PAMPAS: *Journal Of Criminal Law*
Volume 4 Nomor 2, 2023
(ISSN2721-8325)

Pertanggungjawaban Pidana Terhadap Penyalahgunaan Data Pribadi Pada Tindak Pidana Dunia Maya

Dennys Megasari br Nababan, Sahuri Lasmadi, Erwin Erwin
Fakultas Hukum, Universitas Jambi
Author's Email Correspondence: dennysmegasarinababan@gmail.com

ABSTRAK
Artikel ini adalah untuk mengetahui dan menganalisis bagaimana pertanggungjawaban pidana terhadap penyalahgunaan data pribadi pada tindak pidana dunia maya dan juga bagaimana perlindungan hukum dari penyalahgunaan data pribadi tersebut. Metode Penelitian yang digunakan adalah Yuridis Normatif dengan pendekatan perundang-undangan (*statute approach*), pendekatan konsep (*conceptual approach*) dan pendekatan kasus (*case approach*). Hasil Penelitian menunjukkan bahwa di dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi tersebut masih belum dijelaskan secara eksplisit jika terjadinya kegagalan dalam melindungi data dari subjek data pertanggungjawaban pidana yang didapatkan oleh Pengelola Data Pribadi berupa apa saja dan juga terdapat di Pasal 56 bahwa tidak dijelaskan dalam pengelolaan data pribadi subjek data pribadi harus mendapatkan perijinan dalam pengelolaan data tersebut. Saran: hendaknya dilakukan pembaharuan hukum terhadap Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dengan memperjelas pertanggungjawaban pidana apa yang didapatkan oleh pengelola data pribadi dan juga perijinan yang harus eksplisit dijelaskan dalam pengelolaan data pribadi agar tidak menimbulkan pemahaman dimasyarakat bahwa hak mereka diabaikan.

Kata Kunci:
Pertanggungjawaban Pidana; Data Pribadi; Tindak Pidana Dunia Maya

ARTICLE HISTORY
Submission: 2023-07-08
Accepted: 2023-07-08
Publish: 2023-07-31

KEYWORDS: *Criminal Liability; Personal Data; Cyber Crime*

ABSTRACT
This article is to find out and analyze how criminal responsibility is for misuse of personal data in cybercrimes and also how legal protection is from misuse of personal data. The research method used is Normative Juridical with a statutory approach (statute approach), conceptual approach (conceptual approach) and case approach (case approach). The research results show that in Law Number 27 of 2022 Concerning Personal Data Protection it is still not explicitly explained if there is a failure to protect data from criminal liability data subjects obtained by the Personal Data Manager in any form and it is also contained in Article 56 that not explained in the management of personal data the subject of personal data must obtain permission in the management of such data. Suggestion: law reform should be carried out against Law Number 27 of 2022 Concerning Personal Data Protection by clarifying what criminal liability is obtained by personal data managers and also the permits that must be explicitly explained in the management of personal data so as not to create an understanding in the community that their rights are being ignored.

A. PENDAHULUAN

Teknologi merupakan alat berupa berbagai jenis peralatan atau sistem yang berperan dalam memberikan kenyamanan dan kemudahan bagi semua orang. Di tengah revolusi industri yang terus berkembang dari waktu ke waktu, dari industri 1.0 hingga sekarang Industri 4.0, berkolaborasi antara teknologi siber dan teknologi outomasi. Menurut Hanan Widiasmara dalam Sinta Dewi

> "Transformasi digital mempunyai berbagai bentuk di berbagai belahan dunia. Di Jepang beri nama sebagai *Society 5.0*, di Eropa dinamai dengan *Industrial Revolution 4.0,* di Cina dikenal dengan nama *Made in Cina 2025*, di Amerika disebut *Industrial Internet*, dan di Asia dicanangkan dengan *Smart Cities*."[1]

Transformasi digital yang berevolusi sudah dan akan terus merubah segala sesuatunya, mulai dari dasar tanpa teknologi menjadi serba teknologi. Revolusi Industri 4.0 dan peningkatan hubungan antara bisnis dengan kehidupan sehari-hari kini mendorong perubahan dibidang bisnis yang membuat para karyawan dan pelanggan di seluruh dunia menjadi lebih praktis dalam menjalankan aktivitasnya. Pertumbuhan industri ini telah menyebabkan pengumpulan data secara kohesif, baik pemerintah maupun perusahaan swasta berlomba-lomba untuk meningkatkan muatan penyimpanan data mereka. Ditambah dengan munculnya era *big data* dan *artificial intelligence* sehingga data menjadi sebuah objek yang berwujud. Ed Dumbill memberikan pendapat yaitu:

> *"Big data is data that exceeds the processing capacity of conventional database systems. The data is too big, moves too fast, or doesn't fit the structures of your database architectures. To gain value from this data, you must choose an alternative way to process it."*[2]

Yang mana dapat diartikan Big data adalah data yang melebihi kapasitas pengolahan sistem dari database konvensional. Data terlalu besar, bergerak terlalu cepat, atau tidak sesuai dengan struktur arsitektur database yang dimiliki. Untuk mendapatkan nilai dari data ini, pemilik harus memilih cara alternatif untuk memprosesnya. Keunggulan Revolusi Industri 4.0 adalah penyediaan dan pertukaran informasi dapat disampaikan dengan cepat, mudah dan kapan saja menggunakan semua perangkat elektronik, terutama koneksi Internet yang hanya terhubung dengan keberadaan *Big Data*.

Pada era Revolusi Industri 4.0 mulai menggabungkan teknologi komputer dengan telekomunikasi untuk mengubah desain sistem informasi dan merubah pola kerja jaman dahulu. Awalnya, perlu waktu berhari-hari untuk mentransfer data atau data yang harus dikerjakan sebelum dikirim ke bagian lain dunia (dunia maya), yang saat ini dapat terjadi dalam hitungan detik. Oleh karena itu tidak dapat dihindari lagi bahwa hampir setiap aktivitas dalam kehidupan sehari-hari di era digital sangat membutuhkan data pribadi.

Data pribadi terkait erat dengan konsep kerahasiaan pribadi dimana bahwa seseorang memiliki hak untuk menutup atau membuka ruang dalam hidupnya. Ini membuat Data Pribadi semakin penting untuk dijaga kerahasiaanya. Bahkan di

---

[1]Sinta Dewi Rosadi. *Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional,* Cet. 2.PT Refika Aditama, Bandung, 2022, hlm. 2.

[2]Irhamni Ali, "*Big Data:* Apa dan pengaruhnya pada perpustakaan? *(what is Big Data and its Influnce to Library)", Media pustakawan,* Vol 22 No. 4, 2015, hlm. 19.

