LEX LIBRUM
JURNAL ILMU HUKUM
http://www.lexlibrum.id
P-ISSN: 2407-3849 E-ISSN: 2621-9867
Volume 10 Nomor 2 Juni 2024 Page: 187-198

Alamat:
Sekolah Tinggi Ilmu Hukum Sumpah Pemuda.
Jl. Kol. H. Animan Achyad (d/h. Jl. Sukabangun II) KM. 6,5 No. 1610
Kelurahan Sukabangun. Kecamatan Sukarami. 30151. Palembang.
Telp & Fax: 0711-418873 /E-mail: jurnallexlibrum@gmail.com

Simbiosis Mutualisme Badan Publik Dan Pengendali Data Pribadi Terhadap Perlindungan Hukum Kebocoran Atas Privasi Dan Data Pribadi

Derry Angling Kesuma[1]
[1]*Sekolah Tinggi Ilmu Hukum Sumpah Pemuda, E-mail: kesumaderry@gmail.com*

Info Artikel

Kata Kunci:
Data Pribadi,
Perlindungan Hukum,
Kebocoran Data

Doi: 10.46839/lljih.v10i2.984

Abstrak

Kehidupan sosial bermasyarakat memerlukan data pribadi. Sektor keamanan siber juga mencakup perlindungan data pribadi, yang merupakan tanggung jawab instansi terkait seperti Polisi, BSSN, BIN, dan Kementerian Pertahanan. Pertanggungjawaban pidana atas kebocoran data seharusnya tidak melepaskan siapa pun yang melakukannya, termasuk penyelenggara situs darknet yang berubah menjadi black market. Menurut Undang-Undang Perlindungan Data Pribadi, individu, termasuk mereka yang menjalankan bisnis atau membeli online di rumah, dapat dianggap sebagai pengendali data pribadi. Dengan demikian, individu ini secara hukum bertanggung jawab sepenuhnya atas pemrosesan data pribadi yang mereka lakukan. Pemerintah adalah lembaga eksekutif, legislatif, yudikatif, dan lain-lain yang berhubungan dengan operasi negara, disebut sebagai badan publik. Badan publik dapat menjadi pengendali atau prosesor data pribadi, dan diwajibkan oleh Pasal 20 hingga 50 Undang-Undang Perlindungan Data Pribadi. Antara lain, mereka diharuskan untuk menunjukkan bukti persetujuan subjek data pribadi saat melakukan pemrosesan data pribadi, dan menunjukkan bukti lain yang menunjukkan persetujuan subjek data pribadi.

Abstract: *Social life requires personal data. The cybersecurity sector also covers the protection of personal data, which is the responsibility of related agencies such as the Police, BSSN, BIN, and the Ministry of Defence. Criminal responsibility for the data leak should not release anyone who did it, including the administrator of the darknet site that turned into a black market. Under the Personal Data Protection Act, individuals, including those who run a business or purchase online at home, can be considered as controllers of personal data. Thus, these individuals are legally fully responsible for the processing of their personal data. Government is the executive, legislative, judicial, and other bodies related to state operations, called public bodies. A public body may be the controller or processor of personal data, and is required by Articles 20 to 50 of the Personal Data Protection Act. Among other things, they are required to provide proof of the consent of the personal data subject when carrying out the processing of personal data, and to provide other proof that indicates consent to the data subject.*

Keywords: Personal Data, Legal Protection, Data Leakage

PENDAHULUAN

Perdagangan elektronik, juga dikenal sebagai *e-commerce*, adalah salah satu kemajuan yang dihasilkan oleh pertumbuhan ekonomi digital. Penjual dan pembeli dapat melakukan transaksi apa pun tanpa perlu bertemu secara tatap muka melalui *e-commerce*.

