliki konstitusi yang melindungi privasi, seperti Afrika Selatan dan Hungaria, yang memberi orang hak untuk melihat dan mengontrol data pribadi mereka. Selain itu, banyak negara memasukkan perjanjian internasional tentang hak privasi, seperti Konvenan Internasional Tentang Hak Sipil Dan Politik atau Konvensi Eropa Tentang Hak Asasi Manusia, ke dalam hukum nasional mereka. Indonesia adalah salah satunya, dengan ratifikasi ICCPR ke dalam UU No. 12 Tahun 2009. [David Banisar and Simon Davis, 1999 sebagaimana dikutip Sinta Dewi Rosadi, Cyber Law 18].

1.3. UPAYA HUKUM YANG DILAKUKAN

Menurut Pasal 12 ayat (1) UU Data Pribadi, subjek data pribadi memiliki hak untuk menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi terhadap mereka sendiri sesuai dengan ketentuan peraturan perundang-undangan. Selain itu, korban memiliki hak untuk mengajukan gugatan perdata berdasarkan Pasal 26 UU 19/2016, Ayat (1) dan (2), di mana ketentuan yang relevan menyatakan sebagai berikut:

a. Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.
b. Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.

Menurut Pasal 1365 Kode Hukum Perdata, gugatan ganti rugi terhadap pihak yang menyalahgunakan data pribadi adalah gugatan perbuatan melawan hukum. https://www.hukumonline.com/klinik/a/terjadi-pencurian-data-pribadi-tempuh-langkah-ini-lt5d904597bfa6e/ [19]. Patut untuk diketahui bersama bahwa pengendali data pribadi memiliki tanggung jawab untuk melindungi dan memastikan keamanan data pribadi yang mereka proses dengan melakukan, antara lain:

1. Membuat dan menerapkan prosedur teknis operasional untuk melindungi data pribadi dari kerusakan yang disebabkan oleh pemrosesan data pribadi
2. Membuat keputusan tentang tingkat keamanan data pribadi dengan mempertimbangkan jenis data pribadi dan risiko yang terkait dengannya yang perlu dilindungi selama pemrosesan data pribadi.

Jika terjadi kegagalan perlindungan data pribadi, pengendali data pribadi harus memberikan pemberitahuan secara tertulis kepada subjek dan lembaga dalam waktu paling lambat 3 x 24 Jam, dengan memuat identitas pengaduan antara lain:

i. data pribadi yang terungkap
ii. kapan dan bagaimana data pribadi terungkap
iii. upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data pribadi.

Pengendali data pribadi harus memberi tahu masyarakat tentang kegagalan perlindungan data pribadi, misalnya jika kesalahan itu mengganggu layanan publik atau mengganggu kepentingan masyarakat. Pasal 46 ayat (3) dan penjelasannya UU PDP [20]. Namun, perlu diingat bahwa dalam kasus kegagalan perlindungan data pribadi, tidak ada tanggung

jawab untuk memberi tahu subjek data secara tertulis, Pasal 50 ayat (1) UU PDP [21]. yaitu:

a. kepentingan pertahanan dan keamanan nasional
b. kepentingan penegakan hukum
c. kepentingan umum dalam rangka penyelenggaraan negara
d. kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan demi kepentingan negara.

Akan tetapi, pengecualian ini hanya dilakukan untuk memenuhi ketentuan yang ditetapkan oleh undang-undang. Pasal 50 ayat (2) UU PDP [22]. Sebaliknya, Pasal 47 UU PDP secara eksplisit menyatakan bahwa "Pengendali Data Pribadi bertanggung jawab atas pemrosesan Data Pribadi dan mematuhi peraturan perlindungan Data Pribadi." Jika seseorang melanggar Pasal 46 ayat (1) dan (3) serta Pasal 47 UU PDP sebagaimana disebutkan di atas, mereka akan diberi peringatan tertulis, menghentikan pemrosesan data pribadi untuk sementara, menghapus atau memusnahkan data pribadi, dan/atau denda administratif. Sanksi administratif diberikan oleh lembaga. Dendanya tidak boleh melebihi 2 % (persen) dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Konsep hak privasi dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia berbunyi: "Tidak seorangpun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan suratmenyurat juga tak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapatkan perlindungan hukum terhadap gangguan atau pelanggaran seperti itu". Pasal 17 ICCPR, yang diuraikan dalam beberapa ayat, menjadikannya lebih jelas.

1) *Tidak boleh seorangpun yang dapat secara sewewangwenang atau secara tidak sah mencampuri masalah-masalah pribadinya, kelaurganya, rumah atau hubungan surat-menyurat, atau secara tidak sah diserang kehormatan dan nama baiknya*
2) *2)Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan sepertu tersebut diatas.*

Tujuan perlindungan hak privasi hanyalah untuk melindungi orang dari gangguan yang dianggap melanggar hukum atau gangguan yang sewenang-wenang terhadap informasi mereka. Namun, gambaran yang diberikan kurang detail tentang apa yang dimaksud dengan gangguan sewenang-wenang atau melanggar hukum terhadap privasi. Sudah pasti, undang-undang telah menetapkan unsur-unsur yang dapat dilakukan sebagai gangguan yang memenuhi persyaratan yang ditentukan. [Wahyudi Djafar dan Asep Komarudin, Perlindungan Hak Atas Privasi Di Internet Beberapa Penjelasan Kunci, Jakarta: ELSAM, 2014 23].

