BAB IV

PEMBAHASAN

4.1. Upaya *E-commerce* Menjalankan Kewajibannya dalam Hal Memenuhi Hak Pengguna dalam Melindungi Data Pribadinya

Dalam menjalankan kegiatan usahanya, *e-commerce* memanfaatkan *platform online marketplace* sebagai tempat kegiatan usahanya meliputi pengumpulan data pribadi[63] pengguna yang selanjutnya disebut sebagai Penyelenggara Sistem 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*".[64]

Sesuai dengan ketentuan yang di atur dalam Pasal 2 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, penyeleggaraan sistem elektronik terbagi ke dalam 2 (dua) lingkup, yaitu lingkup publik dan lingkup privat."

1. *"Penyelenggara Sistem Elektronik Lingkup Publik merupakan penyelenggara sistem elektronik yang dilakukan oleh instansi penyelenggara negara[65] atau institusi yang ditunjuk oleh instansi penyelenggara negara.[66]*
2. *Penyelenggara Sistem Elektronik Lingkup Privat merupakan penyelenggaraan sistem elektronik oleh orang[67], badan usaha[68], dan masyarakat".[69]*

---

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

[64] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 1 angka (4).

[65] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 1 angka (7). Kementerian atau Lembaga adalah instansi yang mengawasi dan mengeluarkan pengaturan.

[66] *Ibid.* Pasal 1 angka (5).

[67] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 1 angka 36, Orang adalah orang perseorangan dan badan hukum.

[68] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 1 angka 37, Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan yang berbadan hukum maupun non-badan hukum.

[69] *Ibid.* Pasal 1 angka (6).

4.1.1. Kewajiban E-Commerce

Marketplace sebagai pengendali data pribadi, memiliki kewajiban untuk melakukan pemrosesan data pribadi dengan spesifik, transparan dan sah di mata hukum. Pemrosesan data pribadi diatur dalam Pasal 16 ayat (1) dilakukan dengan cara:

1. *"Pemerolehan dan pengumpulan;*
2. *Pengolahan dan penganalisisan;*
3. *Penyimpanan;*
4. *Perbaikan dan pembaruan;*
5. *Penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan/atau*
6. *Penghapusan atau pemusnahan".*[70]

Sebagai penyelenggara sistem elektronik, *e-commerce* berkewajiban untuk menyelenggaraan sistem elektronik secara andal[71], aman[72] dan bertanggung jawab[73] terhadap beroperasinya sistem elektronik. Selain itu, penyelenggara sistem elektronik juga berkewajiban untuk menjamin bahwa sistem elektroniknya tidak memfasilitasi penyebarluasan informasi atau dokumen elektronik yang dilarang ketentuan peraturan perundang-undangan[74] dan merujuk pada Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, terdapat kewajiban-kewajiban yang harus dilakukan oleh penyelenggara system elektronik yang menurut penulis berkaitan dengan kewajiban *e-commerce,* sebagai berikut:

1. *"Dapat menampilkan kembali informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan peraturan perundang-undangan;*

---

[70] *Op cit.* Pasal 16 ayat (1).

[71] Yang dimaksud dengan andal adalah kemampuan system elektronik sesuai dengan kebutuhan penggunaannya.

[72] Yang dimaksud dengan aman adalah system elektronik terlindungi secara fisik dan nonfisik.

[73] Yang dimaksud dengan bertanggung jawab adalah penyelenggara system elektronik bertanggung jawab secara hukum terhadap penyelenggaraan system elektronik.

[74] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 5 ayat (2).

2. *Dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan informasi elektronik dalam penyelenggaraan sistem elektronik;*
3. *Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik;*
4. *Dilengkap dengan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan penyelenggaraan sistem elektronik tersebut; dan*
5. *Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk*[75]*;*
6. ***Memastikan system elektroniknya tidak memfasilitasi penyebarluasan informasi elektronik*** *dan/atau dokumen elektronik yang dilarang sesuai dengan ketentuan perundang-undangan*[76]*;*
7. ***Melaksanakan prinsip perlindungan data pribadi***[77]*;*
8. *Menghapus informasi elektronik dan/atau dokumen elektronik yang tidak relevan*[78] *yang berada di bawah kendalinya atas permintaan orang yang bersangkutan*[79]*;*
9. ***Melakukan pengamanan terhadap komponen system elektronik***[80]*;*
10. *Menjaga kerahasiaan, keutuhan, keautentikan, keteraksesan, ketersediaan, dan dapat ditelusurinya suatu informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan*[81]*; dan*
11. ***Melindugi pengguna dan masyarakat luas dari kerugian yang ditimbulan oleh system elektronik yang diselenggarakannya****".*[82]

Selain itu, dalam melakukan pemrosesan data pribadi *marketplace* yang berkedudukan sebagai pengendali data pribadi berkewajiban untuk:

1. *"Melindungi dan memastikan keamanan data pribadi yang diprosesnya dengan cara:*
   a. *Menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari*

[75] *Ibid.* Pasal 4.
[76] *Op cit.* Pasal 5 ayat (2).
[77] *Op cit.* Pasal 14.
[78] Yang dimaksud dengan tidak relevan adalah penghapusan (*right to erasure*) dan pengeluaran dari daftar mesin pencari (*right to delisting*).
[79] *Ibid.* Pasal 15.
[80] *Op cit.* Pasal 23 .
[81] *Op cit.* Pasal 26.
[82] *Op cit.* Pasal 31.

