BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Umum tentang Perdagangan Elektronik atau Electronic Commerce (*E-commerce*)

Perdagangan Elektronik atau *Electronic Commerce* atau yang lebih dikenal dengan *e-commerce* merupakan kegiatan menjual, membeli, memasarkan, menyebarkan barang dan jasa yang memanfaatkan teknologi internet yang tidak mengharuskan para pihak untuk bertemu secara langsung karena dengan mengandalkan teknologi internet tersebut, seluruh kegiatan baik pembayaran dan pertukaran data dilakukan secara elektronik atau *online.*[22] Lebih luas lagi, *e-commerce* disebut juga sebagai bagian dari *e-business* di mana seluruh aktivitas bisnisnya dilakukan secara *online* dan tidak terbatas hanya pada kegiatan jual beli saja, namun seluruh kegiatan yang mendukung proses kegiatan jual beli dalam menunjang kesuksesan *e-commerce.*

Di lansir dari Kominfo, terdapat 4 (empat) komponen yang diperlukan dalam sistem *e-commerce*, yaitu: *Marketplace/Store*, penjual dan pembeli, *payment gateway*, dan jasa pengiriman.

Pertama, *marketplace* merupakan tempat yang berisikan beberapa penjual dan melakukan transaksi jual beli *online* terhadap pembeli, seperti Tokopedia, Shopee, dan lainnya. Sedangkan *online store* hanya memiliki satu penjual saja sehingga pembeli bisa langsung memesan kebutuhannya ke penjual, seperti Matahari, Zalora, dan lainnya. Kedua, penjual dan pembeli. Penjual adalah pihak yang melakukan penjualan ke pembeli, sedangkan pembeli adalah pihak yang melakukan pembelian ke penjual. Ketiga, *payment gateway* merupakan sistem elektronik yang membantu proses pembayaran dari pembeli ke penjual baik melalui transfer, dompet elektronik (*e-wallet*), dan kartu kredit. Keempat, jasa pengiriman

[22] Pusat Pendidikan dan Pelatihan Perdagangan, "*E-Commerce*" diakses Februari 19 2023, http://pusdiklat.kemendag.go.id/v2019/article/e-commerce.

merupakan jenis transportasi yang akan digunakan untuk melakukan pengiriman barang yang di pesan oleh pembeli.

Mengingat beragamnya kegiatan transaksi dalam *e-commerce,* terdapat 4 (empat) jenis *e-commerce* yang paling sering di pilih dilansir dari Pusat Pendidikan dan Pelatihan Perdagangan Kementerian Dalam Negeri, yaitu:

1. *"E-commerce Business to Business (B2B) merupakan transaksi antar para pihak yang berkepentingan dalam menjalankan kegiatan bisnis yang tujuannya adalah mendapatkan keuntungan seperti pembayaran kartu kredit.*
2. *E-commerce Business to Consumer (B2C) merupakan transaksi elektronik antar pelaku usaha dengan konsumen.*
3. *E-commerce Consumer to Consumer (C2C) merupakan transaksi langsung antara konsumen dengan konsumen.*
4. *E-commerce Consumer to Business (C2B) merupakan transasksi langsung antara konsumen dan produsen yang menjual produk atau jasa secara online".*[23]

Banyak hal yang dijadikan pertimbangan konsumen memilih untuk berbelanja *online* bukan hanya karena lebih menghemat waktu, melainkan konsumen dapat melakukan transaksi di mana pun dan kapan pun, harga barang yang kompetitif serta dapat melakukan transaksi antar negara yang di wadahi oleh *marketplace*.

