BAB II

TINJAUAN PUSTAKA

A. Pengertian Data Pribadi dan Perlindungan Data Pribadi

1. Pengertian Data Pribadi

Setiap informasi privat adalah data pribadi, namun tidak semua informasi pribadi merupakan bagian dari privasi individu. Data berasal dari bahasa Latin jamak yang berarti "apa yang diberikan" .[17]

Beberapa ahli juga telah mendefinisikan definisi data, Menurut Nuzulla Agustina, data merupakan serangkaian angka, fakta, gambar, diagram, kata, simbol, karakter, dan sebagainya mengenai suatu hal yang sering terjadi yang menyampaikan sebuah pemikiran, kondisi, objek, atau situasi. Selain Nuzra, menurut Arikunto Suharsimi, data merupakan sekumpulan informasi dan angka yang dapat digunakan sebagai dasar untuk menyusun informasi.[18]

Van der Sloot menyatakan bahwa istilah data pribadi tidak hanya mencakup informasi yang bersifat sensitif atau pribadi, tetapi juga mencakup data yang bersifat publik dan non-sensitif.

[17] Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6* (1), 132–142. https://doi.org/10.38043/jah.v6i1.4484.

[18] RifqiMulyawan.com. 26 oktober 2024. Ini Dia Sebenarnya Pengertian Data: Menurut Ahli, Sejarah, Fungsi, Jenis, dan Contohnya!. Diakses pada 27 Oktober 2024, dari https://rifqimulyawan.com/blog/pengertian-data/

Bukannya memberikan hak untuk mengendalikan (data), inti dari prinsip-prinsip perlindungan data terletak pada keadilan dan kesetaraan dalam pemrosesan data.

Menurut pakar E. Mutiara dan Kuswwadi, data adalah sekumpulan informasi yang didapat dari suatu pengamatan dan dapat berupa simbol, angka atau karakteristik.[19] Selain itu, pada tahun 2008, negara-negara anggota Uni Eropa menetapkan *General Data Protection Rule* yang mendefinisikan data pribadi sebagai informasi yang dapat mengidentifikasi seseorang yang berkaitan dengan tanda pengenal seperti nama, nomor identifikasi, lokasi individu, data fisik, data fisiologis, identitas, dan lainnya.[20]

Data pribadi merupakan informasi mengenai individu yang mencakup fakta-fakta, komunikasi, serta pendapat yang memiliki keterkaitan dengan orang tersebut dan dirasakan sebagai informasi yang sensitif, sehingga pengumpulan, penggunaan, atau distribusinya dianggap terbatas atau dilarang.[21] Sebenarnya, data pribadi dan privasi adalah dua hal yang saling terkait dan tidak dapat dipisahkan. Meskipun mereka memiliki variasi dalam lingkup serta ketentuan substansinya.

[19] Ibid15.
[20] Search hrw.org. 6 Juni 2018. Peraturan Perlindungan Data Umum Uni Eropa. Diakses pada 29 Oktober 2024, dari https://www.hrw.org/id/news/2018/06/06/318734.
[21] Shofiyah, E. N., & Indri Fogar, S. (2019). Penyalahgunaan data pribadi penerima pinjaman dalam Peer To Peer Lending. *Novum: Jurnal Hukum*, *6*(2), Hal 2-3.

Maka dapat disimpulkan bahwa data pribadi adalah informasi yang berkaitan dengan individu yang mencakup fakta, komunikasi, dan opini yang memiliki keterkaitan antar orang, di mana bersifat sensitif serta dibatasi dalam pengumpulan, penggunaan, dan distribusinya. Pada dasarnya, data pribadi seringkali berupa informasi tentang seseorang seperti jenis kelamin, alamat tempat tinggal, pendidikan, dan rincian pribadi, yang ketika dikumpulkan dapat membentuk profil individu untuk menghasilkan informasi tertentu.