Kegiatan jual beli dapat dilakukan di mana saja asalkan terhubung ke jaringan internet. Ini pasti meningkatkan efisiensi waktu manusia dan mengurangi biaya barang dan jasa. Namun di samping dampak positif tersebut, *e-commerc*e juga memiliki dampak negatif. Salah satunya yaitu rawan terjadinya kejahatan siber. Bentuk-bentuk kejahatan siber yang sering terjadi dalam *e-commerce* yaitu pembayaran menggunakan kartu kredit milik orang lain *(carding)*, akses ilegal ke sistem informasi *(hacking),* perusakan *website*, dan pencurian data pribadi.Kasus kebocoran data Tokopedia yang terjadi pada tahun 2020 adalah salah satu contohnya.[1]Data pribadi adalah rangkaian komunikasi, fakta, atau pendapat yang berkaitan dengan seseorang. Karena data ini sangat pribadi atau sensitif, individu yang bersangkutan ingin mencegah orang lain mengumpulkan, menggunakan, atau menyebarkannya. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menjelaskan definisi data pribadi. "Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya," kata bagian 1 angka 1. Dengan sektor *e-commerce* Indonesia yang semakin berkembang, ancaman kebocoran data pribadi juga menjadi lebih jelas. Presiden Joko Widodo meluncurkan Gerakan 1000 Startup untuk mendorong kemajuan ekonomi digital. Program ini setidaknya telah mendorong pertumbuhan empat startup *unicorn* Indonesia: Go-Jek, Tokopedia, Traveloka, dan Bukalapak. Dengan pertumbuhan startup digital ini, banyak data pribadi konsumen dikumpulkan, termasuk data tentang perilaku konsumen.

Penyelenggara sistem elektronik diwajibkan untuk mengamankan informasi atau dokumen elektronik dan segera melaporkannya kepada aparat penegak hukum atau lembaga terkait menurut PP Nomor 71 Tahun 2019. Tokopedia juga terus bekerja sama dengan Kemenkominfo dan Badan Siber dan Sandi Negara untuk menyelidiki dan mengawasi masalah ini.Tokopedia bertanggung jawab atas kebocoran data pribadi konsumen sesuai dengan Undang-Undang ITE dan peraturan terkait. Tokopedia telah melakukan upaya terbaik untuk melindungi sistem elektroniknya dan menerapkan manajemen risiko sesuai dengan peraturan. Terungkap juga bahwa Belakangan ini isu kebocoran data pribadi dan penawaran transaksi terhadap data pribadi yang bocor kembali merebak. Insiden tersebut tidak hanya melanda data pribadi yang dikelola korporasi melainkan juga lembaga Pemerintah. Tentu publik menjadi khawatir dan mempertanyakan mengapa insiden tersebut seringkali terjadi dan seakan tidak ada penegakan hukumnya. Semua insiden kebocoran data pribadi seakan selesai cukup dengan adanya pemberitaan saja. Korporasi dan instansi terkait seakan cukup memberitahukan kepada publik cukup hanya dengan mengeluarkan pernyataan dan klarifikasi saja. Walhasil, seakan pelaku pencurian data pribadi melenggang dengan leluasa melakukan tindakan tersebut dan seakan merasa sah-sah saja bebas melakukan jual beli data pribadi sebagai mata pencahariannya melakukan penawaran melalui situs *darknet*.

Sementara itu, suatu insiden kebocoran data, tentu kemungkinannya tidak hanya terjadi karena serangan dari luar saja, karena boleh jadi merupakan suatu tindakan pengungkapan dari dalam organisasi itu sendiri. Untuk memperjelas hal itu tentu

[1]HeyLaw Indonesia | *Your Trusted Legal Edutech Platform*

diperlukan pembuktian yang tidak mungkin digantungkan hanya dari pernyataan satu pihak saja, melainkan harus juga dibuktikan oleh audit dari pihak lain ataupun instansi yang terkait. Pemerintah melalui instansi sektoral yang sesuai dengan kewenangan yang diberikan oleh undang-undang, memiliki tugas dan fungsi serta kewenangan untuk melakukan pengawasan atas pelindungan data pribadi masyarakat. Khawatirnya, publik justru akan menilai seakan-akan tidak ada kesadaran hukum bagi korporasi dan instansi terkait untuk melindungi data pribadi masyarakat. Seakan tiada upaya yang dapat dilakukan oleh masyarakat untuk menuntut pelindungan yang lebih baik, karena terkesan bahwa korporasi dan instansi terkait hanya memandang remeh hal tersebut, karena kejadian itu berulang kali terjadi tanpa penegakan hukum yang jelas. Apakah memang tidak ada aturan pertanggungjawaban hukum oleh penyelenggara sistem elektronik terhadap kebocoran tersebut, atau Apakah publik harus menunggu Rancangan Undang-Undang Pelindungan Data Pribadi disahkan dulu baru tindakan tersebut dapat dimintakan pertanggungjawaban hukumnya. Tulisan ini mencoba mengingatkan semua pihak terkait adanya pertanggungjawaban hukum terhadap kebocoran atas privasi dan data pribadi, baik secara perdata, administratif maupun pidana. Oleh karena itulah, maka permasalahan akan dibatasi oleh penulis dengan hanya meneliti mengenai bagaimanakah simbiosis mutualisme badan publik dan pengendali data pribadi terhadap perlindungan hukum kebocoran atas privasi dan data pribadi.