2.2. Tinjauan Umum tentang Perlindungan Data Pribadi

Perkembangan teknologi informasi yang pesat membuat seluruh kegiatan usaha mengandalkan jaringan internet untuk seluruh kegiatannya baik dalam penyimpanan dan pengumpulan data penting yang tentunya membuka peluang untuk para peretas dalam penyalahgunaan data pribadi. Merujuk pada Pasal 1 angka (29) Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik data pribadi adalah:

> *"Setiap data tentang seseorang baik yang teridentifikasi dan/atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan*

[23] Simamora, Caterin M, Pusat Pendidikan dan Pelatihan Perdagangan Kemendag, "*E-Commerce"* diakses Februari 19 2023, http://pusdiklat.kemendag.go.id/v2019/article/e-commerce.

informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau nonelektronik."[24]

Walaupun hingga pertengahan tahun 2022 Indonesia belum memiliki pengaturan sendiri mengenai perlindungan data pribadi, namun di dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) tepatnya dalam Pasal 28G ayat (1) telah di atur 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."[25]

Maka berdasarkan bunyi pasal di atas dikatakan bahwa perlindungan diri pribadi termasuk ke dalam hak asasi manusia, maka data pribadi yang melekat dengan kehidupan seseorang adalah hak setiap manusia yang harus dilindungi. Setelah beberapa peraturan perundang-undangan yang secara tidak khusus mengatur mengenai perlindungan data pribadi, pada 17 Oktober 2022 disahkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menandakan babak baru untuk Indonesia dalam hal perlindungan data pribadi masyarakatnya.

Merujuk pada Pasal 1 angka (2) Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, perlindungan data pribadi merupakan:

"Keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi".[26]

2.2.1. Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Sesuai dengan ketentuan dalam Pasal 1 angka 5 Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-

[24] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 1 angka (29).

[25] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pasal 28G ayat (1).

[26] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 1 angka (2).

Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sistem elektronik merupakan:

> *"Serangkaian peranagkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik".*[27]

Kemudian merujuk pada Pasal 1 angka (1) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, informasi elektronik adalah:

> *"Satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, electronic data interchange (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya".*[28]

Informasi elektronik yang telah tercatat ke dalam sistem elektronik oleh penyelenggara sistem elektronik tentunya harus dipastikan tersimpan dengan aman di dalam jaringan sistem elektronik guna memberikan jaminan perlindungan data pribadi masyarakatnya. Dalam Pasal 26 Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik diatur mengenai penyalahgunaan data pribadi di mana setiap masyarakat yang merasa haknya dirugikan atas dasar bocornya data pribadi mereka merupakan hak mereka agar data mereka terlindungi dan mendapatkan perlindungan hukum.

> *"(1) 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.*

[27] Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 1 angka (5).

[28] *Ibid*. Pasal 1 angka (1).

(2) *Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini."*[29]

Pasal 26 ayat (1) Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan penjelasan bahwa perlindungan data pribadi adalah satu kesatuan dari hak pribadi meliputi menikmati kehidupan yang bebas dari gangguan, berkomunikasi dengan orang lain tanpa harus merasa was-was, dan pengawasan atas teraksesnya informasi kehidupan dan data seseorang.

Disebutkan juga bahwa Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengatur mengenai perbuatan terlarang yang tidak boleh dilakukan seperti: distribusi, transisi, dan terbukanya akses informasi orang lain dengan upaya apapun[30]. Maka, setiap orang yang melakukan tindakan tersebut akan berhubungan langsung dengan ketentuan pidana yang telah diatur dalam Bab XI Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

(1) *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).*[31]
(2) *Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan.atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain".*[32]

[29] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 26 ayat (1) dan (2).
[30] *Ibid.* Pasal 27.
[31] *Ibid*. Pasal 45 ayat (1).
[32] Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 31 ayat (1).

2.2.2. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE 2019)

Sebelum disahkannya Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik sudah terdapat Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Namun seiring dengan perkembangan teknologi dan kebutuhan masyarakat, maka dibutuhkan peraturan yang sesuai dengan kondisi saat itu. Kehadiran Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga sebagai pengaturan pengaturan lebih lanjut dari Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

> *"Penyelenggara sistem elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain."*[33]

Kemudian yang dimaksud dengan pengguna sistem elektronik adalah:

> *"Setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang memanfaatkan barang, jasa, fasilitas, atau informasi yang disediakan oleh penyelenggara sistem elektronik".*[34]

Dalam penyelenggarannya, terdapat dua ruang lingkup penyelenggara sistem elektronik, yaitu ruang lingkup publik dan ruang lingkup privat. Penyelenggara sistem elektronik lingkup publik merupakan instansi penyelenggara negara dan institusi yang tidak bertugas dalam sektor keuangan.[35] Sedangkan penyelenggara sistem elektronik lingkup privat

---

[33] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 1 angka (5).