Privasi adalah hak fundamental yang sangat penting bagi perlindungan kebebasan dan martabat manusia dan dimaksudkan untuk menjadi dasar bagi banyak lembaga hak asasi manusia. Privasi memberikan kemampuan untuk menetapkan dan mengelola batasan untuk melindungi terhadap gangguan yang tidak diinginkan, dan hak untuk memutuskan apa yang dapat dilihat tentang diri Anda. Aturan privasi memberikan legitimasi terhadap hak ini, melindungi kita dari penyalahgunaan kekuasaan yang sewenang-wenang dan melanggar hukum dengan mengurangi informasi tentang kita yang dapat diakses oleh orang lain dan melindungi kita dari pihak-pihak yang berusaha mengendalikannya dan sangat penting untuk melindungi masyarakat.[22]

[22] Djafr, W., & Santoso, M. J. (2019). Perlindungan Data Pribadi Konsep, Instrumen, dan Prinsipnya. *Lembaga Studi Dan Advokasi Masyarakat (ELSAM)*, 2. https://referensi.elsam.or.id/wp-content/uploads/2015/01/Perkembangan-Pemikiran-HAM.pdf

Menurut Julie Innes, privasi adalah keadaan di mana individu memiliki kendali atas keputusannya sendiri, termasuk keputusan mengenai akses, informasi, dan tindakannya sendiri. Selain itu, pakar lain seperti Alan Westin percaya bahwa privasi sepenuhnya bergantung pada individu, kelompok, atau komunitas untuk memutuskan sejauh mana informasi mereka boleh dan tidak boleh dibagikan kepada orang lain.

Telah kita pahami, hak privasi adalah sebuah komponen dari Hak Asasi Manusia yang sudah ada dan terus berkembang hingga kini. Hak ini bersifat global dan termasuk dalam hukum positif di seluruh dunia. Indonesia sendiri memahami hak privasi berdasarkan pandangan Allen Westin yang mana dalam pemikirannya memberikan penjelasan tentang konsep hak privasi di era pra-modern. Seiring dengan kemajuan zaman, konsep yang diadopsi oleh Indonesia terdampak oleh kedatangan budaya Belanda yang pada akhirnya membuat hak privasi diatur dengan adanya undang-undang tertulis seperti yang terdapat dalam perundang-undangan.

Menurut Lousi Brandeis dan Samuel Warren, yang dikenal sebagai pencetus hak privasi, menyampaikan dalam tulisan mereka yang berjudul "*The Right to Privacy*".[23] Brandeis dan Warren berpendapat bahwa privasi harus dihormati dan dijaga. Sebab dalam menjalin hubungan dengan orang lain, seseorang perlu menjaga

[23] *Ibid*

rahasia yang menjadi bagian dari kehidupan pribadinya, agar posisinya tetap pada taraf tertentu. Sebab untuk mewujudkan hal itu, seseorang membutuhkan waktu untuk dirinya sendiri. Sadarilah bahwa privasi sangat penting bagi individu.[24]

Perlindungan privasi merupakan hak yang independen dan tidak bergantung pada hak lainnya. Namun, hak ini akan habis jika seseorang mengungkapkan informasi pribadinya kepada publik. Privasi mencakup hak individu untuk menjalin hubungan keluarga, termasuk bagaimana mereka mengatur pernikahan dan keluarganya, dan tidak ingin orang lain mengetahui hubungan pribadi tersebut. Itu sebabnya Warren menyebutnya sebagai hukum yang menentang dunia. Karena dampaknya sulit diukur, privasi memerlukan perlindungan hukum. Kehilangan ini dianggap jauh lebih serius dibandingkan kehilangan fisik karena berdampak pada kehidupan pribadi. Oleh karena itu, jika terjadi kerugian maka korban berhak mendapatkan ganti rugi.[25]

Namun, hak privasi di sini tidak bersifat sembarangan, melainkan harus memiliki batasan agar tidak merugikan masyarakat. Edmon Makarim menjelaskan mengenai 3 aspek privasi yang terlindungi oleh hukum atau tidak, yaitu:

a. *Privacy of a Person's Persona*

[24] *Ibid*
[25] *Ibid*

Berdasarkan pandangan Willem dan Brandeis mengenai hak untuk privasi (*the right to be let alone*). Ada beberapa bentuk pelanggaran terhadap privasi ini, yaitu:

1. Menerbitkan gambar seseorang di media yang tidak pantas. Contohnya, menggunakan foto seorang pria untuk menggambarkan artikel tentang individu yang mengkonsumsi narkoba tanpa persetujuan pria tersebut.
2. Penggunaan yang salah terhadap nama atau preferensi seseorang untuk kepentingan bisnis.
3. Pengungkapan fakta-fakta yang memalukan di hadapan publik.
4. Mengganggu kesunyian atau kesendirian seseorang.

b. Privacy of data about a person

Hak privasi Anda mengenai informasi pribadi Anda yang dikumpulkan dan digunakan oleh orang lain. Contohnya mencakup kebiasaan pribadi, riwayat kesehatan, informasi pribadi, keanggotaan partai politik, catatan pajak, informasi karyawan, catatan asuransi, dan catatan kriminal. Segala penyalahgunaan data tersebut merupakan pelanggaran hak privasi.[26]

c. Pricvacy of a person's communication

[26] Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53. https://doi.org/10.26740/jsh.v3n1.p53-84

Perlindungan data dalam komunikasi adalah bagian dari hak asasi manusia. Kecuali diwajibkan lain oleh hukum, pemantauan, penyadapan, atau pengungkapan konten komunikasi (termasuk komunikasi elektronik) oleh orang lain merupakan pelanggaran privasi.

William L. Prosser menjelaskan ruang lingkup hak privasi individu dengan menyebutkan setidaknya empat bentuk pelanggaran privasi pribadi:

a. Menghancurkan keterasingan, kesepian, atau hubungan pribadi seseorang.
b. Publikasi fakta pribadi yang memalukan.
c. Iklan yang mengekspos seseorang secara tidak adil ke publik.
d. Kepemilikan gambar seseorang secara tidak sah untuk kepentingan orang lain.

2. Konsep Perlindungan Data Pribadi

Pasal 1 Angka 1 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik memberikan pengertian data pribadi yaitu data orang perseorangan yang disimpan. Itu dijaga sebagai kebenaran, dilindungi dan dirahasiakan. Informasi disebut data pribadi jika merupakan data pribadi tentang seseorang atau jika seseorang dapat diidentifikasi dari informasi tersebut. Misalnya,

Nomor Induk Kependudukan (NIK) Nasional yang tertulis di selembar kertas merupakan informasi. Namun lain halnya jika nomor ponsel berada di sebelah nama pemiliknya, karena merupakan informasi pribadi. kenapa begitu? Nomor ponsel yang tertulis di selembar kertas saja tidak memungkinkan kita untuk menarik kesimpulan apa pun tentang pemiliknya, namun akan terlihat berbeda bila nama pemiliknya tertulis di sebelahnya, itulah sebabnya kita menyebutnya data pribadi. Sangat penting bahwa undang-undang mengatur bahwa keamanan informasi pribadi tidak hanya didasarkan pada sifat informasi tersebut, tetapi juga pada keamanan informasi yang dapat mengidentifikasi pemiliknya.

Gagasan tentang perlindungan tersebar luas di banyak negara dan terutama didasarkan pada kerangka hukum dan pedoman yang berlaku bagi masyarakat, tetapi juga pada aturan yang tidak terucapkan (etika). Samuel Warren dan Louis Brandeis pertama kali mengajukan konsep perlindungan hak pada tahun 1980. Harvard Law Research menerbitkan sebuah pameran yang ditulis oleh Samuel dan Lewis berjudul "Hak atas Keamanan." Mereka menjelaskan bahwa mengakui hak seseorang untuk "dibiarkan sendirian" adalah masalah hak asasi manusia, sehingga Warren menolak gagasan bahwa keselamatan adalah hak setiap orang yang harus dijamin oleh hakim. Perlindungan data pribadi sangat penting

karena merupakan dasar harga diri individu dan ekspresi pendapat.[27] Anggapan Warren dan Brandies ditanggapi oleh Berzanson bahwa hak atas keamanan atas informasi pribadi digunakan sebagai konsep hukum dalam suatu praktik untuk menghargai hak seseorang untuk dapat menikmati hidupnya sesuai dengan hak yang dimilikinya. Keamanan perlindungan atas informasi individu apabila tidak diamankan, apabila penyebaran data individu seseorang dapat menimbulkan kerugian baik yang material maupun yang tidak penting.