gangguan pemrosesan data pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan

b. *Menentukan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi;*[83]

2. *Menjaga kerahasiaan data pribadi;*[84]
3. *Mengawasi setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi;*[85]
4. *Melindungi data pribadi dari pemrosesan yang tidak sah;*[86] *dan*
5. *Mencegah data pribadi diakses secara tidak sah dengan menggunakan system elektronik yang andal, aman, dan bertanggung jawab".*[87]

Merujuk pada Pasal 29 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, kewajiban dasar *e-commerce* sebagai penyelenggara system elektronik harus menyampaikan informasi ke pengguna nya untuk melindungi kepentingan pengguna seminimal mungkin mengenai:

1. *"Identitas penyelenggara system elektronik;*
2. *Objek yang ditransaksikan;*
3. *Kelaikan atau kemanan system elektronik;*
4. *Tata cara penggunaan perangkat;*
5. *Syarat kontrak;*
6. *Prosedur mencapai kesepakatan;*
7. ***Jaminan privasi dan/atau perlindungan data pribadi**; dan*
8. *Nomor telepon pusat pengaduan".*[88]

4.1.2. Kesepakatan *E-Commerce*

Setelah *e-commerce* menyampaikan informasi dasar mengenai kewajibannya sebagai penyelenggara, kesepakatan dan tanggung jawab antara penyelenggara dengan pengguna mengenai kontrak elektronik tersebut dijadikan sebagai dasar dari dilakukannya transaksi elektronik.

[83] Pasal 35.
[84] Pasal 36.
[85] Pasal 37.
[86] Pasal 38.
[87] Pasal 39.
[88] *Op cit.* Pasal 29.

Sehingga terhitung dari pengguna menyetujui kontrak elektronik yang disediakan *e-commerce* seperti syarat dan ketentuan (*terms and conditions*) merupakan tanggung jawab kedua belah pihak sesuai dengan peraturan perundang-undangan yang berlaku. Dengan disepakatinya *terms and conditions*, transaksi elektronik dapat dilaksanakan jika sudah sesuai dengan ketentuan dalam Pasal 1320 KUHPerdata *jo.* Pasal 46 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dimana perjanjian sah ketika:

1. *"Terdapat kesepakatan para pihak;*
2. *Dilakukan oleh subjek hukum yang cakap atau yang berwenang sesuai dengan ketentuan peraturan perundang-undangan;*
3. *Terdapat hal tertentu; dan*
4. *Objek transaksi tidak boleh bertentangan dengan peraturan perundang-undangan, kesusilaan, dan ketertiban umum".*[89]

Kegiatan usaha yang saat ini mengandalkan *online marketplace* sebagai *platform* yang menyediakan tempat untuk para penjual dengan produknya yang akan dijual ke pembeli tentunya membutuhkan kesepakatan dan perjanjian antara pengguna dan *marketplace* yang menyediakan *platform* tersebut sesuai dengan ketentuan yang di atur dalam Pasal 1313 Kitab Undang-Undang Hukum Perdata, bahwa:

> "*Suatu persetujuan adalah suatu perbuatan dimana satu orang atau lebih mengikatkan diri terhadap satu orang lain atau lebih*".[90]

Pengguna yang sudah terdaftar dan memiliki akun di *marketplace* dianggap telah menyetujui *terms and conditions* yang diatur masing-masing *marketplace. Marketplace* sebagai penyedia layanan sudah seharusnya menyimpan berbagai informasi rahasia atau data pribadi milik pengguna sebagai bentuk upaya perlindungan. Ketika terjadi kebocoran data pribadi, tentunya meresahkan pemilik data pribadi karena dapat dikatakan data pribadi adalah aset yang memiliki

[89] Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik. Pasal 46 ayat (2).
[90] Kitab Undang-Undang Hukum Perdata. Pasal 1313.

nilai untuk kegiatan bisnis yang berkaitan dengan pengguna internet untuk dijadikan preferensi *e-commerce*. Maka, *marketplace* sudah seharusnya memiliki sistem keamanan yang kuat dan alternative pencegahan guna menghindari kebocoran data pribadi, seperti yang diatur dalam Pasal 1366 Kitab Undang-Undang Hukum Perdata:

> *"Setiap orang bertanggung jawab, bukan hanya atas kerugian yang disebabkan perbuatan-perbuatan, melainkan juga atas kerugian yang disebabkan kelalaian atau kesembronoannya".*[91]

Marketplace sebagai penyelenggara sistem elektronik berkewajiban untuk melindungi data pribadi pengguna sesuai dengan Pasal 26 ayat (1) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

> *"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".*[92]

Persetujuan yang di maksud dalam Pasal 26 ayat (1) di atas bukan hanya sekedar menyetujui, namun harus ada kesadaran untuk menyetujui penggunaan dan pemanfaatan data pribadi apakah sesuai atau tidak dengan kepentingan yang diberitahukan saat perolehan data. Dalam hal ini, penggunaan setiap informasi pribadi seseorang termasuk ke dalam hak pribadi (*privacy rights*) seseorang, meliputi:

1. *"Hak untuk menikmati kehidupan pribadi dan bebas dari segala macam gangguan;*
2. *Hak untuk dapat berkomunikasi dengan orang lain tanpa tindakan memata-matai; dan*
3. *Hak untuk mengawasi akses informasi tentang kehidupan pribadi dan data seseorang".*[93]

Namun, jika pengguna merasa hak yang dimiliki di langar oleh penyelenggara sistem elektronik, maka sesuai dengan ketentuan

---

[91] Kitab Undang-Undang Hukum Perdata. Pasal 1366.