Indonesia terdapat beberapa peraturan yang mengatur tentang hal tersebut dan memberikan jaminan keamanan privasi data. Menurut Pasal 1 angka 22 Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan menyatakan bahwa "Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya". Kemudian, peraturan delegasi dari Undang-Undang Informasi dan Transaksi Elektronik yaitu Pasal 15 ayat (1) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik memuat tentang kewajiban dari penyelenggara Sistem Elektronik yang menyatakan bahwa:

"Penyelenggara Sistem Elektronik wajib:

a. menjaga rahasia, keutuhan, dan ketersediaan Data Pribadi yang dikelolanya;
b. menjamin bahwa perolehan, penggunaan, dan pemanfaatan Data Pribadi berdasarkan persetujuan pemilik Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
c. menjamin penggunaan atau pengungkapan data dilakukan berdasarkan persetujuan dari pemilik Data Pribadi tersebut dan sesuai dengan tujuan yang disampaikan kepada pemilik Data Pribadi pada saat perolehan data."[3]

Dalam Penjelasan Pemerintah Mengenai Rancangan Undang-Undang tentang Perlindungan Data Pribadi yang dapat dilihat dalam website resmi DPR menyatakan bahwa di skala internasional telah melihat bahwa pentingnya peraturan perlindungan data pribadi, baik secara regional maupun nasional sebagai hal yang mendesak. Saat ini, setidaknya ada 132 negara yang memiliki instrumen hukum yang secara khusus mengatur perlindungan data pribadi. Misalnya, Malaysia pada 2010, Filipina pada 2012, Singapura pada 2012, dan Thailand pada 2019.[4] Di banyak negara, perlindungan Data Pribadi berfokus pada jangkauan keberlakukan penggunaan data pribadi secara ekstrateritoreial, jenis pembagian data pribadi, prinsip-prinsip perlindungan data pribadi, hak-hak pemilik data pribadi, kondisi hukum untuk pemrosesan data pribadi dan sanksi untuk pelanggaran data pribadi.

Perlindungan data pribadi di Indonesia saat ini diatur secara sektoral dan parsial di 31 peraturan perundang-undangan, antara lain:

1. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.
2. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.
3. Undang-Undang Nomor 23 Tahun 1999 tentang Hak Asasi Manusia.
4. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
5. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan.
6. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

[3]Pasal 15 ayat (1) Peraturan Pemerintah Nomor 82 Tahun 2012 *tentang Penyelenggara Sistem dan Transaksi Elektronik.*

[4]"Penjelasan Pemerintah Mengenai Rancangan Undang-Undang tentang Perlindungan Data Pribadi", hlm. 4.

7. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
8. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Dalam Anas Aditya Wijarnako Perkembangan teknologi yang berkaitan dengan data pribadi memiliki dua efek yang berbeda tergantung pada penggunaannya. Ini adalah aspek positif dan negatif yang memiliki dampak signifikan pada perkembangan kejahatan.[5] Badan Pengkajian dan Penerapan Teknologi (BPPT) mengatakan perkembangan teknologi informasi dan komunikasi (TIK) berperan penting dalam meningkatkan kecepatan dan efisiensi berbagai layanan. Namun, juga membawa risiko penyalahgunaan teknologi informasi dari ancaman siber terhadap hal-hal yang menyebabkan terjadinya pengerusakan atau membahayakan teknologi informasi dan komunikasi. Retensi data yang terintegrasi dan terhubung dalam sistem kontrol melalui otomatisasi sistem, sistem komunikasi, pengawasan dan kecerdasan buatan, keamanan digital atau keamanan internet harus menjadi perhatian utama.

Dalam melakukan pengamanan Penyelenggara juga haruslah menyiapkan suatu tindakan yang dapat menjamin seseorang bahwa kerahasian datanya tersimpan dengan aman tanpa adanya kerugian yang ditimbulkan apabila terjadinya suatu kegagalan dalam melakukan pengamanan yang dapat menyababkan sebuah Data terbongkar ke Dunia Maya (jejaring internet). Apabila sistem keamanan digital ini diabaikan dan tidak adanya solusi terhadap terjadinya sebuah kegagalan dalam melakuan pengamanan maka akan menimbulkan suatu kesalahan yang dimana harus dipertanggungjawabkan oleh si penyelenggara sistem elektronik tersebut.

Indonesia dalam penjagaan informasi pribadi masih kurang kesadaran diri seseorang yang mana dapat menyebabkan kurangnya *security digital* saat ini, yang mana dalam memberikan suatu infromasi/identitas pribadi haruslah berhati-hati baik dalam membuka situs tertentu ataupun yang lainnya. Berikut merupakan kasus-kasus yang pernah terjadi di Indonesia:

1. Dalam jurnal Hanif Nurwa Rochman yang dikutip dalam buku Sinta Dewi Rosadi menuliskan bahwa di Indonesia sejumlah kasus tentang kebocoran data pribadi konsumen dan juga penyalahgunaan data pribadi 13 juta data akun pengguna Bukalapak dijual di Dream Market dengan harga US $5000 dan pada 4 Mei 2020, mencuat kasus tentang bocornya 91 juta data pengguna *marketplace* Tokopedia yang diperjualbelikan di *dark web* dengan harga US $50005.
2. Menurut laporan yang dikeluarkan oleh lembaga konsultan McKinsey, kasus-kasus kebocoran data selalu mencuri data pribadi pengguna, seperti data identitas diri seperti NIK (KTP), SIM, NPWP, Paspor, user ID dan *password*¸ pin ATM, kode verifikasi, kode respon/OTP, nomor kartu kredit dan CVV atau data informasi lainnya.

[5]Anas Aditya Wjanarko, Ridwan, Aliyth Prakarsa, "Peran Digital Forensik dalam Pembuktian Tempus Deliscti Sebagai Upaya Pertanggungjawaban Pidana Pelaku Pembutan Video Pornografi", *PAMPAS: Journal Of Criminal,* Vol 2 No. 2, 2011, hlm. 70.