[34] *Ibid.* Pasal 1 angka (11).

[35] *Ibid.* Pasal 2 ayat (3) dan (4).

merupakan penyelenggara yang diawasi oleh kementerian atau lembaga dan penyelenggara yang mempunyai portal, situs atau aplikasi daring yang menawarkan dan mendagangkan barang atau jasa, keuangan, pembayaran digital, pengoperasian layanan komunikasi, layanan mesin pencari dan pemrosesan data pribadi.[36]

Seperti yang di atur dalam Pasal 2 ayat (5) huruf b poin 6 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik mengenai pemrosesan data pribadi, dalam menjalankan prinsip perlindungan data pribadi, penyelenggara sistem elektronik harus melakukan pemrosesan data pribadi dengan cara: *perolehan dan pengumpulan, pengolahan dan penganalisisan, penyimpanan, perbaikan dan pembaruan, penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan, serta penghapusan atau pemusnahan*[37] meliputi:

a. *"Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan sepengetahuan dan persetujuan dari pemilik data pribadi;*
b. *Pemrosesan data pribadi dilakukan sesuai dengan tujuannya;*
c. *Pemrosesan data pribadi dilakukan dengan menjamin hak pemilik data pribadi;*
d. *Pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dapat dipertanggungjawabkan, dan memperhatikan tujuan pemrosesan data pribadi;*
e. *Pemrosesan data pribadi dilakukan dengan melindungi keamana data pribadi dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta pengubahan atau perusahan data pribadi;*
f. *Pemrosesan data pribadi dilakukan dengan memberitahukan tujuan pengumpulan, aktivitas pemrosesan, dan kegagalan perlindungan data pribadi, dan;*
g. *Pemrosesan data pribadi dimusnahkan dan/atau dihapus kecuali masih dalam masa retensi sesuai*

[36] *Ibid.* Pasal 2 ayat (5).
[37] *Ibid.* Pasal 14 ayat (2).

dengan kebutuhan berdasarkan ketentuan peraturan perundang-undangan".[38]

Dalam menjalankan kewajibannya, penyelenggara sistem elektronik berkewajiban untuk mengupayakan segala cara untuk pencegahan teraksesnya informasi atau dokumen elektronik[39] dengan cara mengamankan komponen sistem elektronik dengan cara menjalankan sarana dan prosedur pengamanan sistem elektronik dan menyediakan sistem keamanan yang meliputi sistem pencegahan, prosedur, dan penanggulangan bencana.[40]

2.2.3. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Permenkominfo 20/2016)

Disahkannya Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik merupakan hasil pertimbangan dari Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaran Sistem dan Transaksi Elektronik yang mengatur lebih lanjut mengenai perlindungan data pribadi. Di dalam Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, data pribadi diartikan sebagai berikut:

"Data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenarannya dan dilindungi kerahasiaannya".[41]

Sesuai dengan Pasal 26 Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, pemilik data pribadi berhak atas:

a. *"Kerahasiaan data pribadinya;*
b. *Mengajukan pengaduan dalam rangka penyelesaian sengketa data pribadi atas kegagalan perlindungan*

[38] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 14 ayat (1).
[39] *Ibid*. Pasal 26 ayat (1).
[40] *Ibid.* Pasal 24 ayat (1) dan (2).
[41] Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi. Pasal 1 angka (1).