[92] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 26 ayat (1).

[93] *Ibid.* Penjelasan Umum Pasal 26 ayat (1).

dalam Pasal 26 ayat (2) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, bahwa:

> "*Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan undang-undang ini".*[94]

Di dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik juga mengenal prinsip pertanggungjawaban (*presumed liability)* di mana prinsip ini merupakan prinsip pertanggungjawaban secara hukum. Prinsip *presumed liability* dapat di lihat di dalam Pasal 15 yang menyatakan bahwa:

1. *"Setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya;*
2. *Penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektroniknya; dan*
3. *Ketentuan sebagaimana di maksud pada ayat (2) tidak berlaku dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak pengguna sistem elektronik".*[95]

Seperti yang dijelaskan dalam penjelasan Pasal 15 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang di maksud dengan andal adalah ketika kemampuan sistem elektronik sesuai dengan kebutuhan penggunaannya, aman dalam melindungi fisik dan nonfisik sistem elektronik, dan adanya pihak yang bertanggung jawab dalam penyelenggaraan sistem. Maka, apabila terjadi kesalahan dalam sistem elektronik, penyelenggara system elektronik harus membuat pengumuman tertulis kepada pengguna nya. Dan, jika benar terjadi kebocoran data pribadi sebagaimana yang di maksud dalam Pasal 26 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, para pengguna dapat mengajukan

[94] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 26 ayat (2).

[95] Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Pasal 15.

ganti rugi selama memenuhi unsur-unsur yang telah di atur dalam Pasal 1365 KUHPerdata, yaitu:

1. *"Adanya perbuatan;*
2. *Adanya unsur kesalahan;*
3. *Adanya kerugian; dan*
4. *Adanya hubungan sebab akibat antara kesalahan dan kerugian".*[96]

Bentuk pengimplementasian peraturan yang berlaku saat ini, penulis menggunakan *terms and conditions* salah satu *e-commerce* di Indonesia yaitu PT Tokopedia. Di dalam *terms and conditions* PT Tokopedia yang penulis kutip, diatur mengenai:

> "*Pengguna*[97] *dalam hal ini, Mitra Tokopedia*[98] *tunduk pada Kebijakan Privasi dan Syarat dan Ketentuan yang tertulis di bawah ini".*[99]
>
> *"Dengan mendaftar dan/atau menggunakan Mitra Tokopedia, maka Pengguna dianggap telah membaca, mengerti, memahami dan menyetujui semua isi dalam Syarat dan Ketentuan ini".*[100]
>
> *"Dengan menggunakan fitur Veifikasi Pengguna, maka Pengguna dianggap telah menyetujui dan mematuhi Syarat dan Ketentuan ini, Ketentuan Situs, dan Kebijakan Privasi".*[101]

Sebagaimana yang diatur dalam Pasal 1320 KUHPerdata, terdapat 4 (empat) syarat sahnya suatu perjanjian, salah satunya adalah kecakapan para pihak untuk mengikatkan diri dalam suatu perjanjian. Di dalam poin B.2 syarat dan ketentuan Mitra Tokopedia disebutkan bahwa:

---

[96] Kitab Undang-Undang Hukum Perdata. Pasal 1365.

[97] Yang dimaksud dengan Pengguna adalah pihak yang menggunakan layanan Tokopedia.

[98] Yang dimaksud dengan Mitra Tokopedia adalah Pengguna yang telah mendaftarkan diri melalui Situs/Aplikasi untuk membeli Barang Digital maupun barang Fisik dari *Partner* melalui Situs/Aplikasi dan menjualnya Kembali secara *offline.*

[99] PT Tokopedia, "*Syarat dan Ketentuan Mitra Tokopedia",* diakses Mei 23 2023. https://www.tokopedia.com/help/article/syarat-dan-ketentuan-mitra-tokopedia.

[100] *Ibid.*

[101] Tokopedia Care, "*Syarat dan Ketentuan Verifikasi Pengguna*", diakses Mei 29 2023. https://www.tokopedia.com/help/article/syarat-dan-ketentuan-verifikasi-pengguna.

> "*Mitra Tokopedia dengan ini menyatakan bahwa Mitra Tokopedia adalah orang yang cakap dan mampu untuk mengikatkan dirinya dalam sebuah perjanjian yang sah dan menurut hukum".*[102]

Sebagaimana syarat dan ketentuan yang disebutkan dalam poin B.2 tersebut, hanya orang yang cakap hukum yang dapat mengikatkan diri ke dalam perjanjian, sehigga maka dapat dikatakan seluruh pengguna Tokopedia harus cakap hukum sebelum memutuskan untuk mendaftarkan diri sebagai Pengguna Tokopedia.