Inovasi data telah tercipta begitu cepat sehingga memiliki dampak kritis pada kehidupan sosial. Kantor-kantor yang diiklankan oleh teknologi data berkontribusi pada kecepatan jaringan web. Bersamaan dengan itu, keterbukaan dorongan inovatif menimbulkan isu seputar hak orang untuk menjaga privasi beberapa data.[28] Melalui dorongan inovatif, penyebaran data yang sederhana dan cepat telah menciptakan risiko terhadap keamanan dengan memberikan peluang luar biasa bagi mereka yang memiliki akses ke data individu. Dengan cara ini, data telah melahirkan etika modern bahwa setiap pihak yang memiliki data berisi ruang yang terus-menerus tersebar ke pihak lain.

[27] Dewi, S. (2016). Op.cit, hlm. 25-26.

[28] Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1), 22–30. https://doi.org/10.20961/yustisia.v5i1.8712 Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 239–249. https://doi.org/10.29303/jtsw.v34i3.218.

Sebagai suatu kerangka kemajuan, inovasi data kini mampu mengumpulkan, menyimpan, membagi, dan menganalisa informasi dengan cara yang sebelumnya tidak terbayangkan, sehingga lahirlah hak keamanan untuk menciptakan hak guna menjamin informasi perorangan, sebagaimana tertuang dalam Pasal 17 *Human Rights Committee General Commnt No. 16 on the Rights to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation.*

Konsep jaminan informasi menyatakan bahwa orang memiliki hak untuk memutuskan apakah mereka akan bergabung dengan komunitas dan setelah itu berbagi atau memperdagangkan informasi pribadi di antara mereka dan hak untuk memutuskan kondisi apa yang harus dipenuhi untuk melakukannya.[29] Hukum keamanan informasi pada umumnya juga menggabungkan langkah-langkah keamanan untuk melindungi keamanan data pribadi dan mengizinkan penggunaannya oleh orang lain selama sesuai dengan kondisi yang diperlukan.

Beberapa negara telah lebih mengontrol standar keamanan informasi dan banyak arahan nasional juga telah memasukkannya sebagai bagian dari hukum nasional. Beberapa contohnya adalah :

[29] Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1), 22–30. https://doi.org/10.20961/yustisia.v5i1.8712 Priscyllia, F. (2019). Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum. *Jatiswara*, *34*(3), 239–249. https://doi.org/10.29303/jtsw.v34i3.218.

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; *the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* (1980); *and the Guidelines for the regulation of computerized personal data files* (*General Assembly resolution* 45/95 *and* E/CN.4/1990/72). Jaminan informasi juga merupakan hak asasi manusia yang penting. Pernyataan Hak Asasi Manusia ASEAN yang baru-baru ini dianut oleh negara-negara ASEAN juga dengan jelas mengakui kebenaran perlindungan informasi dalam Pasal 21. Setidaknya ada lebih dari 75 negara yang hukumnya mengarahkan jaminan informasi.[30]

Beberapa negara memiliki undang-undang khusus yang menjamin keamanan dan informasi pribadi warga negaranya. Hal ini khususnya berlaku di negara-negara Eropa dan Amerika Serikat, yang memiliki undang-undang khusus yang menjamin keamanan dan informasi pribadi. Namun, konsep keamanan di Eropa dan Amerika Serikat memiliki karakteristik yang khas. Amerika Serikat tidak memiliki kendali tunggal untuk mengamankan perlindungan dan informasi yang dapat dikaitkan secara khusus. Sementara itu, di dalam Uni Eropa karena merupakan koordinat lokal Eropa, keamanan perlindungan dan informasi pribadi diatur oleh

[30] Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2018). Op.cit, hlm. 492.

pengaturan supranasional dalam kerangka *the EU Data Protection Directive*.