kerahasiaan data pribadinya oleh penyelenggara sistem elektronik kepada menteri;

c. *Mendapatkan akses atau kesempatan untuk mengubah atau memperbarui data pribadinya tanpa mengganggu sistem pengelolaan data pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;*
d. *Mendapatkan akses atau kesempatan untuk memperoleh historis data pribadinya yang pernah diserahkan kepada penyelenggara sistem elektronik sepanjang masih sesuai dengan ketentuan peraturan perundang-undangan; dan*
e. *Meminta pemusnahan data perseorangan tertentu miiknya dalam sistem elektronik yang dikelola oleh penyelenggara sistem elektronik, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan".*[42]

Maka, melihat hak dari pemilik data pribadi, penyelenggara sistem elektronik berkewajiban untuk:

a. *"Melakukan sertifikasi sistem elektronik yang dikelolanya sesuai dengan ketentuan peraturan perundang-undangan;*
b. *Menjaga kebenaran, keabsahan, kerahasiaan, keakuratan dan relevansi serta kesesuaian dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan, dan pemusnahan data pribadi;*
c. *Memberitahukan secara tertulis kepada pemilik data pribadi jika terjadi kegagalan perlindungan rahasia data pribadi dalam sistem elektronik yang dikelolanya, dengan ketentuan pemberitahuan sebagai berikut:*
    1. *Harus disertai alasan atau penyebab terjadinya kegagalan perlindungan rahasia data pribadi;*
    2. *Dapat dilakukan secara elektronik jika pemilik data pribadi telah memberikan persetujuan untuk itu yang dinyatakan pada saat dilakukan perolehan dan pengumpulan data pribadinya;*
    3. *Harus dipastikan telah diterima oleh pemilik data pribadi jika kegagalan tersebut mengandung potensi kerugian bagi yang bersangkutan; dan*
    4. *Pemberitahuan tertulis dikirimkan kepada pemilik data pribadi paling lambat 14 (empat belas) hari sejak diketahui adanya kegagalan tersebut;*

[42] *Ibid.* Pasal 26.

5. *Memiliki aturan internal terkait perlindungan data pribadi yang sesuai dengan ketentuan peraturan perundang-undangan;*
6. *Menyediakan rekam jejak audit terhadap seluruh kegiatan penyelenggaraan sistem elektronik yang dikelolanya;*
7. *Memberikan opsi kepada pemilik data pribadi mengenai data pribadi yang dikelolanya dapat/atau tidak dapat digunakan dan/atau ditampilkan oleh/pada pihak ketiga atas persetujuan sepanjang masih terkait dengan tujuan perolehan dan pengumpulan data pribadi;*
8. *Memberikan akses atau kesempatan kepada pemilik data pribadi untuk mengubah atau memperbarui data pribadinya tanpa mengganggu sistem pengelolaan data pribadi, kecuali ditentukan lain oleh ketentuan peraturan perundang-undangan;*
9. *Memusnahkan data pribadi sesuai dengan ketentuan dalam peraturan menteri ii atau ketentuan peraturan perundang-undangan lainnya yang secara khusus mengatur di masing-masing instansi pengawas dan pengatur sektor untuk itu; dan*
10. *Menyediakan narahubung (contact person) yang mudah dihubungi oleh pemilik data pribadi terkait pengelolaan data pribadinya".*[43]

Upaya perlindungan data pribadi di dalam Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik hampir sama dengan Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik[44], yang membedakan hanya upaya perbaikan dan pembaruan yang terdapat dalam Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Dalam rangka melindungi data pribadi seseorang harus berlandaskan asas perlindungan data pribadi yang baik, meliputi:

a. *"Penghormatan terhadap data pribadi sebagai privasi;*
b. *Data pribadi bersifat rahasia sesuai persetujuan dan/atau berdasarkan ketentuan peraturan perundang-undangan;*

[43] *Ibid.* Pasal 28.
[44] *Ibid.* Pasal 2 ayat (1).

c. *Berdasarkan persetujuan;*
d. *Relevansi dengan tujuan perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, dan penyebarluasan;*
e. *Kelaikan sistem elektronik yang digunakan;*
f. *Iktikad baik untuk segera memberitahukan secara tertulis kepada pemilik data pribadi atas setiap kegagalan perlindungan data pribadi;*
g. *Ketersediaan aturan internal pengelolaan perlindungan data pribadi;*
h. *Tanggung jawab atas data pribadi yang berada dalam penguasaan pengguna;*
i. *Kemudahan akses dan koreksi terhadap data pribadi oleh pemilik data pribadi; dan*
j. *Keutuhan, akurasi, dan keabsahan serta kemutakhiran data pribadi".*[45]