Mitra Tokopedia sebagai Pengguna yang telah mendaftarkan diri dan menyerahkan informasi pribadi nya kepada Tokopedia setuju dan Tokopedia berwenang untuk mengolah informasi yang didaftarkan Pengguna sebagaimana yang diatur dalam poin B.1 Syarat dan Ketentuan Mitra Tokopedia sebagai berikut:

> "*Mitra Tokopedia hanya dapat digunakan oleh Pengguna yang telah mendaftarkan diri, menyetujui Syarat dan Ketentuan ini serta yang sudah diverifikasi sesuai kebijakan dari Tokopedia".*[103]

Poin C.5 Syarat dan Ketentuan Verifikasi Pengguna:

> *"Pengguna menyetujui dan memberikan hak dan wewenang kepada Tokopedia untuk menggunakan, mengungkapkan, dan/atau mengolah Informasi Pengguna yang diberikan oleh Pengguna unuk kepentingan pelaksanaan Verifikasi Pengguna, termasuk melakukan komparasi atau pencocokan dengan informasi atau data lain yang dimiliki oleh Tokopedia atau Partner yang bekerjasama dengan Tokopedia, dan menyimpan informasi tersebut dalam Situs/Aplikasi".*[104]

Maka dari itu menindaklanjuti poin B.1 Syarat dan Ketentuan Mitra Tokopedia dan poin C.5 Syarat dan Ketentuan Verifikasi Pengguna, Tokopedia mengatur poin D.1 berupa:

---

[102]Tokopedia Care, "*Syarat dan Ketentuan Mitra Tokopedia*", diakses Mei 29 2023. https://www.tokopedia.com/help/article/syarat-dan-ketentuan-mitra-tokopedia.

[103] *Ibid.*

[104] Tokopedia Care, "*Syarat dan Ketentuan Verifikasi Pengguna*", diakses Mei 29 2023. https://www.tokopedia.com/help/article/syarat-dan-ketentuan-verifikasi-pengguna.

> *"Tokopedia tanpa pemberitahuan terlebih dahulu kepada Mitra Tokopedia, memiliki kewenangan untuk melakukan Tindakan yang perlu atas setiap dugaan pelanggaran atau pelanggaran Syarat dan Ketentuan ini dan/atau hukum yang berlaku, yakni Tindakan berupa suspense akun, dan/atau penghapusan akun Mitra Tokopedia".*[105]

Jika melihat dari poin D.1 Syarat dan Ketentuan Mitra Tokopedia, Tokopedia sebagai Pengendali Data Pribadi, sudah seharusnya menjalankan kewajibannya dalam melindungi informasi pribadi milik Pengguna seperti yang di atur dalam Pasal 39 Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik."

> *"Selain itu, PT Tokopedia sebagai Pengendali Data Pribadi mengatur secara khusus mengenai kebijakan perlindungan data pribadi pengguna dengan membatasi akses data pribadi yang ditampilkan dalam pemrosesan pemesanan".*[106]

Dalam rangka menjaga keamanan dan kerahasiaan informasi, terdapat peraturan yang mengatur mengenai minimun standar perlindungan dari peretasan di atur dalam Pasal 7 Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi yang mengatur bahwa:

1. *"Penyelenggaran Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis harus menerapkan standar SNI*[107] *ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya;*
2. *Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik tinggi harus menerapkan standar SNI ISO/IEC 27001;*
3. *Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik rendah harus menerapkan pedoman Indeks Keamanan Informasi; dan*

---

[105] PT Tokopedia, "*Syarat dan Ketentuan Mitra Tokopedia",* diakses Mei 23 2023. https://www.tokopedia.com/help/article/syarat-dan-ketentuan-mitra-tokopedia.

[106] Tokopedia Pusat Edukasi Seller, "*[Pesanan] Penerapan Kebijakan Perlindungan Data Pribadi Pembeli",* diakses Mei 29 2023. https://seller.tokopedia.com/edu/kebijakan-data-pembeli/.

[107] SNI adalah dokumen berisi ketentuan teknik, persyaratan, dan karakteristik suatu kegiatan atau hasil kegiatan yang ditetapkan oleh Badan Standarisasi Nasional.

4. *Ketentuan mengenai pedoman Indeks Keamanan Informasi sebagaima dimaksud pada ayat (3) diatur dalam Peraturan Menteri".*[108]

Yang dimaksud *International Organization for Standardization* (ISO) dalam ayat (1) adalah organisasi internasional independent yang bertujuan untuk mengembangkan standar internasional di berbagai bidang terlebih dalam lingkungan bisnis. Karena dilihat dari kondisi saat ini, sertifikasi ISO dijadikan sebagai *seal of approval* di mana suatu organisasi telah memenuhi standar yang ditetapkan oleh ISO di berbagai bidang seperti manajemen kualitas, manajemen lingkungan, dan keamanan informasi[109] Perlu diketahui bahwa terdapat beberapa jenis standar ISO yang paling umum di ambil oleh beberapa perusahaan baik di bidang *quality management* hingga IT *Security,* seperti ISO 9001, ISO 14001, ISO 27001, ISO 45001, dan ISO 20000.

Di Indonesia sendiri, merujuk pada Pasal 7 ayat (2) Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 bahwa PSE harus menyelenggarakan system elektronik tinggi dengan menetapkan ISO/IEC 27001. Yang dimaksud dengan ISO 27001 adalah standar internasional untuk keamanan informasi yang bertujuan untuk membantu organisasi dalam melindungi data sensitif dan meminimalkan resiko keamanan[110]. Dilansir dari *The British Standards Institution* (BSI)[111], PT Tokopedia dalam menjalankan kegiatan usahanya telah memiliki sertifikasi yang diminta dalam Pasal 7 Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, yaitu ISO/IEC 27001:2013 dan ISO/IEC 27701:2019[112].

---

[108] Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Pasal 7.

[109] Aulia Reta Faulina, "*Apa itu ISO: Pengertian, Manfaat, Jenis, dan Badan Sertifikasinya*", 21 Mei 2023, https://solarindustri.com/blog/iso-adalah/.