METODE PENELITIAN

Dalam penelitian ini, pendekatan yuridis normatif dengan pendekatan deskriptif digunakan. Tujuan dari pendekatan ini adalah untuk menggambarkan suatu masalah dengan memberikan penjelasan yang akurat dan faktual tentang fakta-fakta dan karakteristik subjek penelitian. Penelitian ini menggunakan metode normatif kualitatif untuk melakukan analisis data. Peraturan perundang-undangan yang berkaitan dengan penelitian ini merupakan sumber hukum utama.

PEMBAHASAN

Secara historis, istilah privasi dan data pribadi sebenarnya bukanlah hal yang baru. Meskipun *International Covenant on Civil and Political Rights* (ICCPR) tidak secara tegas menyebutkan istilah ‘data pribadi’, namun secara substansial pelindungan atas data pribadi adalah bagian dari privasi atau kehidupan pribadi setiap orang. Pelindungan atas data pribadi tidak hanya diatur di konvensi regional Uni Eropa *General Data Protection Regulation*, melainkan juga regional lainnya seperti Afrika (*African Union Convention on Cyber Security and Personal Data Protection*) dan juga Asia. Di dalam *ASEAN Declaration of Human Rights* (2012) secara tegas dinyatakan bahwa data pribadi adalah bagian dari privasi meski tidak diuraikan lebih detail.[2] Pembahasan tentang perlindungan data pribadi yang sering kali dibahas di dalam konteks hukum siber. Ditambah lagi dengan diterapkannya *General Data Protection Regulation* di Uni Eropa yang efektif berlaku pada 28 Mei 2018 yang secara *paralel* diikuti oleh berbagai negara dalam memberlakukan

[2] Edmon Makarim, *https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef/?page=all*. 2020.

aturan hukum tentang perlindungan data pribadi.[3] Dalam perbincangan atas pengaturan data pribadi, sebenarnya terdapat aspek internasional yang perlu diketahui, yaitu transfer data, yang mana di dalam ketentuan *General Data Protection Regulation* disyaratkan pengiriman data lintas territorial hanya diijinkan jika negara penerima data memiliki standar yang sama dan/atau lebih tinggi dari negara pengirim. Akibat ketentuan tersebut di atas, maka banyak negara yang mengadopsi ketentuan *General Data Protection Regulation* agar dalam aktivitas pengiriman data lintas negara diperbolehkan. Di lain pihak, bagi negara yang tidak memiliki standar yang sama dengan *General Data Protection Regulation*, maka harus menerima konsekwensi tidak dapat dikirimkannya data dari negara lain yang memiliki standar perlindungan data yang lebih tinggi. Dengan tidak dapat dikirimkannya data ke suatu negara yang belum memiliki standar perlindungan data yang baik maka tentunya akan menyulitkan dalam aktivitas diantaranya, penegakkan hukum, perdagangan, dan sebagainya.

Saat ini, Indonesia memiliki lebih dari 30 undang-undang sektoral yang menyebarluaskan undang-undang tentang perlindungan data pribadi, yang berarti negara itu sudah melindungi data pribadi, meskipun belum sepenuhnya. Sebenarnya, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik juga mengatur perlindungan data pribadi, tetapi karena bentuknya yang tidak jelas, seringkali dianggap bahwa Undang-Undang Informasi dan Transaksi Elektronik tidak mengatur perlindungan data pribadi sama sekali. Pasal 26 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik mengatur perlindungan data pribadi. Sebagai objek dari Undang-Undang Informasi dan Transaksi Elektronik, data pribadi dalam bentuk elektronik yang disimpan, ditransfer, atau ditransmisikan adalah subjek dari Undang-Undang Informasi dan Transaksi Elektronik. Oleh karena itu, ketentuan yang mengatur perlindungan data pribadi dalam Undang-Undang Informasi dan Transaksi Elektronik tidak terbatas pada Pasal 26 saja. Dalam hal Undang-Undang Informasi dan Transaksi Elektronik, beberapa konsep utama yang dapat digunakan untuk menetapkan data pribadi (dalam bentuk elektronik) sebagai objek Undang-Undang Informasi dan Transaksi Elektronik adalah informasi elektronik dan dokumen elektronik, yang berarti semua jenis informasi elektronik dan dokumen elektronik, termasuk data pribadi. Oleh karena itu, membaca ketentuan Undang-Undang Informasi dan Transaksi Elektronik tentang data pribadi memiliki dua kemungkinan, yaitu:

(1)data pribadi yang bentuknya elektronik,

(2)data pribadi bisa berbentuk informasi elektronik dan/atau dokumen elektronik. Dengan dua kualifikasi di atas, maka segala macam bentuk data pribadi yang bentuknya elektronik adalah objek dari Undang-Undang Informasi dan Transaksi Elektronik.

Selanjutnya, Pasal 30, 31, 32, 34, dan 36 Undang-Undang Informasi dan Transaksi Elektronik melarang melindungi informasi elektronik dan/atau dokumen elektronik, termasuk data pribadi. Pasal-pasal ini melarang secara tidak langsung melindungi data

[3] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime Di Indonesia,* PT. Raja Gafindo persada Jakarta, 2007, hlm. 32

pribadi. Ketentuan yang ada di dalam pasal 26 Undang-Undang Informasi dan Transaksi Elektronik adalah subset dari rezim perlindungan data pribadi, yaitu hak untuk penghapusan informasi yang dianggap sudah tidak relevan. Ada beberapa istilah yang digunakan untuk menggambarkan penghapusan ini, seperti *right to be forgotten, right to oblivion, right to be let alone.* Namun, kami mengenal istilah-istilah tersebut di atas dalam konteks hukum positif dengan "penghapusan informasi yang tidak relevan".

Kebutuhan akan pengaturan data pribadi menunjukkan tanggung jawab negara untuk melindungi warganya dan kekuatan negara di dunia internasional. Dalam situasi saat ini, Undang-Undang Informasi dan Transaksi Elektronik hanya berfungsi untuk melindungi warga negara negara karena cakupannya belum mampu menggabungkan dengan sistem hukum perlindungan data pribadi seperti *General Data Protection Regulation*. Di masa depan, kami berharap pemerintah dapat segera mengeluarkan undang-undang yang mengatur perlindungan data pribadi. Dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Undang-Undang PDP) mengatur bahwa orang perorangan termasuk yang melakukan kegiatan bisnis atau *e-commerce* di rumah dapat dikategorikan sebagai pengendali data pribadi. Sehingga ia bertanggung jawab secara hukum atas pemrosesan data pribadi yang diselenggarakannya dan memenuhi ketentuan yang ada dalam Undang-Undang Perlindungan Data Pribadi.[4] Apa saja yang tergolong data pribadi yaitu:

a. yang bersifat spesifik, meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi; dan/atau data lainnya sesuai dengan ketentuan peraturan perundang- undangan;
b. Data pribadi yang bersifat umum, meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

Undang-Undang Perlindungan Data Pribadi sendiri merupakan pengejawantahan dari Pasal 28G ayat (1) UUD 1945 yang berbunyi: *Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi.*

Pengertian pelindungan data pribadi berdasarkan Pasal 1 angka 2 Undang-Undang Perlindungan Data Pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Dengan kemajuan teknologi dan informasi saat ini, layanan bank harus memberikan layanan yang cepat, nyaman, aman, dan mudah digunakan oleh klien kapan pun melalui laptop atau smartphone mereka. Oleh karena itu, diciptakan inovasi digital berbasis media elektronik, elektronik banking *(e-banking).* Layanan pertama, SMS *Banking*, dapat diakses melalui smartphone melalui SMS *(Short Message Service),* memiliki berbagai fitur seperti informasi tentang saldo rekening, mutasi rekening, tagihan kartu kredit, suku bunga, dan pembayaran. *Mobile Banking (M-Banking)* menawarkan layanan yang menggunakan

[4]Ayyi Achmad Hidayah and Shila Ezerli, "*Kasus Kebocoran Data Semakin Banyak, Belanja Daring Rentan*" (Lokadata.id, 2020), https://lokadata.id/artikel/kasus-kebocoran-data- semakin-banyak-belanja-daring-paling-rentan.