3. Diawal tahun 2021 lebih dari 98,2 juta orang terkena dampak dari sepuluh pelanggaran data terbesar di dunia, dengan tiga dari sepuluh pelanggaran terbesar terjadi di perusahaan teknologi.[6]

Hendri mengemukakan bahwa perkembangan teknologi ini merupakan akibat dari pola-pola prilaku dan kebutuhan di masyarakat, karena perilaku dan keinginan masyarakatlah, teknologi semakin maju dan mereka juga yang telah mengembangkan cara untuk melakukan kejahatan, sebagaimana adigium "dimana ada masyarakat disitu ada kejahatan".[7] Kesalahan juga diartikan secara umum, yaitu perbuatan yang secara objektif tidak patut, karena perbuatan itu setidak-tidaknya dapat dicela. Sehingga dengan demikian dikatakan sebagai suatu kesalahan haruslah memiliki unsur-unsur sebagai berikut:

a. Adanya kemampuan bertanggungjawab;
b. Hubungan batin antara si pembuat dengan perbuatannya yang berupa sengaja *(dolus)* atau Kealpaan *(culpa);*
c. Tidak adanya alasan penghapus kesalahan atau tidak ada alasan pemaaf;[8]

Oleh karena itu kesalahan yang dimaksudkan adalah sengaja *(intention/dolus/opzet)* dan kealpaan *(negligence/culpa)* artinya kesengajaan *(dolus)* yang diartikan sebagai suatu kesengajaan dengan maksud dan sengaja sebagai kepastian serta kesengajaan sebagai kemungkinan sedangkan kealpaan *(culpa)* artinya kesalahan yang lebih ringan daripada kesengajaan karena ketidak hati-hatian dan tidak menduga bahwa akibat dari terjadinya perbuatan kesalahan tersebut merupakan keadaan jiwa dari si pembuat dan hubungan batin antara si pembuat dengan perbuatannya guna mempertanggungjawabkan pidana yang dilakukannya. Apabila seseorang telah memenuhui unsur-unsur sebagaimana yang telah dikemukakan diatas maka orang tersebut berhak dan harus mempertanggungjawabkan kesalahannya.

Dalam hukum pidana seseorang yang memiliki kesalahan dapat dipertanggungjawabkan kesalahannya berupa tanggung jawab pidana apabila kesalahannya tersebut mengandung unsur-unsur dari Pertanggungjawaban Pidana. Dalam Pasal 46 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjelaskan bahwa apabila dalam Pelindungan Data Pribadi mengalami kegagalan maka Pengendali Data Pribadi haruslah menyampaikan pemberitahuan kepada Subjek Data Pribadi dan adapun pemberitahuannya tersebut berupa data pribadi apa yang terungkap, kapan dan bagaimana Data pribadi tersebut dapat terungkap, upaya penanganan dan pemulihan apa yang didapat terkait dengan kegagalan tersebut.

Apabila dilihat bahwa kegagalan dalam pelindungan data pribadi tersebut merupakan suatu kesalahan yang dimana dapat dipertanggungjawabkan. Kesalahannya yaitu berupa ketidak hati-hatian Pengendali Data Pribadi dalam melakukan perlindungan terhadap sebuah data. Apabila dikaitkan perbuatan yang telah dilakukan oleh Pengendali Data Pribadi dengan unsur-unsur yang dari suatu kesalahan yang dapat dipertanggungjawabkan maka suatu perbuatannya tersebut

[6]Sinta Dewi Rosadi, *Op.Cit.,* hlm. 5.

[7]Hendri Diansah, Usman, Yulia Monita, "Kebijakan Hukum Pidana Terhadap Tindak Pidana *Carding", PAMPAS:Journal Of Criminal,* Vol 3 No. 1, 2022, hlm. 16. 2022.

[8]Moeljatno. *Asas-asas Hukum Pidana,* Cet. 8, Edisi Revisi, Renika Cipta, Jakarta, 2008, hlm. 147-138.

telah memenuhi unsur-unsurnya yang dimana pertama, adanya kemampuan bertanggung jawab dari pihak Pengendali data pribadi. Pihak pengendali data pribadi mampu bertanggung jawab dikarenakan perbuatannya tersebut telah diatur dalam Pasal 47 yang berbunyi "Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Pelindungan Data Pribadi." Kedua, perbuatan Pengendali Data Pribadi tersebut merupakan perbuatan yang dapat dicela karena kealpaannya dalam melakukan suatu pelindungan data pribadi yang mengakibatkan terjadinya suatu kegagalan dalam pelindungan data pribadi, kegagalan inilah yang dapat mengakibatkan suatu penyalahgunaan data pribadi yang mana juga akibat dari penyalahgunaannya tersebut seseorang yang disalahgunakan datanya mendapatkan kerugian. Ketiga, tidak adanya alasan pembenar dan pemaaf yang dapat dimintai dari Pengendali Data Pribadi, alasan pembenar dan pemaaf sendiri dapat dikenakan apabila seseorang yang melakukannya tidak memiliki kecakapan hukum seperti kurangnya daya perfikir ataupun ketidak cakapan mental. Namun jika dilihat pengendali data pribadi merupakan suatu badan yang dapat dinyatakan cakap hukum sehingga dapat dimintai pertanggungjawaban pidananya.

Pada Pasal 46 pertanggungjawaban yang diberikan oleh Undang-undang Perlindungan Data Pribadi ini merupakan pertanggungjawaban administrasi yang dimana apabila dilihat dari kesalahannya, kesalahan tersebut seharusnya sudah dikenakan sanksi pidana karena telah memenuhi unsur-unsur dari suatu pertanggungjawaban. Kesalahan yang ditimbulkan dari kegagalan pelindungan data pribadi akan menimbulkan sebuah kejahatan yang dimana kejahatan tersebut salah satunya yaitu Penyalahgunaan data pribadi inilah yang membuat terjadinya sebuah tindak pidana dunia maya *(CyberCrime)*. Tindak pidana yang dimaksudkan yaitu melanggar sebuah peraturan yang sudah ditetapkan. Dalam Dikdi M. Aried Mansur dan Elisatrus Gultom menuliskan bahwa

> "Secara umum yang dimaksud kejahatan komputer atau kejahatan dunia maya adalah upaya mamasuki atau menggunakan fasilitas komputer atau jaringan komputer tanpa ijin dan dengan melawan hukum dengan atau tanpa menyebabkan perubahan dan atau kerusakan pada fasilitas komputer yang dimasuki atau digunakan tersebut."[9]

Dalam Anita Sinaga bahwa Suatu undang-undang tidak dapat ditegakkan apabila pasal dalam undang-undang tersebut memiliki penafsiran yang berbeda-beda, peraturannya tidak jelas atau konsep dalam peraturan tersebut belum ada "Bagaimana bisa dapat diterapkan suatu aturan terhadap pelaku tindak pidana jika hukumnya saja tidak jelas dan tegas".[10] Hukum harus menjadi jaminan bagi masyarakat. Tetapi jika sebuah Pasal dalam peraturan Perundang-undangan saja tidak memiliki makna yang sah dalam hukum oleh karena itu tidak dapat digunakan sebagai dasar hukum, atau jika hukum tidak dapat diterapkan, ini dapat menyebabkan ketidakpastian hukum.