[110] *Ibid.*

[111] BSI adalah organisasi standarisasi tertua di dunia dalam forum pengembangan standar internasional.

[112] *The British Standards Institution* (BSI), diakses Juni 14 2023, https://www.bsigroup.com/en-GB/validate-bsi-issued-certificates/client-directory-profile/PT_TOK-0047786234-000."

PT Tokopedia telah mendapatkan sertifikasi ISO/IEC 27001:2013 sejak 10 Februari 2021 dan akan berakhir pada 9 Februari 2024 dengan nomor sertifikasi IS 736149 dengan ruang lingkup yang bergerak di bidang system manajemen keamanan informasi dalam operasi TI dalam layanan pembayaran, pintek, logistic, layanan pelanggan, barang digital, akun, *platform* pengguna, iklan teratas dan ritel baru[113]. Selain itu, PT Tokopedia juga mendapatkan sertifikasi ISO/IEC 27701:2019 sejak 23 Desember 2021 dan akan berakhir pada 9 Februari 2024 dengan nomor sertifikasi PM 759908 dengan ruang lingkup yang bergerak di bidang system manajemen informasi privasi sebagai prosesor PII oleh operasi TI dalam layanan pembayaran, pintek, logistic, layanan, pelanggan, barang digital, akun, *platform* pengguna, iklan teratas dan ritel baru[114].

Selain mendapatkan sertifikasi ISO, dalam hal melindungi data pengguna Tokopedia dari pihak yang tidak berwenang, PT Tokopedia menerapkan system keamanannya dengan metode enkripsi. Data-data yang terenkripsi meliputi *e-mail*, alamat lengkap dan nomor telepon, sehingga hanya pihak-pihak terkait dan berwenang saja yang dapat mengakses data-data yang terenkripsi tersebut[115]. Metode enkripsi yang digunakan adalah *asymmetric key encryption* yang dinamakan "RSA *Encryption"* dengan menggunakan sepasang kunci meliputi kunci publik dan kunci pribadi. Bentuk implementasi dari RSA *Encryption* dengan cara Tokopedia (Pihak Pertama) akan mengenkripsi data menggunakan kunci public pihak kedua, kemudian Pengguna (Pihak Kedua) harus mendekripsikan pesan yang terenkripsi menggunakan kunci pribadi mereka. Walaupun data yang sudah terenkripsi merupakan data yang sama, pesan yang akan muncul akan selalu berbeda dan unik.[116]Selain melakukan enkripsi data, PT Tokopedia juga

[113] *Ibid.*
[114] *Ibid.*
[115] Tokopedia API, "*Encryption*", https://developer.tokopedia.com/openapi/guide/guides/encryption/, diakses 16 Juni 2023.
[116] *Ibid.*

menghimbau para penggunanya untuk menghindari penipuan dan kebocoran data dari pihak yang tidak bertanggung jawab, dengan cara: merahasiakan kode OTP atau PIN, merahasiakan data pribadi, mengganti *password* akun secara berkala, dan memastikan situs resmi Tokopedia.[117]

4.2. Bentuk Tanggung Jawab *E-commerce* atas Kebocoran Data Pribadi Pengguna Ditinjau dari Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

Jika dalam melaksanakan tugasnya, *marketplace* gagal dalam melindungi data pribadi pengguna, maka *marketplace* sebagai pengendali data pribadi bertanggung jawab atas data pribadi para pengguna nya sebagaimana yang di atur dalam Pasal 47 bahwa:

> "*Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menujukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Perlindungan Data Pribadi".*[118]

Jika gagal, maka pengendali data pribadi harus membuat harus bertanggung jawab atas kelalaiannya dengan cara menyampaikan pemberitahuan tertulis ke subjek data pribadi dan Lembaga serta memberitahukan ke masyarakat mengenai kegagalan perlindungan data pribadi dengan menyertakan bagaimana kronologi kebocoran data pribadi dan bagaimana penanganan serta pemulihan datanya paling lambat tujuh puluh dua jam.[119]

Sebagai contoh bentuk pengimplementasian Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, penulis yang pada sebelumnya telah mengangkat PT Tokopedia sebagai contoh kasus, penulis akan memberikan analisa hukum mengenai kebocoran data pengguna Tokopedia. Pada 20 Maret 2020, terjadi peretasan sembilan puluh satu juta akun pengguna dan tujuh juta akun pedagang Tokopedia meliputi *username*, alamat *e-mail*, nama lengkap, tanggal lahir, jenis kelamin, nomor telepon, dan kata sandi yang di jual oleh

---

[117] Tokopedia Care, "*Jaga Keamanan Akun Tokopedia*", diakses Juni 16 2023. https://www.tokopedia.com/help/article/t-0054-jaga-keamanan-akun-tokopedia.

[118] Pasal 47.

[119] Pasal 46.