smartphone melalui *Subscriber Identity Modul* (SIM) kartu, *Unstructured Suplementary Service Data (USSD)*, dan aplikasi yang dapat diinstal dan diunduh oleh pelanggan. Layanan *M-Banking* ini menawarkan informasi tentang saldo rekening, mutasi rekening, suku bunga, tagihan kartu kredit, lokasi ATM dan cabang terdekat, serta informasi tentang pembelian dan pembayaran. Selain itu, ada layanan perbankan *online,* yang memungkinkan Anda melakukan transaksi perbankan melalui internet dengan menggunakan PC, *desktop, tablet,* laptop, atau smartphone yang terhubung ke internet. Fitur layanan internet banking antara lain informasi umum rekening tabungan/giro, kartu kredit, mutasi rekening, *transfer* dana, pembelian, serta pembayaran yang dapat mempermudah para nasabah untuk mengaksesnya.[5]

Salah satu komponen paling penting dari kehidupan sosial bermasyarakat adalah data pribadi. Ini terutama berlaku di era digitalisasi saat ini, ketika semua aspek kehidupan bergantung pada teknologi, seperti kemampuan setiap orang untuk terhubung satu sama lain tanpa mengorbankan waktu atau jarak. Pasal 1 angka 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik yang berbunyi "Data pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya".[6] Menurut Pasal 1 angka 6 Ketentuan Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Pribadi Nasabah menjelaskan bahwa "Data Pribadi Nasabah adalah identitas yang lazim disediakan oleh Nasabah kepada Bank dalam rangkamelakukan transaksi keuangan dengan Bank. Selain itu, karena pelindungan data pribadi adalah juga bagian dari sektor keamanan siber, maka hal tersebut juga tidak lepas dari kewenangan instansi terkaitnya, antara lain; Polri, BSSN, BIN dan Kementerian Pertahanan. Penggunaan anggaran negara yang merupakan uang rakyat untuk mengadakan alat dan perangkat keamanan serta diklat para aparat tentu tidaklah murah. Maka menjadi pertanyaan bagi publik, bagaimana dan sejauh mana penggunaan perangkat tersebut telah dapat menciptakan manfaat bagi kepentingan publik.[7] Masyarakat berhak meminta kejelasan dan akuntabilitas dalam proses pencegahan dan penegakan hukumnya, serta mempertanyakan mengapa situasi kebocoran data pribadi seakan terus berulang kali terjadi. Apakah insiden akan terus terjadi karena berbagai instansi yang terkait tersebut seakan lupa atau sangat sulit berkoordinasi demi menjaga kepentingan publik. Bukan suatu hal yang tidak mungkin bagi setiap warga negara yang dirugikan untuk menggugat PMH kepada instansi yang terkait, karena tidak menjalankan kewenangannya sebagaimana mestinya. Hal tersebut dapat dipersepsikan sebagai tindakan pembiaran yang telah merugikan publik.

Jikalau berbicara mengenai pertanggungjawaban pidana terhadap kebocoran data seharusnya juga tidak melepaskan siapa yang menjadi penadahnya, termasuk penyelenggara situs darknet yang menjadi *black-market*. Penawaran data pribadi yang diperoleh secara melawan hukum adalah laksana memperdagangkan barang curian di pasar

[5] Dwi Ayu Astrini, "*Perlindungan Hukum Terhadap Nasabah Bank Pengguna Internet Banking Dari Ancaman Cybercrime*", Jurnal Privatum, 3(1), 2015, hlm. 149.

[6] *Ibid*

[7] *Ibid*

gelap sebagaimana diatur dalam Pasal 480 KUHP. Selain pelaku utama tentu ada tindakan penyertaan yang harus dikejar oleh para penegak hukum, seperti korporasi dan instansi yang dengan sengaja tidak memiliki dan menjaga sistem keamanan elektronik mereka terhadap pengelolaan data pribadi yang baik. Selayaknya juga dapat dikatakan harus turut serta bertanggung jawab sebagai penyedia sarana untuk melakukan kejahatan kepada publik. Lebih lanjut, dalam Pasal 65 ayat (2) dalam Undang-Undang Perdagangan juga terdapat ketentuan pidana korporasi, jika PMSE melakukan perdagangan yang tidak sesuai dengan apa yang telah dinyatakannya.