[9]Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum dan Teknologi Informasi*, Cet. 2, Refika Aditama, Bandung, 2005, hlm. 7.

[10]Anita Br Sinaga, Usman, Dheny Wahyudi, "Perbuatan Menguntit *(Stalking)* dalam Perspektif Kebijakan Hukum Pidana Indonesia", *PAMPAS:Journal Of Criminal,*Vol 2 No. 2, 2021, hlm. 18.

A. METODE PENELITIAN

Penelitian hukum dilakukan untuk mengahasilkan argumentasi, teori, atau konsep baru sebagai preskripsi dalam menjawab masalah dihadapi. Artikel ini didasarkan pada penelitian yuridis normative dengan menggunakan pendekatan perundang-undangan (*statute approach*), pendekatan konsep (*conceptual approach*) dan pendekatan kasus (*case approach*). Selanjutnya analisis terhadap permasalahan ini melalui berbagai tahap yaitu menginventarisir, melakukan sistematisasi, dan terakhir dilakukan interpretasi.

B. PEMBAHASAN

1. Pengaturan Pertanggungjawaban Atas Penyalahgunaan Data Pribadi Berdasarkan Peraturan Perundang-Undangan

Dalam konteks perlindungan data pribadi, istilah yang sering digunakan adalah informasi pribadi dan data pribadi. Perlindungan data pribadi merupakan isu yang sudah berkembang dan menjadi perhatian di Indonesia. Dewan Perwakilan Rakyat Republik Indonesia (DPR RI) akhirnya telah mengesahkan Rancangan Undang-Undang Perlindungan Data Pribadi menjadi Undang-undang dalam rapat Paripurna yang telah dilakukan pada hari selasa tanggal 20 September 2022.

Pengesahan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi membawa angin segar, Pasalnya selama ini ketentuan tentang Perlindungan Data Pribadi diatur dalam peraturan yang terpisah-pisah, Berikut merupakan beberapa peraturan tentang Data Pribadi yang menjadi evalusi dan analisis terciptanya Undang-Undang Perlindungan Data Pribadi.

a. Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

Dalam industri telekomunikasi merupakan industri yang perkembangannya dinilai sangat pesat dengan ekonomi yang tinggi pula. Sejak Indonesia telah aktif dalam idustri telekomunikasi disitu pula Indonesia mulai mengembangkan kebijakan dan peraturan perundang-undangan mengenai telekomunikasi dengan mengesahkan UU No. 3 Tahun 1989 tentang Telekomunikasi. Lalu, Undang-undang tersebut disempurnakan serta disesuaikan lagi dengan kemajuan telekomunikasi dengan mengesahkan Undang-undang No. 36 Tahun 1999 tentang Telekomunikasi yang dianggap mampu untuk menyesuaikan dengan perkembangan telekomunikasi.

Perpindahan informasi dan data pribadi saat ini terjadi dengan mudah dan sangat cepat. Menurut Pasal 1 angka 1 Undang-undang No 36 Tahun 1999 tentang Telekomunikasi bahwa "Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari hasil informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara dan bunyi melalui sistem kawat, optik, radio, atau sistem elektromagnetik lainnya;"

Dilihat dari defenisi tersebut maka penyelenggaraan telekomunikasi sangat berkaitan dengan interkoneksi, transmisi, serta perpindahan data dengan sistem elektromagnetik dengan sangat cepat. Penyalahgunaan jaringan internet yang mengganggu berjalannya akses jaringan, mengganggu ketertiban umum atau pribadi maka dapat dikenakan sanksi sebagaimana yang diatur dalam Pasal 22 yang dimana berbunyi

Pasal 22

"Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah atau memanipulasi:

a. akses ke jaringan telekomunikasi; dan atau
b. akses ke jasa telekomunikasi; dan atau
c. akses ke jaringan telekomunikasi khusus."[11]

Pasal tersebut melarang dilakukannya tindakan yang dapat mengakses kejaringan telekomunikasi dengan tidak sah. Selain itu penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dilarang dalam bentuk apa pun sebagaimana diatur dalam Pasal 40 "Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun."

Dalam Sinta Dewi "informasi yang dimiliki oleh seseorang adalah hak pribadi yang harus dilindungi, sehingga penyadapan haruslah dilarang."[12] Pengaturan sanksi pidana sebagaimana dalam memberikan kepastian hukum pada Pasal 22 dan Pasal 40 tertulis dalam Pasal 50 dan Pasal 56 dalam Pasal 50 mengatakan bahwa "Barang siapa melanggar ketentuan sebagaimana dimaksud dalam Pasal 22, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan atau denda paling banyak Rp. 600.000.000,00 (enam ratus juta rupiah)." Dan pada Pasal 56 ketentuan sanksinya berupa "Barang siapa yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 40, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun."

b. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Landasan pemikiran yang mendasari lahirnya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diundangkan pada tanggal 21 April 2008 yakni akibat keberasaan dunia maya atau dunia siber (*cyberspace*) bahwa sebuah konstruksi maya yang diciptakan oleh komputer yang di dalamnya berisi data-data abstrak yang berfungsi sebagai aktualisasi diri, wadah bertukar gagasan, dan sarana penguatan demokrasi.

Dalam pemanfaatan teknologi informasi, perlindungan data pribadi menjadi salah satu bagian dari hak privasi. Pengaturan mengenai pertanggungjawaban pidana terhadap perlindungan data pribadi yang diberikan oleh Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik terdapat dalam Pasal 32 yang dimana berbunyi

Pasal 32

"(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

[11]Pasal 22 Undang-undang No 36 Tahun 1999 tentang *Telekomunikasi.*
[12]Sinta Dewi Rosadi, *Op.Cit.,* hlm. 107.

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawna hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atu Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.

(3) Terhadap perbuatna sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya satu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya."[13]

Adapun berkaitan dengan pengenaan dengan sanksi yang diberikan kepada pihak yang diketahui merupakan pelaku dari kejahatan penggunaan data pribadi tanpa izin yang tanpa hak ikut campur atas pribadi orang lain dan telah memenuhi unsur dari tindak pidana pada Undang-undang Informasi dan Transaksi Elektronik terdapat dalam Pasal 48 Undang-undang Nomor 11 Tahun 2008.