Whysodank (peretas) di *darkweb* "*Empire Market*" sebesar tujuh puluh empat juta rupiah. Pada hari Sabtu, 2 Mei 2020, diketahuinya peretasan data pribadi Tokopedia ketika peretas mempublikasikan hasil peretasan yang dilakukannya pada 20 Maret 2020 di "*Raid Forum".* Kemudian pada sore harinya 2 Mei 2020 tepatnya pukul 16.15 WIB, ketika layanan pencegahan dan pengawasan kebocoran data dari Israel yang diakui oleh @underthebreach membuat cuitan mengenai peretasan dan menyebutkan akun resmi Tokopedia. Akun tersebut juga menyebutkan bahwa saat itu peretas masih memecahkan *hash password* dan meminta bantuan peretas lainnya untuk membuka *hash* tersebut. *Hash password* adalah algoritma *one-way hasing* atau pengenkripsian satu arah, maka jika kata sandi sudah dienkripsi tidak akan bisa di dekripsi lagi, sedangkan *hash* merupakan proses enkripsi password.[120] Kemudian, akun tersebut juga membuat ciutan bahwa seseorang telah membocorkan 15 (lima belas) juta data pengguna perusahaan teknologi besar asal Indonesia yang menjalankan *e-commerce* "Tokopedia" pada Maret 2020 berikut dengan nama lengkap, *e-mail,* dan nomor telepon pengguna. Pada hari Sabtu, 2 Mei 2020 tepatnya pukul 21.00 WIB, *Vice Preident of Corporate Communications* Tokopedia, Nuraini Razak menanggapi cuitan tersebut dengan mengakui adanya upaya pencurian data terhadap pengguna, namun Tokopedia memastikan kata sandi para pengguna berhasil terlindungi.

Namun, keesokan harinya pada hari Minggu, 3 Mei 2020, peretas dengan *username* "ShinyHunters" membuat pengumumam bahwa ia telah menjual 91 (sembilan puluh satu) juta pengguna Tokopedia di *darkweb* "*Empire Market*" sebesar US$ 5.000 atau setara dengan Rp 74.000.000,- (tujuh puluh empat juta) rupiah di mana sebelumnya akun @underthebreach menyebutkan hanya 15 (lima belas) juta data pengguna yang teretas. Atas cuitan peretas tersebut, Nuraini Razak langsung melakukan pemeriksaan dan menyatakan tidak ada kebocoran data metode pembayaran pengguna.

---

[120] Asih, Dini Nur "*Pakar Bahas Hash-Salt Password untuk Kecoh Peretas Tokopedia*" diakses Februari 16 2023, https://www.cnnindonesia.com/teknologi/20200504084443-185-499681/pakar-bahas-hash-salt-password-untuk-kecoh-peretas tokopedia#:~:text=Hash%20password%20merupakan%20algoritma%20one,hash%20maka%20akan%20menjadi%20kerkw23.

Menanggapi kasus peretasan Tokopedia yang terjadi, Ketua Lembaga Riset Keamanan Siber dan Komunikasi Indonesia *Communication & Information System Security Research Center* (CISSReC), Dr. Pratama Persadha[121], peretas menyebarluaskan 15 (lima belas) juta akun untuk mengajak peretas lainnya untuk mencari siapa yang berhasil membuka *hash password* nya dan apabila *hash* sudah berhasil terbuka, sudah dapat dipastikan peretas akan mengambilalih akun-akun media sosial yang menggunakan *e-mail* yang sama di Tokopedia, karena biasanya pengguna menggunakan satu *e-mail* untuk macam-macam *platform.* Maka dari itu, Dr. Pratama Prasadha meminta Tokopedia untuk bertanggungjawab atas peretasan yang terjadi dan menyadarkan para pengguna atas peretasan data yang terjadi dengan cara melakukan sosialisasi dengan segala sarana media mengenai tindakan apa saja yang harus dilakukan oleh para pengguna seperti mengganti kata sandinya dan mengaktifkan *One Time Password* (OTP) lewat SMS guna mencegah terjadinya peretasan di *platform* lain yang menggunakan *e-mail* yang sama.[122]

Imbas atas bocornya data pengguna Tokopedia berujung memasuki ranah hukum dengan gugatan yang dilayangkan oleh Komunitas Konsumen Indonesia (KKI) selaku Penggugat terhadap Menteri Komunikasi dan Informatika, (Tergugat I) dan PT Tokopedia (Tergugat II) melalui gugatan yang didaftarkan di *e-court* Pengadilan Negeri Jakarta Pusat pada 6 Mei 2020 dengan nomor pendaftaran gugatan PN JKT.PST-0520201XD dan terdaftar dengan nomor perkara 235/Pdt.G/2020/PN.JKT.PST pada 8 Mei 2020. Dasar Penggugat melayangkan gugatan terhadap Para Tergugat adalah kelalaian Tokopedia dalam menyimpan dan melindungi data pribadi serta hak privasi pengguna aplikasi Tokopedia dan kelalaian Menkominfo dalam menjalankan pengawasan penyelenggaraan sistem elektronik Tokopedia sehingga pihak ketiga dapat menguasai data pribadi pengguna. Dalam gugatannya, Penggugat meminta Tergugat I untuk mencabut tanda daftar penyelenggara sistem elektronik

[121] Kusbiantoro Didik, "*Pakar: Kasus peretasan Tokopedia bisa menjalar ke akun medsos*" diakses Februari 16 2023, https://jatim.antaranews.com/berita/376965/pakar-kasus-peretasan-tokopedia-bisa-menjalar-ke-akun-medsos.