Konsep dasar jaminan informasi individu pertama kali muncul sekitar tahun 1960. Kemudian pada tahun 1970, Jerman adalah negara pertama yang memerintahkan arahan keamanan informasi yang kemudian diikuti oleh undang-undang nasional Swedia pada tahun 1973, Amerika Serikat pada tahun 1974, dan Prancis pada tahun 1978. Konsep keamanan informasi pada dasarnya dapat dikaitkan khususnya dengan privasi, dan pemikiran itu sendiri dapat dikaitkan dalam kategori perlindungan yang lebih luas. Melihat perlindungan data sebagai bagian dari keamanan konsisten dengan pemahaman bahwa perlindungan dapat menjadi kerangka privasi, atau hak untuk membatasi atau menutup data, atau hak untuk membatasi akses individu, atau mengendalikan data yang terkait dengan diri sendiri.[31] Namun, ada perbedaan penting dalam hal ruang lingkup, alasan, dan substansi perlindungan dan jaminan informasi. Keamanan informasi secara tegas mengamankan nilai-nilai yang tidak menjadi inti dari perlindungan seperti perlunya pelatihan yang wajar, persetujuan, keaslian, dan non-diskriminasi. Ungkapan konsep perlindungan informasi erat kaitannya dengan

[31] Sasongko, Dwipayana, D. P., Jumangin, & Roselawati, C. P. (2020). Konsep Perlindungan Hukum Data Pribadi dan Sanksi Hukum atas Penyalahgunaan Data Pribadi oleh Pihak Ketiga. *Proceeding of Conference on Law and Social Studies*, *1*(2), 16–27. http://prosiding.unipma.ac.id/index.php/COLaS%0Ahttp://prosiding.unipma.ac.id/Index.Php/COLaS%0Ahttp://prosiding.unipma.ac.id/index.php/COLaS.

hak untuk menghargai kehidupan pribadi dan keluarga.[32] Konsep jaminan informasi merupakan kunci dari masalah perdagangan dan keuangan dalam bidang data perdagangan di masa kini. Praktik bisnis canggih saat ini sering kali mencakup pengendalian informasi seperti pembagian informasi klien, penghitungan pengumpulan informasi dan penggalian informasi, pembuatan profil klien, pemantapan penanganan informasi global, dan bentuk-bentuk perdagangan lainnya.[33]

3. Pentingnya Perlindungan Data Pribadi

Mengingat banyaknya insiden penyalahgunaan data pribadi, sangat penting untuk memastikan bahwa data pribadi dilindungi. Seiring dengan meningkatnya jumlah pengguna ponsel dan internet, pentingnya melindungi data pribadi pun meningkat. Sejumlah insiden, terutama yang berkaitan dengan pengungkapan data pribadi individu yang berujung pada penipuan dan kejahatan pornografi, telah memperkuat perdebatan tentang pentingnya memiliki peraturan hukum untuk melindungi data pribadi. Perlindungan data pribadi berkaitan dengan konsep privasi. Konsep privasi sendiri merupakan gagasan untuk menjaga integritas dan martabat pribadi. Hak atas privasi juga berarti bahwa individu dapat memilih siapa

[32] Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. Jurnal Yustisia, 5 (1) Januari - April 2016.
[33] Ibid.

yang mempunyai informasi tentang dirinya dan bagaimana informasi tersebut digunakan.

Konsep perlindungan data berarti bahwa individu mempunyai hak untuk memutuskan apakah akan membagikan atau menukar informasi pribadinya.[34] Selain itu, individu juga mempunyai hak untuk menentukan kondisi di mana transfer data pribadi mereka terjadi. Selain itu, ini juga membantu melindungi privasi Anda. Hak atas privasi telah berkembang dan kini dapat digunakan untuk merumuskan hak untuk melindungi data pribadi.

Perlindungan data pribadi diatur oleh Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Pasal 28G ayat (1) menyatakan: Data tersebut juga dikaitkan dengan konsep hak keluarga, kehormatan, martabat dan harta benda yang dimilikinya. Lebih lanjut, setiap orang berhak merasa aman dan terlindungi dari ancaman dan ketakutan untuk melakukan atau tidak melakukan sesuatu. Ini adalah hak asasi manusia yang mendasar.