Sesuai dengan ketentuan Pasal 2 ayat (2) huruf a, data pribadi merupakan bagian dari privasi, yang dalam hal ini privasi merupakan:

> *"Kebebasan pemilik data pribadi untuk menyatakan rahasia atau tidak menyatakan rahasia data pribadinya".*[46]

Sehingga, dalam pelaksanaannya penyelenggara sistem elektronik harus menghormati privasi subjek data pribadi dengan cara memverifikasi langsung kebenarannya ke subjek data pribadi lalu disimpan ke dalam sistem dalam bentuk data yang sudah terenkripsi[47].

Penyelenggara sistem elektronik wajib memiliki pusat pemulihan bencana (*disaster recovery center)* dan pusat data (*data center*). Pusat pemulihan bencana (*disaster recovery center*) adalah wadah *back-up* data, informasi dan sistem yang rusak baik karena ulah manusia maupun bencana alam. Sedangkan, pusat data (*data*

[45] Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi. Pasal 2 ayat (2).
[46] *Ibid*. Pasal 2 ayat (3).
[47] *Ibid.* Pasal 15.

center) adalah wadah penempatan sistem komponen dan elektronik baik untuk penyimpanan, penempatan mauun pengolahan data.[48]

Di dalam Pasal 36 ayat (1) Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik telah di atur mengenai sanksi administratif yang dikenakan jika pihak yang melakukan tindakan ilegal dengan data pribadi seseorang, yakni:

> *"Setiap orang yang memperoleh, mengumpulka, mengolah, menganalisis, menyimpan, menampilkan, mengumpulkan, mengirimkan, dan/atau menyebarluaskan data pribadi tanpa hak atau tidak sesuai dengan ketentuan dalam peraturan menteri ini atau peraturan perundang-undangan lainnya dikenai sanksi administratif sesuai dengan ketentuan peraturan perundang-undangan berupa:*
>
> *a. Peringatan lisan;*
> *b. Peringatan tertulis;*
> *c. Penghentian sementara kegiatan; dan/atau*
> *d. Pengumuman di situs dalam jaringan (website online)".*[49]

2.2.4. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Data pribadi merupakan data seseorang yang secara langsung maupun tidak langsung teridentifikasi atau yang dapat dikombinasikan dengan informasi lainnya melalui sistem elektronik atau nonelektronik.[50] Sedangkan, perlindungan data pribadi adalah upaya perlindungan dalam tahapan pengolahan data pribadi agar hak konstitusional setiap subjek terpenuhi.[51]

Di dalam Undang-Undang No, 27 Tahun 2022 tentang Perlindungan Data Pribadi, terdapat beberapa pihak yang terlibat dalam perlindungan data pribadi, antara lain:

---

[48] *Ibid.* Pasal 17.

[49] Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Pasal 36 ayat (1).

[50] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 1 angka (1).

[51] *Ibid*. Pasal 1 angka (2).

a. Subjek Data Pribadi, merupakan orang perseorangan yang memiliki data.[52]
b. Pengendali Data Pribadi, setiap pihak yang secara sendiri maupun bersama yang memegang kendali atas pemrosesan data pribadi;
c. Prosesor Data Pribadi, setiap pihak yang secara sendiri maupun bersama dalam memproses data atas nama pengendali data pribadi; dan
d. Korporasi merupakan badan hukum atau non-badan hukum yang berisikan orang-orang dan kekayaan yang terstruktur.[53]