[122] Wicaksono Adhi, "*Kronologi Lengkap 91 Juta Akun Tokopedia Bocor dan Dijua*l" diakses Februari 16 2023, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

Tergugat II dan meminta Tergugat II untuk membayar denda administratif sebesar Rp 100.000.000.000,- (seratus miliar rupiah).[123] Setelah melalui proses persidangan selama 5 (lima) bulan, gugatan dimenangkan oleh Para Tergugat dengan pertimbangan Majelis Hakim sebagai berikut:

> *"Menimbang, bahwa Penggugat jelas-jelas menuntut agar Tergugat I menerbitkan Keputusan Tata Usaha Negara yang mengikat dan bersifat final terhadap Tergugat I hal tersebut merupakan tindakan yang dilakukan oleh Tergugat I, berdasarkan pertimbangan tersebut seharusnya Penggugat mengajukan gugatan kepada Pengadilan Tata Usaha Negara dan bukan kepada Pengadilan Negeri".*[124]

Berdasarkan pertimbangan Majelis Hakim tersebut di mana Penggugat menuntut Tergugat I untuk menerbitkan Keputusan Tata Usaha Negara, pada akhirnya gugatan tersebut dimenangkan oleh Para Tergugat karena atas gugatan tersebut seharusnya KKI mengajukan gugatan ke Pengadilan Tata Usaha Negara bukan ke Pengadilan Negeri karena Pengadilan Negeri tidak memiliki kewenangan absolut[125] untuk menangani perkara tersebut sebagaimana yang di atur dalam Pasal 134 H.I.R dikatakan bahwa:

> *"Jika perselisihan itu suatu perkara yang tidak masuk kekuasaan pengadilan negeri, maka pada setiap waktu dalam pemeriksaan perkara itu, dapat diminta supaya hakim menyatakan dirinya tidak berkuasa dan hakim pun wajib pula mengakuinya karena jabatannya".*[126]

Sebagai bentuk pengimplementasian Pasal 46 mengenai pemberitahuan tertulis ke subjek data pribadi dan Lembaga, di mana PT Tokopedia menindaklanjuti kejadian tersebut dengan memberikan pemberitahuan tertulis melalui *e-mail* yang dikirimkan langsung oleh CEO PT Tokopedia pada 12 Mei 2020 yang berisikan sebagai berikut:

"*Kepada semua pengguna Tokopedia yang saya hormati,*

---

[123] Widyastuti, Rr. Ariyani Yakti, "*Data Pengguna Dibobol, KKI Gugat Tokopedia dan Menkominfo*", diakses Februari 16 2023, https://bisnis.tempo.co/read/1339802/data-pengguna-dibobol-kki-gugat-tokopedia-dan-menkominfo.

[124] Putusan Nomor 235/Pdt.G/2020/PN.Jkt.Pst. Komunitas Konsumen Indonesia melawan Menteri Komunikasi dan Informatika Republik Indonesia dan PT Tokopedia.

[125] Kewenangan absolut merupakan penyangkalan mengenai wewenang yang berhubngan dengan sifat perkaranya.

[126] *Herzien Inlandsch Reglement (H.I.R) Reglemen Indonesia yang Diperbaharui (R.I.B)*. Pasal 134.

Bisnis Tokopedia adalah bisnis kepercayaan. Sebagai perusahaan teknologi dengan platform marketplace terbesar di Indonesia, Tokopedia telah dipercaya oleh lebih dari 90 juta masyarakat Indonesia. Kepercayaan ini adalah sebuah amanah dan tanggung jawab yang selalu kami pegang teguh. Selama 11 tahun Tokopedia melayani masyarakat Indonesia, kami selalu memberi perhatian lebih kepada system keamanan kami. Kami terus membangun, mengembangkan, dan meningkatkan prosedur serta system antisipasi dan mitigasi kami, sesuai dengan standar terbaik dunia.

Pada tanggal 2 Mei 2020, kami menyadari adanya pencurian data oleh pihak ketiga yang tidak berwenang terkait informasi pengguna Tokopedia. Selain pemberitahuan yang telah kami informasikan sebelumnya, kami ingin memberikan informasi terbaru terkait Langkah-langkah yang telah kami ambil hingga saat ini untuk mengatasi kejadian tersebut.

Pertama, setelah mengetahui kejadian ini, kami langsung memberikan informasi kepada seluruh pengguna Tokopedia, memulai proses investigasi dan mengambil Langkah-langkah yang perlu dilakukan untuk memastikan akun dan transaksi tetap terjaga. Kami terus pastikan bahwa kata sandi telah dienkripsi dengan enkripsi satu arah.

Kedua, kami telah berkomunikasi dan bekerja sama dengan pemerintah, antara lain Kementerian Komunikasi dan Informatika serta Badan Siber dan Sandi Negara untuk melakukan investigasi atas kejadian ini sekaligus memastikan keamanan dan perlindungan atas data pribadi anda.

Ketiga, selain melakukan invstigasi internal dengan teliti, kami juga telah menunjuk institusi independent kelas dunia yang memiliki spesialisasi di bidang keamanan siber dalam membantu investigasi dan identifikasi Langkah-langkah yang diperlukan guna lebih meningkatkan lagi perlindungan data para pengguna Tokopedia.

Pengguna kami adalah prioritas utama. Maka dari itu, sebagai Langkah pencegahan tambahan, kami senantiasa mengajak seluruh pengguna Tokopedia mengikuti anjuran Langkah pengamanan agar semua tetap terlindungi, seperti memastikan bahwa anda selalu mengganti kata sandi akun Tokopedia secara berkala, tidak menggunakankata sandi yang sama di berbagai platform digital, dan menjaga OTP dengan tidak memberikan kode OTP tersebut kepada pihak manapun termasuk yang mengatasnamakan Tokopedia dan untuk alasan apapun.