Ketentuan ini dapat dikaitkan dengan aspek pelindungan data pribadi dalam *privacy statement* yang dikemukakan oleh PSE tersebut. Pengenaan pidana korporasi sangat diperlukan penegakannya agar setiap PSE menyadari kewajiban hukumnya.[8] Jika tidak, maka dengan kompleksitas sistem elektronik, PSE cenderung akan dapat melakukan penipuan kepada pengguna sistemnya, melalui rangkaian tipu muslihat via *code* pada sistem elektroniknya atau mungkin cenderung membiarkan penerobosan dan pencurian data yang dilakukan di depan mata. Bukan tidak mungkin ada potensi keuntungan atas klaim asuransi disana. Undang-Undang Perlindungan Data Pribadi ini mengatur bahwa orang perorangan termasuk yang melakukan kegiatan bisnis atau *e-commerce* di rumah dapat dikategorikan sebagai pengendali data pribadi.[9] Sehingga orang ini bertanggung jawab secara penuh secara hukum atas pemrosesan data pribadi yang diselenggarakannya dan memenuhi ketentuan yang ada dalam Undang-Undang Perlindungan Data Pribadi ini. Dan didalam Undang-Undang Perlindungan Data Pribadi mengatur mengenai Implementasi kewajiban perlindungan data pribadi oleh Pengendali Data Pribadi adalah sebagai berikut: [10]

1. Wajib memiliki dasar pemrosesan data pribadi (Pasal 20 UU-PDP);
2. Wajib melakukan pemrosesan data pribadi secara terbatas dan spesifik, sah secara hukum, dan transparan (Pasal 27 UU-PDP);
3. Wajib melakukan pemrosesan data pribadi sesuai dengan tujuan pemrosesan data pribadi (Pasal 28 UU-PDP);
4. Wajib memastikan akurasi, kelengkapan, dan konsistensi data pribadi sesuai dengan ketentuan peraturan perundang-undangan (Pasal 29 UU-PDP);
5. Wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi (Pasal 31 UU-PDP);
6. Wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya (Pasal 35 UU-PDP);
7. Wajib menjaga kerahasiaan data pribadi dalam melakukan pemrosesan data pribadi (Pasal 36 UU-PDP);

[8]Wahyudi Djafar, "*Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan,"* Jurnal Becoss 1(1). (2019): p. 147–54.

[9]Isi UU Perlindungan Data Pribadi Undang-Undang No 27 Tahun 2022 (tirto.id), diakses 1 November 2023

[10]Isi UU Perlindungan Data Pribadi Undang-Undang No 27 Tahun 2022", https://tirto.id/gFk7, diakses 1 November 2023

8. Wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi (Pasal 37 UU-PDP);
9. Wajib melindungi data pribadi dari pemrosesan yang tidak sah (Pasal 38 UU-PDP);
10. Wajib mencegah data pribadi diakses secara tidak sah (Pasal 39 UU-PDP);
11. Wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi (Pasal 47 UU-PDP);
12. Wajib menunjuk pejabat atau petugas yang melaksanakan fungsi Perlindungan Data Pribadi (Pasal 53 UU-PDP).

Dalam Undang-Undang Perlindungan Data Pribadi terdapat pengendali data pribadi dan prosesor data pribadi. Pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi.[11]Sedangkan yang dimaksud dengan prosesor data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan pemrosesan data pribadi atas nama pengendali data pribadi. Badan publik adalah Lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD, atau organisasi non-pemerintah sepanjang sebagian atau seluruh dananya bersumber dari APBN dan/atau APBD, sumbangan masyarakat, dan/atau luar negeri. Dengan kata lain, badan publik merupakan pemerintah yang dapat menjadi pengendali data pribadi maupun prosesor data pribadi.