Pasal 48

"(1) Setiap Orang yang memenuhi unsur sebagaimana imaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Psal 32 ayat (3) dipidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah)."[14]

c. Undang-Undang Nomor 24 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 24 Tahun 2006 Tentang Administrasi Kependudukan

Undang-undang tentang Administrasi Kependudukan mengatur tentang kerahasiaan dan keamanan data peristiwa kependudukan dan peristiwa penting yang terdapat dalam Pasal 8 ayat (1) huruf e Undang-Undang Nomor 24 Tahun 2016 tentang Administrasi Kependudukan.

Pasal 8 ayat (1)

"Instansi Pelaksana melaksanakan urusan Administrasi Kependudukan dengan kewajiban yang meliputi:

a. mendaftar Peristiwa Kependudukan dan mencatat Peristiwa Penting;
b. memberikan pelayanan yang sama dan profesional kepada setiap Penduduk atas pelaporan Peristiwa Kependudukan dan Peristiwa Penting;

[13]Pasal 32 Undang-Undang Nomor 11 Tahun 2008 Tentang *Informasi dan Transaksi Elektronik.*

[14]Pasal 48 Undang-Undang Nomor 11 Tahun 2008 Tentang *Informasi dan Transaksi Elektronik.*

c. mencetak, menerbitkan, dan mendistribusikan Dokumen Kependudukan;
d. mendokumentasikan hasil Pendaftaran Penduduk dan Pencatatan Sipil;
e. menjamin kerahasiaan dan keamanan data atas Peristiwa Kependudukan dan Peristiwa Penting; dan
f. melakukan verifikasi dan validasi data informasi yang disampaikan oleh Penduduk dalam pelayanan Pendaftaran Penduduk dan Pencatatan Sipil."[15]

Instansi Pelaksana Administrasi Kependudukan menjadi penanggung jawab dan juga diberikan hak akses dalam urusan kerahasian dan keamanan data bagi penduduk. Keamanan data yang dimaksud sebagaimana dalam huruf e meliputi data pribadi penduduk yang dijelaskan dalam Pasal 84 ayat (1) dimana Data Pribadi memuat nomor Kartu Keluarga (KK), keterangan tentang catatan fisik dan/atau mental, Nomor Induk Kependudukan (NIK), NIK ibu kandung, NIK ayah, tanggal/bulan/tahun lahir, dan beberapa isi catatan peristiwa penting.

Dalam pengaksesan sebuah data kependudukan haruslah sesuai dengan peraturan yang ada. Apabila terjadi sebuah pelanggaran atau ilegal akses maka akan diberikan ancaman pidana sesuai dengan ketentuan yang berlaku sebagaimana larangan yang terdapat dalam Pasal 77 dan Pasal 86. Pasal 77 berbunyi "Setiap orang dilarang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi Data Kependudukan dan/atau elemen data Penduduk." Lalu pada Pasal 86 berbunyi:

Pasal 86

"(1) Menteri sebagai penanggung jawab memberikan hak akses Data Pribadi kepada petugas provinsi dan petugas Instasi Pelaksana.
(1a) Petugas sebagaimana dimaksud pada ayat (1) dilarang menyebarluaskan Data Pribadi yang tidak sesuai dengan kewenangannya.
(2) Ketentuan lebih lanjut mengenai persyaratan, ruang lingkup, dan tata cara mengenai pemberian hak akses sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Menteri."[16]

Ancaman Pidana atas pelanggaran privasi serta penyalahgunaan data pribadi dalam administrasi kependudukan selanjutnya diatur dalam Pasal 94 dan Pasal 95 A

Pasal 94

"Setiap orang yang memerintahkan dan/atau memfasilitasi dan/atau melakukan manipulasi Data Kependudukan dan/atau elemen data Penduduk sebagaimana dimaksud dalam Pasal 77 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 75.000.000,00 (tujuh puluh lima juta rupiah)."[17]

[15]Pasal 8 ayat (1) Undang-Undang Nomor 24 Tahun 2016 tentang *Administrasi Kependudukan.*

[16]Pasal 86 Undang-Undang Nomor 24 Tahun 2016 tentang *Administrasi Kependudukan.*

[17]Pasal 94 Undang-Undang Nomor 24 Tahun 2016 Tentang *Perubahan Atas Undang-Undang Nomor 24 Tahun 2006 Tentang Administrasi Kependudukan.*

Pasal 95A

"Setiap orang yang tanpa hak menyebarluaskan Data Kependudukan sebagaimana dimaksud dalam Pasal 79 ayat (3) dan Data Pribadi sebagaimana dimaksud dalam Pasal 86 ayat (1a) dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp. 25.000.000,00 (dua puluh lima juta rupiah)."[18]

Dalam beberapa peraturan yang telah ditulis diatas dapat dilihat bahwa selama ini peraturan tentang Data Pribadi masih diatur diberbagai peraturan sesuai dengan konsentrasinya. Sehingga, pemerintahan Indonesia menerbitkan Peraturan mengenai Perlindungan Data Pribadi demi mengisi kekosongan hukum di Indonesia. Undang-undang tentang Perlindungan Data Pribadi ini selalu dihubungkan dengan hak privasi (*privacy rights*). Pasal 1 angka 1 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menjelaskan defenisi dari Data Pribadi. Dimana Pasal 1 angka 1 berbunyi "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik."

Dilihat dari defenisi tersebut bahwa Data Pribadi digunakan sebagai tanda pengenal agar orang lain mampu mengidentifikasi kita sebagai subjek hukum. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi mengatur tentang pemrosesan Data Pribadi yang tercatat dalam Pasal 16 yang dimana Pasal tersebut menjadi prinsip dari perlindungan Data Pribadi.

Pasal 16

"(1) Pemrosesan Data Pribadi meliputi:
   a. pemrolehan dan pengumpulan;
   b. pengolahan dan penganalisisan;
   c. penyimpanan;
   d. perbaikan dan pembaruan;
   e. penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau
   f. penghapusan atau pemusnahan.

(2) Pemrosesan Data Pribadi sebagaimana dimaksud pada ayat(1) dilakukan sesuai dengan prinsip Perlindungan Data Pribadi meliputi:
   a. pengumpulan Data Pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan;
   b. pemrosesan Data Pribadi dilakukan sesuai dengan tujuannya;
   c. pemrosesan Data Pribadi dilakukan dengan menjamin hak Subjek Data Pribadi;

[18]Pasal 95 A Undang-Undang Nomor 24 Tahun 2016 Tentang *Perubahan Atas Undang-Undang Nomor 24 Tahun 2006 Tentang Administrasi Kependudukan.*

d. pemrosesan Data Pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan;
e. 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/atu penghilangan Data Pribadi;
f. pemrosesan Data Pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan Perlindungan Data Pribadi;
g. Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan Subjek Data Pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan; dan
h. pemrosesan Data Pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas.