Kami memahami bahwa kejadian ini telah menimbulkan ketidaknyamanan pada seluruh pengguna. Maka dari itu, kami ingin mengucapkan terima kasih yang sebesar-besarnya kepada seluruh pengguna Tokopedia atas dukungan anda yang tiada henti kepada kami di tengah tantangan kali ini.

Salam,
William Tanuwijaya

Founder & CEO Tokopedia".[127]

Pada tahun 2020, belum ada pengaturan yang jelas mengenai perlindungan data pribadi sehingga Ketika terjadi kebocoran data pengguna Tokopedia tidak ada dasar hukum yang kuat. Sedangkan jika merujuk pada Pasal 46 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, disebutkan bahwa Pengendali Data Pribadi wajib membuat pengumuman tertulis paling lambat 72 (tujuh puluh dua) jam ke subjek data pribadi dan lembaga. Namun melihat dari *e-mail* yang dikirimkan oleh CEO PT Tokopedia dan disesuaikan dengan Undang-Undang Perlindungan Data Pribadi, dapat dikatakan bahwa PT Tokopedia lalai menjalankan kewajiban Pasal 46. Sehingga, jika mengikuti peraturan yang berlaku saat ini, PT Tokopedia dapat dikenakan sanksi administrative sebagaimana" yang di atur dalam Pasal 57 ayat (2), berupa:

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) dan ayat (3),*** *Pasal 47, Pasal 48 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) dikenai sanksi administrative.*
2. ***Sanksi administrative sebagaimana 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 administrative.***
3. *Sanksi administrative berupa denda administrative sebagaimana dimaksud pada ayat (2) huruf d paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.*
4. *Penjatuhan sanksi administrative sebagaimana dimaksud pada ayat (2) diberikan oleh Lembaga.*
5. *Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi adminsitratif sebagaimana dimaksud apda ayat (3) diatur dalam Peraturan Pemerintah".*[128]

[127] Agung Pratnyawan, "*Akui Data Pelanggan Tokopedia Dicuri, Ini Surat Terbuka William Tanuwijaya*", diakses Mei 23 2023. https://www.hitekno.com/internet/2020/05/13/123324/akui-data-pelanggan-tokopedia-dicuri-ini-surat-terbuka-william-tanuwijaya.

[128] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 57.

Seluruh kegagalan dan kelalaian akan dikenakan sanksi administratif oleh lembaga berupa: *peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi dan/atau denda adminstratif*[129] sebagaimana yang telah di atur dalam Pasal 57 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Sebelumnya di dalam Pasal 12 ayat (1) disebutkan bahwa subjek data pribadi berhak menggugat dan meminta ganti rugi ketika dalam pemrosesan data pribadinya terjadi pelanggaran. Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur Pasal 64 mengenai tata cara penyelesaian sengketa dan hukum acara yang digunakan, maka dalam hal ini gugatan dan ganti rugi yang di maksud dalam Pasal 12 ayat (1) adalah sebagai berikut:

1. *"Penyelesaian sengketa perlindungan data pribadi dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternative lainnya sesuai dengan ketentuan peraturan perundang-undangan;*
2. *Hukum acara yang belaku dalam penyelesaian sengketa dan/atau proses peradilan perlindungan data pribadi sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan hukum acara yang berlaku sesuai dengan ketentuan peraturan perundang-undangan;*
3. *Alat bukti yang sah dalam undang-undang ini meliputi:*
    a. *Alat bukti sebagaimana dimaksud dalam hukum acara; dan*
    b. *Alat bukti lain berupa informasi elektronik dan/atau dokumen elektronik sesuai dengan ketentuan peraturan perundang-undangan.*
4. *Dalam hal diperlukan untuk melindungi data pribadi, proses persidangan dilakukan secara tertutup".*[130]

Selain para pihak yang terlibat yang telah disebutkan penulis dalam pemrosesan data pribadi, tentunya terdapat tindakan pelanggaran lainnya yang dapat memberikan ancaman terhadap subjek data pribadi berikut dengan ancaman pidananya, yang penulis uraikan dalam tabulasi sebagai berikut:

[129] *Ibid.*
[130] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 64.

NO.	BENTUK PELANGGARAN	ANCAMAN PIDANA
1.	"Memperoleh atau mengumpulkan data pribadi orang lain untuk menguntungkan diri sendiri atau orang lain yang menyebabkan kerugian terhadap subjek data pribadi".[131]	"Pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)".[132]
2.	"Mengungkapkan data pribadi yang bukan miliknya".[133]	"Pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda palng banyak Rp 4.000.000.000,00 (empat miliar rupiah)".[134]
3.	"Menggunakan data pribadi yang bukan miliknya".[135]	"Pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah)".[136]
4.	"Membuat data pribadi palsu atau memalsukan data pribadi untuk menguntungkan diri sendiri atau orang lain yang dapat merugikan orang lain"[137]	"Pidana penjara paling lama 6 (enam) tahun dan.atau pidana denda paling banyak Rp 6.000.000.000,00 (enam miliar rupiah)".[138]

[131] *Ibid.* Pasal 65 ayat (1).
[132] *Ibid.* Pasal 67 ayat (1).
[133] *Ibid.* Pasal 65 ayat (2).
[134] *Ibid.* Pasal 67 ayat (2).
[135] *Ibid.* Pasal 65 ayat (3).
[136] *Ibid.* Pasal 67 ayat (3).
[137] Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 66.
[138] *Ibid.* Pasal 68.