Kewajiban pengendali data pribadi diatur dalam Pasal 20 sampai dengan Pasal 50 Undang-Undang Perlindungan Data Pribadi di antaranya wajib menunjukkan bukti persetujuan yang telah diberikan subjek data pribadi saat melakukan pemrosesan data pribadi, wajib menjaga kerahasiaan data pribadi, dan wajib mencegah data pribadi diakses secara tidak sah.Sementara itu, kewajiban prosesor data pribadi tercantum dalam Pasal 51 sampai dengan Pasal 52 UU-PDP antara lain wajib melakukan pemrosesan data pribadi berdasarkan perintah pengendali data pribadi, wajib mendapatkan persetujuan tertulis dari pengendali data pribadi sebelum melibatkan prosesor data pribadi lain. Pengendali data pribadi dan prosesor data pribadi wajib menunjuk pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi dalam hal:

a. pemrosesan data pribadi untuk kepentingan pelayanan publik;
b. kegiatan inti pengendali data pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; dan
c. kegiatan inti pengendali data pribadi terdiri dari pemrosesan data pribadi dalam skala besar untuk data pribadi yang bersifat spesifik dan/atau data pribadi yang berkaitan dengan tindak pidana.

[11] *Ibid*

Pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi ditunjuk berdasarkan profesionalitas, pengetahuan mengenai hukum, praktik pelindungan data pribadi, dan kemampuan untuk memenuhi tugas-tugasnya. Pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi bertugas paling sedikit:

a. menginformasikan dan memberikan saran kepada pengendali data pribadi atau prosesor data pribadi agar mematuhi ketentuan UU-PDP;
b. memantau dan memastikan kepatuhan UU-PDP dan kebijakan pengendali data pribadi atau prosesor data pribadi;
c. memberikan saran mengenai penilaian dampak pelindungan data pribadi dan memantau kinerja pengendali data pribadi dan prosesor data pribadi; dan
d. berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan data pribadi.

Subjek data pribadi adalah orang perseorangan yang pada dirinya melekat data pribadi, yang tidak lain adalah diri kita sebagai masyarakat. Mengenai hak-hak subjek data pribadi diatur lebih lanjut di dalam Pasal 5 sampai dengan Pasal 15 UU-PDP antara lain berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi, berhak mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi tentang dirinya, serta berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya.Namun, berdasarkan Pasal 15 ayat (1) UU-PDP menyebutkan: Hak-hak Subjek Data Pribadi sebagaimana dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) dikecualikan untuk:

a. kepentingan pertahanan dan keamanan nasional;
b. kepentingan proses penegakan hukum;
c. kepentingan umum dalam rangka penyelenggaraan negara;
d. kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau
e. kepentingan statistik dan penelitian ilmiah.

Adapun yang dimaksud dalam kepentingan proses penegakan hukum seperti kepentingan yang berkaitan dengan upaya atau langkah dalam rangka menjalankan atau menegakkan aturan hukum berdasarkan ketentuan peraturan perundang-undangan antara lain proses penyelidikan, penyidikan, dan penuntutan. Kemudian yang dimaksud dengan kepentingan umum dalam rangka penyelenggaraan negara seperti penyelenggaraan administrasi kependudukan, jaminan sosial, perpajakan, kepabeanan, dan pelayanan perizinan berusaha terintegrasi secara elektronik. Pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya, dengan melakukan:

a. penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi; dan
b. penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi.

Dalam hal terjadi kegagalan pelindungan data pribadi, pengendali data pribadi wajib menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada subjek data pribadi dan lembaga, dengan 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 pengendali data pribadi.

Bahkan dalam hal tertentu misalnya jika kegagalan itu mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat, pengendali data pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan pelindungan data pribadi. Namun patut dicatat, kewajiban menyampaikan pemberitahuan secara tertulis kepada subjek data pribadi saat terjadi kegagalan perlindungan data pribadi dikecualikan untuk:

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

Akan tetapi, pengecualian ini hanya dalam rangka pelaksanaan ketentuan undang-undang. Di sisi lain, dalam Pasal 47 Undang-Undang Perlindungan Data Pribadi secara tegas menyebutkan bahwa: "*Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Pelindungan Data Pribadi"*.