(3) Ketentuan lebih lanjut mengenai pelaksanaan pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah."[19]

Pemrosesan Data Pribadi sebagaimana yang telah dijelaskan diatas dapat dilihat bahwa setiap pergerakan dalam pemrosesan sebuah Data Pribadi haruslah dilakukan sesuai dengan tujuan dan dilakukan dengan melindungi keamanan Data Pribadi dari segala sesuatu akses yang dilakukan dengan cara tidak sah. Undang-Undang ini juga mengatur secara detail prihal siapa saja yang dapat memproses Data Pribadi tersebut yang ditercantum dalam Pasal 18.

Pasal 18

"(1) Pemrosesan Data Pribadi dapat dilakukan oleh 2 (dua) atau lebih Pengendali Data Pribadi.
(2) Dalam hal Pemrosesan Data Pribadi dilakukan oleh 2 (dua) atau lebih Pengendali Data Pribadi harus memenuhi syarat minimal:
a. terdapat perjanjian antara para Pengendali Data Pribadi yang memuat peran, tanggung jawab, dan hubungan antar-Pengendali Data Pribadi;
b. terdapat tujuan yang saling berkaitan dan cara pemrosesan Data Pribadi yang ditentukan secara bersama; dan
c. terdapat narahubung yang ditunjuk secara bersama-sama."[20]

Undang-undang mensyaratkan bahwa jika pemrosesan data pribadi dilakukan dua atau lebih, pengontrol data juga harus mematuhi persyaratan minimumnya, masing-masing harus ada perjanjian antara pengontrol data pribadi yang harus mencakup peran tanggung jawab, dan hubungan antara pengontrol data. Dalam melakukan sebuah pemrosesan Data Pribadi

[19]Pasal 16 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.
[20]Pasal 18 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.

pengendali Data Pribadi juga harus melindungi dan memastikan keamanan Data Pribadi sebagaimana yang telah dicantumkan dalam Pasal 35.

Pasal 35

"Pengendali Data Pribadi wajib melindungi dan memastikan kemanan Data Pribadi yang diprosesnya, dengan melakukan :

a. penyusunan dan penerapan langkah teknis operasional untuk melindungi Data Pribadi dari gangguan pemrosesan Data Pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan
b. penentuan tingkat keamanan Data Pribadi dengan memperhatikan sifat dan risiko dari Data Pribadi yang harus dilindungi dalam pemrosesan Data Pribadi."[21]

Sehingga Pengendali Data Pribadi memiliki tanggung jawab untuk meningkatkan keamanan Data Pribadi. Apabila Pengendali Data Pribadi tidak dapat memastikan dan melindungi sebua kemananan Data Pribadi atau jika terjadinya sebuah kegagalan dalam melindungi sebuah Data Pribadi maka Pengendali Data Pribadi wajib memberitahukan kepada masyarakat bahwa telah terjadi kegagalan dalam melindungi Data Pribadi sebagaimana yang telah diatur dalam Pasal 46.

Pasal 46

"(1) Dalam hal terjadi kegagalan Perlindungan Data Pribadi, Pengendali Data Pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambar 3 × 24 (tiga kali dua puluh empat) jam kepada:
   a. subjek Data Pribadi; dan
   b. lembaga.

(2) Pemberitahuan tertulis sebagaimana dimaksud pada ayat (1) minimal memuat:
   a. Data Pribadi yang terungkap;
   b. kapan dan bagaimana Data Pribadi terungkap; dan
   c. upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pegendali Data Pribadi.

(3) Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Perlindungan Data Pribadi."[22]

Di Indonesia, seringkali ada kekurangan dalam penerapan sanksi perdata, administratif dan pidana terhadap tindakan peradilan. Secara khusus, dilihat dalam undang-undang ini, tidak ada ketentuan yang secara jelas menyimpulkan bahwa penerapan sanksi perdata atau administratif harus menjadi prioritas dalam menyelesaikan sengketa atas penanganan data pribadi, dari pada sanksi pidana.

Apabila dilihat dari Pasal 46 tersebut kegagalan Perlindungan Data Pribadi merupakan suatu kesalahan yang dimana dapat dipertanggungjawabkan bukan hanya dari pertanggungjawaban administrasi saja namun juga dapat dipertanggungjawabkan pidananya.

[21]Pasal 35 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.
[22]Pasal 46 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.

Pertanggungjawaban Pidana dapat diberikan apabila memenuhi syarat-syarat dari sebuah kesalahan yang dimana kesalahannya terdapat dalam kegagalan melindungi sebuah Data Pribadi, jika dilihat kesalahan tersebut sudah memenuhi unsur-unsur dari sebuah kesalahan sebagaimana yang telah dijelaskan dalam Bab 2 tentang Pertanggungjawaban Pidana.

Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi ini jika terjadinya sebuah kegagalan dalam melindungi Data Pribadi hanya dikenakan sebuah sanksi administrasi saja sebagaimana yang telah tertulis dalam Pasal 57.

Pasal 57

"(1) Pelanggaran terhadap ketentuan Pasal 20 ayat (1), Pasal 21, Pasal 24, Pasal 25 ayat (2), Pasal 26 ayat (3), Pasal 27, Pasal 28, Pasal 29, Pasal 30, Pasal 31, Pasal 32 ayat (1), Pasal 33, Pasal 34 ayat (1), Pasal 35, Pasal 36, Pasal 37, Pasal 38, Pasal 39 ayat (1), Pasal 40 ayat (1), Pasal 41 ayat (1) dan ayat (3), Pasal 42 ayat (1), Pasal 43 ayat (1), Pasal 44 ayat (1), Pasal 45, Pasal 46 ayat (1), Pasal 49, Pasal 51 ayat (1) dan ayat (5), Pasal 52, Pasal 53 ayat (1), Pasal 55 ayat (2), dan Pasal 56 ayat (2) sampai dengan ayat (4) dikenakan sanksi administratif.

(2) Sanksi administratif sebagaiamana yang dimaksud pada ayat (1) berupa:
   a. peringatan tertulis;
   b. penghentian sementara kegiatan pemrosesan Data Pribadi;
   c. penghapusan atau pemusnahan Data Pribadi; dan/atau
   d. denda administratif.

(3) Sanksi administratif berupa denda administratif sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

(4) Penjatuhan sanski administratif sebagaimana dimaksud pada ayat (2) diberikan oleh lembaga.