Hak asasi manusia termasuk hak untuk melindungi data pribadi mereka. Indonesia telah menetapkan berbagai undang-undang yang mengatur privasi sebelum undang-undang tentang perlindungan data pribadi disahkan. Untuk memahami bagaimana negara ini mengatur perlindungan data pribadi, kita akan membahas dan melihat undang-undang yang paling baru, yaitu undang-undang tentang perlindungan data pribadi.

1.4. SANKSI HUKUM DALAM PERETASAN (PENCURIAN) DATA PRIBADI

Berdasarkan undang-undang penyelenggara sistem elektronik dapat dimintai pertanggungjawaban secara hukum atas segala tindakan yang melanggar undang-undang yang berlaku. Atas ketidakpatuhan terhadap undang-undang tersebut, penyelenggara dapat dimintai pertanggungjawaban secara administratif, perdata, atau pidana.

A. Sanksi Administrasi

Berdasarkan undang-undang sebelumnya, kementerian atau lembaga yang bertanggung jawab atas perlindungan data pribadi setidaknya memiliki tanggung jawab administratif untuk melindungi data pribadi. Kementerian-kementerian ini termasuk Kementerian Kominfo, yang bertanggung jawab untuk menjalankan sistem elektronik, Kementerian Perdagangan, dan Badan Pelindungan Konsumen Nasional, yang melindungi konsumen sebagai pengguna sistem. Setiap sektor memiliki lembaga yang memiliki kewenangan, tugas pokok, dan fungsi untuk melakukan pembinaan, pengawasan, pencegahan, dan penindakan.

Sesuai dengan PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, korporasi dapat diberi sanksi administratif oleh Kominfo sebelum UU PDP. Blokir sistem perusahaan juga dapat dilakukan oleh kominfo untuk mencegah pengguna lain mengalami hal yang sama. Pemulihan dan normalisasi untuk keluar dari daftar hitam hanya dapat dilakukan jika semua masalah kebocoran data telah diselesaikan dan hak-hak pengguna dan konsumen yang dirugikan telah dipulihkan. Edmon Makarim https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef?page=2 [24].

Sebaliknya, bab 8 UU PDP saat ini dengan jelas mengatur sanksi administratif tersebut. Jika pengendali dan prosesor data pribadi melanggar beberapa pasal UU PDP, seperti yang disebutkan dalam Pasal 57 ayat (2), lembaga yang berwenang dalam penyelenggaraan perlindungan data pribadi yang telah diamanatkan oleh UU PDP dapat memberikan sanksi administratif. Sanksi administratif dapat berupa:

1. Peringatan tertulis
2. Penghentian sementara kegiatan pemrosesan Data Pribadi

3. Penghapusan atau pemusnahan Data Pribadi
4. Denda administratif

B. Secara Perdata

Mengenai pertanggungjawaban perdata, UU PDP tidak mengaturnya secara khusus. Namun, Pasal 12 Perihal Gugatan UU PDP memberikan hak kepada subjek data pribadi untuk berhakmenggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi atas nama mereka sesuai dengan ketentuan peraturan perundang-undangan. UU PDP tidak mengatur bagaimana proses gugatan ini dilakukan, tetapi memberi wewenang kepada pihak yang bertanggung jawab untuk melakukannya. Pasal 26 UU ITE sebelumnya juga mengatur dan menjamin bahwa orang yang melanggar haknya dapat menggugat penggunaan informasi melalui media elektronik yang berkaitan dengan data pribadi tanpa persetujuan orang yang bersangkutan.

Setidaknya, pelanggaran terhadap perlindungan data pribadi dapat digugat sebagai perbuatan melawan hukum berdasarkan dasar kesalahan, seperti yang diatur dalam Pasal 1365 KUHPerdata, atau ketidakpatutan, seperti yang diatur dalam Pasal 1366 KUHPerdata. Prinsip kehati-hatian ditetapkan dalam Pasal 3 UU ITE dan mewajibkan setiap penyelenggara sistem elektronik, baik korporasi maupun pemerintah, untuk menerapkan akuntabilitas sistem elektronik, yang berarti harus andal, aman, dan bertanggung jawab.

Menurut Pasal 15 UU ITE, setiap penyelenggara sistem elektronik bertanggung jawab secara hukum sepanjang masa, kecuali jika kesalahan terjadi karena kesalahan konsumen atau pengguna sistem elektronik atau akibat kejadian alam (force majeure). Jika penyelenggara tidak memberikan informasi yang sebenarnya tentang kebocoran data pribadi, kebohongan publik dan hak atas kejelasan data pengguna atau konsumen akan muncul. Jika ini terjadi, penyelenggara harus bertanggung jawab atas kebocoran data yang terjadi sehingga ini akan merugikan setiap pengguna data yang kerahasisaan datanya tidak dijaga sedemikian rupa sehingga bisa berdampak buruk bagi pengguna data tersebut.