Dalam penerapannya, Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi menerapkan asas-asas yang harus dipatuhi, seperti:

a. "Asas Perlindungan, berarti setiap tindakan pemrosesan data pribadi harus memberikan perlindungan terhadap subjek data pribadi guna menghindari penyalahgunaan data pribadi;
b. Asas Kepastian Hukum, berarti setiap tindakan pemrosesan data pribadi harus berlandaskan hukum agar mendapatkan pengakuan hukum baik di dalam maupun di luar pengadilan;
c. Asas Kepentingan Umum, dalam penegakkan perlindungan data pribadi harus mementingkan kepentingan umum baik dalam penyelenggaran Negara, pertahanan, dan keamanan nasional;
d. Asas Kemanfaatan yang dimaksud adalah dalam pengaturan perlindungan data pribadi harus memberikan manfaat terhadap kepentingan nasional;
e. Asas Kehati-hatian, berarti para pihak yang terlibat dalam pemrosesan dan pengawasan data pribadi harus mengupayakan agar tidak terjadi kerugian;
f. Asas Keseimbangan, dalam mengupayakan perlindungan data pribadi harus seimbang antara hak subjek data pribadi dengan hak Negara;

[52] *Ibid.* Pasal 1 angka (6).
[53] *Ibid.* Pasal 1 angka (4), (5), (6), dan (8).

g. *Asas Pertanggungjawaban yang dimaksud adalah pihak yang bertanggung jawab dalam pemrosesan dan pengawasan data pribadi atas tindakannya agar tidak merugikan hak subjek data pribadi; dan*
h. *Asas Kerahasiaan yang dimaksud adalah data pribadi harus terlindungi dari pihak-pihak yang berniat untuk melakukan tindakan penyalahgunaan data pribadi".*[54]

Pengendali data pribadi dalam melakukan pengumpulan data pribadi milik subjek data pribadi berkewajiban memastikan keamanan dan perlindungan data pribadi dengan cara:

1. *"Menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan peraturan perundang-undangan; dan*
2. *Menentukan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi."*[55]

Di dalam Pasal 4, dalam pemrosesan data pribadi perlu diketahui bahwa data pribadi dikelompokkan menjadi data pribadi yang bersifat spesifik dan bersifat umum. Data pribadi spesifik yang dimaksud antara lain:

1. *"Data dan informasi kesehatan;*
2. *Data biometric;*
3. *Data genetika;*
4. *Catatan kejahatan;*
5. *Data anak;*
6. *Data keuangan pribadi; dan/atau*
7. *Data lainnya sesuai dengan ketentuan peraturan perundang-undangan."*[56]

Sedangkan yang di maksud dengan data pribadi umum adalah:

1. *"Nama lengkap;*
2. *Jenis kelamin;*

[54] Penjelasan Umum Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 3.
[55] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 35.
[56] *Ibid.* Pasal 4 ayat (2).

3. *Kewarganegaraan;*
4. *Agama;*
5. *Status perkawinan; dan/atau*
6. *Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang."*[57]

Setiap subjek data pribadi memiliki hak atas data pribadinya yang secara tersirat di atur dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, yaitu:

1. *"Melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi tentang dirinya sesuai dengan ujuan pemrosesan data pribadi;*[58]
2. *Mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan;*[59]
3. *Menunda atau membatasi pemrosesan data pribadi secara proporsional sesuai dengan tujuan pemrosesan data pribadi;*[60] *dan*
4. *Menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan."*[61]

Selain itu, pengendali data pribadi juga berkewajiban untuk mencegah data pribadi digunakan secara ilegal. Jika data pribadi gagal dilindungi, pengendali data pribadi harus bertanggung jawab atas kelalaiannya dengan cara menyampaikan pemberitahuan tertulis ke subjek data pribadi dan Lembaga dengan menyertakan bagaimana kronologi kebocoran data pribadi dan bagaimana penanganan serta pemulihan datanya paling lambat 72 (tujuh puluh dua) jam.[62]

[57] *Ibid.* Pasal 4 ayat (3).
[58] *Ibid.* Pasal 6.
[59] *Op cit.* Pasal 8.
[60] *Ibid.* Pasal 11.
[61] *Ibid.* Pasal 12 ayat (1).
[62] *Ibid*. Pasal 46 ayat (1) dan (2).