(5) Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi administratif sebagaimana dimaksud pada ayat (3) diatur dalam Peraturan Pemerintah."[23]

Untuk mencegah penyalahgunaan data pribadi, ini harus menjadi titik kritis/poin penting dalam Undang-Undang Perlindungan Data Pribadi. Kegagalan dalam melindungi Data Pribadi ini seharusnya juga diberikan sanksi pidana karena sebuah kesalahan haruslah dapat dipertanggungjawabkan perbuatannya. Dalam ketentuan pidana pada Undang-undang ini diatur dalam Pasal 67

Pasal 67

"(1) Setiap Orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan Data Pribadi yang buka miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama

[23]Pasal 57 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.

5 (lima) tahun dan/atau pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

(2) Setiap Orang yang dengan sengaja dan melawan hukum mengungkapkan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

(3) Setiap Orang yang dengan sengaja dan melawan hukum menggunakan Data Pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."[24]

Ketentuan pidana sebagaimana dijelaskan di atas diberikan bagi orang yang secara sadar dan melawan hukum memperoleh atau mengumpulkan Data Pribadi, mengungkapkan Data Pribadi, menggunakan Data Pribadi milik orang lain. Kegagalan dalam melindungi data pribadi dapat menyebabkan sebuah kesalahan yang dimana orang lain dapat dengan sengaja menggunakan Data Pribadi orang lain dengan sembarangan yang dapat menyebabkan kerugian bagi pemilik Data Pribadi.

Sehingga perlu diperhatikan lagi bahwa masih terdapat ketentuan yang tidak tegas dalam memberikan sanksi dari pertanggungjawaban pidana terhadap Perlindungan Data Pribadi yang dimaksud dalam Pasal 46 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi karena dalam Pasal 46 tidak mengatur bagaimana bentuk dari pertanggungjawaban pidana jika terjadinya sebuah kegagalan dalam Perlindungan Data Pribadi.

2. Perlindungan Hukum Atas Penyalahgunaan Data Pribadi Berdasarkan Asas Kepastian Hukum.

Perlindungan Hukum terhadap Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi merupakan Undang-undang yang yuridiksi hukumnya bersifat transnasional baik dari keperdataan, administratif dan pidana. Jaminan perlindungan Hukum yang diberikan undang-undang ini kepada pemilik Data Pribadi di Indonesia dalam menempuh penyelesaian sengketa dengan pengendali Data Pribadi di luar negara Indonesia memiliki kelemahan dalam penerapan pada Undang-Undang Perlindungan Data Pribadi ini.

Pada Bab VII Pasal 56 ayat (1) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi mengemukakan bahwa Pengendali Data Pribadi dapat melaksanakan proses pentransferan Data Pribadi untuk Pengendali dan/atau prosesor Data Pribadi di luar wilayah hukum Negara Indonesia.

Pasal 56

"(1) Pengendali Data Pribadi dapat melakukan transfer Data Pribadi kepada Pengendali Data Pribadi dan/atau Prosesor Data Pribadi di

[24]Pasal 67 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.

luar wilayah hukum Negara Republik Indonesia sesuai dengan ketentuan yang diatur dalam Undang-Undang ini.

(2) Dalam melakukan transfer Data Pribadi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib memastikan negara tempat kedudukan Pengendali Data Pribadi dan/atau Prosesor Data Pribadi yang menerima transfer Data Pribadi memiliki tingkat Perlindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini.

(3) Dalam hal ketentuan sebagaimana dimaksud pada ayat (2) tidak terpenuhi, Pengendali Data Pribadi wajib memastikan terdapat Perlindungan Data Pribadi yang memadai dan bersifat mengikat.

(4) Dalam hal ketentuan sebagaimana dimaksud pada ayat (2) dan ayat (3) tidak terpenuhi, Pengendali Data Pribadi wajib mendapatkan persetujuan Subjek Data Pribadi.

(5) Kentuan lebih lanjut mengenai transfer Data Pribadi diatur dalam Peraturan Pemerintah."[25]

Pada ayat (1) dalam Pasal tersebut tidak secara tegas memberikan frasa "dengan persetujuan pemilik Data Pribadi" setelah frasa "Pengendali Data Pribadi.....kepada Pengendali Data Pribadi" di luar wilayah hukum Indonesia. Sehingga ketetapan yang telah dibuat tersebut dapat mengakibatkan hak absolut (*absolute rights*) pemilik Data Pribadi diabaikan dan ketentuan tersebut hasilnya akan bertentangan dengan tujuan utama dibentuknya Undang-Undang Perlindungan Data Pribadi ini.

Dalam Pasal tersebut seolah-olah tidak mementingkan hak Pemilik Data dalam mendapatkan pemberitahuan sebagaimana yang telah dijelaskan dalam Undang-Undang tersebut bahwa Subjek Data Pribadi memilik hak untuk dimintai persetujuan apabila Pengendali Data Pribadi melalukan suatu pemrosesan terhadap sebuah Data Pribadi dari Subjek Data Pribadi sebagaimana yang tertulis dalam Pasal 20 dan Pasal 21 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Pasal 20

"(1) Pengendali Data Pribadi wajib memiliki dasar pemrosesan Data Pribadi.

(2) Dasar pemrosesan Data Pribadi sebagaimana dimaksud pada ayat (1) meliputi:

a. persetujuan yang sah secara eksplisit dari Subjek Data Pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah disampaikan oleh Pengendali Data Pribadi kepada Subjek Data Pribadi;

b. pemenuhan kewajiban perjanjian dalam hal Subjek Data Pribadi merupakan salah satu pihak atau untuk memenuhi permintaan Subjek Data Pribadi pada saat akan melakukan perjanjian;

[25]Pasal 56 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.

c. pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan;
d. pemenuhan pelindungan kepentingan vital Subjek Data Pribadi;
e. pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan; dan/atau
f. pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi."[26]

Pasal 21

"(1) Dalam hal pemrosesan Data Pribadi berdasarkan persetujuan sebagaimana dimaksud dalam Pasal 20 ayat (2) huruf a, Pengendali Data Pribadi wajib menyampaikan informasi mengenai:
a. osesan Data Pribadi;
b. tujuan pemrosesan Data Pribadi;
c. jenis dan relevansi Data Pribadi yang akan diproses;
d. jangka waktu retensi dokumen yang memuat Data Pribadi;
e. rincian mengenai Informasi yang dikumpulkan;
f. jangka waktu pemrosesan Data Pribadi; dan
g. hal Subjek Data Pribadi.