Berdasarkan ketentuan tersebut, setiap pengguna sistem elektronik dapat menggugat ganti rugi kepada perusahaan atau lembaga pemerintah yang mengintip dan memproses data pribadi. Peradilannya tidak mudah untuk membuktikan kerugian immaterial relatif.

C. Secara Pidana

Kegiatan intrusi dari luar (akses ilegal) ke dalam sistem atau insiden di luar sistem (interception atau man in the middle attack) dapat menyebabkan data bocor. Orang dalam juga dapat membocorkan data ke luar sistem yang seharusnya menjaga kerahasiaan data pengguna. Korporasi harus bertanggung jawab atas sistem

keamanan fisik dan logis karena mereka adalah pengendali dan proseor data. Setidaknya, UU PDP memberikan payung hukum untuk penegakan hukum pidana terhadap penyalahgunaan data pribadi. Ketentuan pidana UU PDP mengatur hukuman bagi individu yang melanggarnya, serta hukuman bagi perusahaan yang mengendalikan dan memproses data pribadi. Sanksi yang dapat dikenakan atas tindak pidana dapat berupa penjara atau denda. Mereka juga dapat dikenakan sanksi tambahan seperti perampasan keuntungan, harta kekayaan yang diperoleh atau diperoleh dari tindak pidana, dan pembayaran ganti kerugian.

Pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau perusahaan dapat dipidana jika tindak pidana dilakukan oleh perusahaan. Korporasi dapat dipidana hanya dengan denda, tetapi juga dapat dibubarkan. [Pasal 70 UU Perlindungan Data Pribadi UU Nomor 27 Tahun 2022. 25]. Berdasarkan sanksi yang ada dalam UU PDP, jelas bahwa negara memiliki dasar hukum untuk memaksa penyelenggara sistem elektronik, termasuk pengendali data dan prosesor data, untuk memastikan bahwa mereka mengelola data dan sistem dengan cara yang paling efektif. Hal ini disebabkan fakta bahwa data pribadi masyarakat sebelumnya tidak aman karena potensi kebocoran dan penyalahgunaan data untuk kejahatan.

UCAPAN TERIMAKASIH

Terimakasih Kepada Ibu, istri, anak serta keluarga besar yang selalu memberikan support dan doa sehingga penulis dalam keadaan sehat dan lancar dalam melaksanakan kegiatan penelitian

Terimakasih kepada seluruh tim yang tidak dapat disebutkan namanya satu demi satu, ini semua bisa selesai karena terjalinnya silaturahmi dan hubungan yang komunikatif dengan baik dan lancar.

DAFTAR PUSTAKA

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

https://jdih.kominfo.go.id/infografis/view/21

Firdaus, Indriana. Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan, Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia. DOI: https://doi.org/10.52005/rechten.v4i2.98

Priscyllia, Fanny. Perlindungan Privasi Data Pribadi Dalam Perspektif Perbandingan Hukum, Jatiswara, 34.3 (2019) 1–5 https://doi.org/10.29303/jatiswara.v34i3.218

Niffari, Hanifan. Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain Jurnal Hukum Dan Bisnis (Selisik), 6.1 (2020), 1–14Https://Doi.Org/10.35814/Selisik.Vol 6.1699.

Herryani, MRTR. Perlindungan Hukum Terhadap Kebocoran Data Pribadi Konsumen Online Marketace, Transparansi Hukum, 5.1 (2022), 110–33. DOI: https://doi.org/10.30737/transparansi.v5i1.3096.

Peraturan Pemerintah Republik Indonesia Nomor 7l Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik.

Rahardjo, Satjipto, Ilmu Hukum, PT Citra Aditya Bakti, Bandung, 2000.

M Hadjon, Philipus, 1987, Perlindungan Bagi Rakyat Indonesia, PT Bina Ilmu, Surabaya, 1987.

Djafar, Wahyudi dan Jodi Santoso, M, Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipnya, Lembaga Studi dan Advokasi Masyarakat, Jakarta, 2019.

Djafar, Wahyudi dan Ruben Fritz, Bernhard dan Lintang, Blandina, Perlindungan data Pribadi Usulan Pelembagaan Kebijakan dari Perspektif HAM, Jakarta: 2016.

Makarim, Edmon, Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi, Kolom Hukumonline.com

Banisar, David and Davis, Simon, dikutip Dewi Rosadi, Sinta, Cyber Law, 1999.

https://www.hukumonline.com/klinik/a/terjadi-pencurian-data-pribadi-tempuh-langkah-ini-lt5d904597bfa6e/

Djafar, Wahyudi dan Komarudin, Asep, Perlindungan Hak Atas Privasi Di Internet Beberapa Penjelasan Kunci, ELSAM, Jakarta, 2014.

Kharisma Arrasuli, Beni, Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi, Vol. 7 No. 2 (2023): Unes Journal of Swara Justisia Juli 2023, https://doi.org/10.31933/ujsj.v7i2.351