Pelanggaran terhadap ketentuan Pasal 46 ayat (1) dan (3) serta Pasal 47 Undang-Undang Perlindungan Data Pribadi sebagaimana disebut di atas dikenai sanksi administratif berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, dan/atau denda administratif. Penjatuhan sanksi administratif diberikan oleh lembaga dan untuk denda paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

KESIMPULAN

Kehidupan sosial bermasyarakat memerlukan data pribadi. Pertanggungjawaban pidana atas kebocoran data pribadi seharusnya tidak melepaskan siapa pun yang melakukannya, termasuk penyelenggara situs darknet yang berubah menjadi black market. Orang-orang, termasuk mereka yang melakukan bisnis atau berbelanja online di rumah mereka, dapat dikategorikan sebagai pengendali data pribadi oleh Undang-Undang Perlindungan Data Pribadi, yang mengatur bahwa memperdagangkan barang curian di pasar gelap adalah perbuatan yang melanggar hukum. Oleh karena itu, individu ini secara hukum bertanggung jawab sepenuhnya atas pemrosesan data pribadi yang dilakukannya dan harus mematuhi ketentuan yang diatur dalam Undang-Undang Perlindungan Data Pribadi. Badan publik adalah lembaga eksekutif, legislatif, yudikatif, dan lain-lain yang fungsi dan tugas utamanya berkaitan dengan penyelenggaraan negara. Badan publik

sebagian atau seluruhnya didanai oleh APBN dan/atau APBD, atau oleh organisasi non-pemerintah sebagian atau seluruhnya didanai oleh APBN dan/atau APBD, atau oleh sumbangan masyarakat, luar negeri, atau lainnya. Dengan kata lain, badan publik adalah pemerintah yang memiliki otoritas untuk mengawasi data pribadi dan prosedur.

DAFTAR PUSTAKA

Achmad Ali. (2002). *Menguak Tabir Hukum (Suatu Kajian Filosofis dan Sosiologis)*. Jakarta: Toko Gunung Agung

Adami Chazawi.(2011) *Pelajaran Hukum Pidana Bagian* I. Jakarta: Rajawali Pers.

Admaja Priyatno.(2004) *Kebijakan Legislasi Tentang SistemPertanggungjawaban Pidana Koorporasi Di Indonesia*. Bandung: Cv. Utomo.

Andi Hamzah.(2004), *Asas-Asas Hukum Pidana* Edisi Revisi. Jakarta: Rineka Cipta.

B.W, A. (2007). *Tindak Pidana Mayantara Perkembangan Kajian Cybercrime di Indonesia.* Jakarta: PT. Rajagrafindo Persada.

Cst Kansil, Christine, S.T Kansil, Engelien R, Palandeng dan Godlieb N Mamahit. (2009). *Kamus Istilah Hukum*, Jakarta.

Domikus R. (2010). *Filsafat Hukum Mencari: Memahami dan Memahami Hukum.* Yogyakarta: Laksbang Pressindo

Erdianto Effendi.(2014). *Hukum Pidana Indonesia Suatu Pengantar*. Bandung: PT. Refika Aditama.

Indriyanto Seno Adji.(1991). *Korupsi Dan Hukum Pidana*. Jakarta: Kantor Pengacara dan Konsultasi Hukum “Prof. Oemar Seno Adji & Rekan, 2002.

Lutfhie Aunie. *Transformasi Politik Dan Ekonomi Kerajaan Aceh (1641-1699)Dalam Pranata Islam Di Indonesia :Pergualatan Sosisal, Politik, Hukum Dan Pendidikan.* Jakarta: Logos Wacana Ilmu, 2001.

Mansur, D. d. (2005). *Cyberlaw Aspek Hukum Informasi* . Bandung: PT. Refika Aditama

Nawawi Arief, Barda.(2007). *Tindak Pidana Mayantara Perkembangan Kajian Cbercrime Di Indonesia.* Jakarta: PT. Raja Gafindo persada.

N., M. (2017). *Pengantar Hukum Siber Indonesia.* Depok: Rajawali Pers.

Oemar Seno Adji. *Etika Profesional Dan Hukum Pertanggungjawaban PidanaDokte*r. Jakarta: Erlangga.

Peter, M. (2008). *Pengantar Ilmu Hukum*. Jakarta: Kencana.

Rahmanuddin Tomalili.(2012). *Hukum Pidana*. Yogyakarta: CV. Budi Utama.

Rosadi, S. (2015). *Cyberlaw Aspek Data Privasi Menurut Hukum Internasional,Regional, dan Nasional.* Refika Aditama.

Soerjono Soekanto, S. M. (2013). *Penelitian Hukum Normatif Suatu Tinjauan Singkat.* Jakarta: PT. Raja Grafindo Persada.

W., D. (2017). *Big Data dan Pengumpulan Data Skala Besar di Indonesia: Pengantar untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi (Internet dan Hak Asasi Manusia).* Jakrta: Pusdok Elsam.