(2) Dalam hal terdapat perubahan Informasi sebagaimana dimaksud pada ayat (1), Pengendali Data Pribadi wajib memberitahukan kepada Subjek Data Pribadi sebelum terjadi perubahan Informasi."[27]

Dalam Pasal diatas dapat dilihat bahwa dalam Pemrosesan Data Pribadi Pengendali Data Pribadi haruslah meminta persetujuan kepada Subjek Data Pribadi secara sah dan juga Pengendali Data Pribadi wajib menyampaikan informasi mengenai tujuan-tujuan yang akan dicapai dalam pemrosesan Data Pribadi. Hal ini jelas bahwa Pasal 56 ayat (1) bertentangan dengan tujuan utama dari Perlindungan Data Pribadi.

Pada Pasal 20 ayat (2) huruf a dijelaskan bahwa Pengendali Data Pribadi harus meminta persetujuan secara eksplisit dari Subjek Data Pribadi dan juga dijelaskan pada Pasal 21 ayat (1) huruf a apabila Pengendali melakukan pemrosesan Data Pribadi harus memberitahukan kepada Subjek Data Pribadi mengenai informasi untuk apa digunakannya Data Pribadi tersebut. Pasal 56 ayat (4) dijelaskan bahwa "Pengendali Data Pribadi wajib mendapatkan persetujuan Subjek Data Pribadi jika ketentuan dari kewajiban Pengendali Data Pribadi untuk memastikan negara penerima transfer Data Pribadi memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi dari peraturan perundang-undangan ini dan memastikan Pelindungan Data Pribadi memadai dan bersifat mengikat". Dalam Pasal ini dapat diartikan bahwa Pengendali Data

[26]Pasal 20 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.
[27]Pasal 21 Undang-Undang Nomor 27 Tahun 2022 Tentang *Perlindungan Data Pribadi*.

Pribadi hanya akan meminta persetujuan kepada Subjek Data Pribadi apabila hal-hal tersebut terpenuhi. Sedangkan, sudah dijelaskan bahwa setiap Pengendali Data Pribadi melakukan pemrosesan haruslah ada ijin terlebih dahulu dari Subjek Data Pribadi.

Perlindungan terhadap Data Pribadi adalah bagian dari penghormatan atas hak privasi (*the right of privacy*) harus di mulai dengan memberikan kepastian hukum.Oleh karena itu, jaminan atas perlindungan terhadap Data Pribadi harus dimuat dalam instrumen hukum yang memiliki kekuatan tertinggi yaitu konstitusi dan juga instrumen hukum tersebut haruslah bersifat tegas agar dapat memberikan perlindungan yang eksplisit terhadap masyarakat. Kepastian hukum harus dijaga demi keamanan dan ketertiban suatu negara dan pada akhirnya hukum positif harus selalu ditaati.

Bertolak dari uraian diatas maka dalam melakukan perlindungan hukum terhadap Data Pribadi haruslah sebuah peraturan tersebut bersifat tegas agar masyarakat dapat merasa terlindungi haknya. Ketiadaan bentuk kepastian hukum yang jelas terhadap penyalahgunaan data pribadi akan berakibat terhadap kesejahteraan masyarakat.

D. SIMPULAN

Dalam Undang-Undang Perlindungan Data Pribadi masih belum mengatur secara tegas tentang pemidanaan terhadap apabila terjadinya kegagalan dalam melindungi Data Pribadi sebagaimana yang diatur dalam Pasal 46 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 46 dalam terjadinya sebuah kegagalan Perlindungan Data Pribadi dikenakan sanksi Administratif saja. Ketidakjelasan pengaturan mengenai pertanggungjawaban pidana apabila terjadinya kegagalan Perlindungan Data Pribadi pada Tindak Pidana Dunia Maya ini menimbulkan ketidakpastian hukum bagi Subjek Hukum dalam mendapatkan Perlindungan akan Data Pribadinya.

Tidak hanya dalam Pasal 46 saja, pada Pasal 56 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi juga tidak secara eksplisit menjelaskan tentang Perijinan dalam pengelolaan Data Pribadi yang dilakukan di luar wilayah hukum Negara Republik Indonesia. Ketidaktegasan yang terdapat pada Pasal 56 tersebut dapat menyebabkan Perlindungan akan Data Pribadi menjadi rentan terjadinya sebuah Penyalahgunaan Data Pribadi.

DAFTAR PUSTAKA

Dokumen Hukum

Republik Indonesia, *Undang-Undang Tentang Telekomunikasi.* UU Nomor 36 Tahun 1999. LNRI 154, TLNRI 3881.

_____.*Undang-Undang tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik*.UU Nomor 19 Tahun 2016. LNRI 251, TLNRI 5952.

_____.*Undang-Undang TentangPerubahan Atas Undang-Undang Nomor 24 Tahun 2006 Tentang Administrasi Kependudukan.* UU Nomor 24 Tahun 2016. LNRI 120, TLNRI 5893.

_____.*Undang-Undang Tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.*UU Nomor 24 Tahun 2013. LNRI Nomor 232, TLNRI Nomor 5375.

_____.*Undang-Undang tentang Perlindungan Data Pribadi*. UUNomor 27 Tahun 2022, LNRI 196, TLNRI 6820.

_____.*Peraturan Pemerintah tentang Penyelenggara Sistem dan Transaksi Elektronik*. PPNomor 82 Tahun 2012, LNRI 189, TLNRI 5348.

Buku

Dikdik M. Arief Mansur dan Elisatris Gultom, *Cyber Law Aspek Hukum dan Teknologi Informasi*, Cetakan Ke-2, Refika Aditama, Bandung, 2005.

Moeljatno. *Asas-asas Hukum Pidana,* Cetakan Ke-8, Edisi Revisi, Renika Cipta, Jakarta, 2008.

Sinta Dewi Rosadi. *Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional,* Cetakan Ke-2, Refika Aditama, Bandung, 2022

Jurnal

Irhamni Ali, "*Big Data:* Apa dan pengaruhnya pada perpustakaan? *(what is Big Data and its Influnce to Library)", Media pustakawan,* Vol 22 No. 4, (2015).

Anas Aditya Wjanarko, Ridwan, Aliyth Prakarsa, "Peran Digital Forensik dalam Pembuktian Tempus Deliscti Sebagai Upaya Pertanggungjawaban Pidana Pelaku Pembutan Video Pornografi", *PAMPAS: Journal Of Criminal,* Vol 2 No. 2, (2011).

Hendri Diansah, Usman, Yulia Monita, "Kebijakan Hukum Pidana Terhadap Tindak Pidana *Carding", PAMPAS:Journal Of Criminal,* Vol 3 No. 1, (2022).

Anita Br Sinaga, Usman, Dheny Wahyudi, "Perbuatan Menguntit *(Stalking)* dalam Perspektif Kebijakan Hukum Pidana Indonesia", *PAMPAS:Journal Of Criminal,*Vol 2 No. 2, (2021).