Selain itu, beberapa peraturan nasional telah dikeluarkan untuk melindungi data pribadi, termasuk:

a. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Dalam Undang-Undang

[34] Rahmatullah, I. (2021). Pentingnya Perlindungan Data Pribadi Dalam Masa Pandemi Covid-19 Di Indonesia. *Adalah*, *5*(1), 11–20. https://doi.org/10.15408/adalah.v5i1.19811.

ini negara bertanggung jawab melindungi kepentingan umum dari penyalahgunaan informasi elektronik dan transaksi elektronik serta mencegah kebocoran data melalui keamanan siber. Pemerintah melalui *Kementerian Komunikasi dan Informatika (Kominfo)* memiliki peran untuk mengawasi penyelenggara sistem elektronik. Beberapa kelemahan UU ITE: a) UU ITE tidak secara spesifik mengatur prinsip-prinsip perlindungan data pribadi seperti transparansi, akuntabilitas, atau keamanan yang ketat, b) Tidak ada pengawasan independen yang memastikan kepatuhan penyelenggara sistem elektronik, c) Sanksi administratif masih minim dan tidak memiliki efek jera yang kuat).

b. Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan (Dalam Undang-Undang ini negara wajib menjamin pengelolaan arsip yang berisi data pribadi dalam lingkup lembaga negara dan swasta, serta memastikan perlindungan arsip rahasia. Beberapa kelemahan UU ini: a) Tidak mengatur spesifik mengenai kebocoran arsip digital dalam konteks teknologi informasi, dan b) Tidak adanya mekanisme pemulihan atau sanksi bagi kebocoran arsip yang mengandung data pribadi).

c. Undang-Undang Nomor 56 Tahun 1999 Tentang Rakyat Terlatih (Dalam undang-undang ini negara bertanggung jawab terhadap pengelolaan data rakyat terlatih, termasuk menjaga kerahasiaan identitas mereka. Beberapa kelemahan UU ini: a) Regulasi ini tidak relevan secara langsung dengan perlindungan data pribadi digital, dan b) Tidak ada mekanisme keamanan khusus atau akuntabilitas jika terjadi kebocoran data).

d. Undang-Undang Nomor 24 Tahun 2013 Tentang Revisi Administrasi Kependudukan (Dalam Undang-Undang ini negara wajib melindungi data pribadi warga, seperti Nomor Induk Kependudukan (NIK), alamat, dan data keluarga. Hal ini diwujudkan melalui *Dukcapil*. Beberapa kelemahan UU ini: a) Praktik pengelolaan data masih rentan kebocoran, terutama dalam integrasi sistem administrasi kependudukan dengan layanan publik lainnya, b) Tidak ada sanksi tegas bagi petugas atau pihak ketiga yang lalai).

e. Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan (Dalam undang-undang ini Negara berkewajiban menjaga kerahasiaan data kesehatan pasien. Fasilitas layanan kesehatan bertanggung jawab atas penyimpanan dan pemrosesan data tersebut. Beberapa kelemahan dalam UU ini: a) Pengaturan perlindungan data kesehatan belum

terintegrasi dengan keamanan sistem elektronik, dan b) Lemahnya pengawasan terhadap lembaga kesehatan dalam pengelolaan data).

f. Undang-Undang Nomor 11 Tahun 2012 Tentang Sistem Peradilan Pidana Anak (Dalam undang-undang ini negara wajib melindungi data anak dalam sistem peradilan pidana. Data anak tidak boleh dipublikasikan demi kepentingan pemulihan anak. Kelemahan dalam undang-undang ini adalah fokus perlindungan hanya mencakup data anak di ranah peradilan, belum mengakomodasi perlindungan dalam sistem elektronik yang terintegrasi).

g. Undang-Undang Nomor 3 Tahun 1997 Tentang Pengadilan Anak (Dalam undang-undang ini negara berkewajiban melindungi identitas dan data pribadi anak yang berhadapan dengan hukum dalam proses peradilan. Identitas anak harus dirahasiakan untuk melindungi hak dan martabatnya. Kelemahan dalam undang-undang ini adalah UU ini hanya mencakup perlindungan identitas anak di ruang peradilan, belum spesifik mengatur perlindungan data pribadi anak dalam sistem elektronik atau media digital dan Belum ada mekanisme pengawasan dan sanksi tegas bagi pihak yang melanggar kerahasiaan data anak).

h. Undang-Undang Nomor 10 Tahun 2011 Tentang Perubahan Atas Undang-Undang Nomor 32 Tahun 2007 Tentang Perdagangan Berjangka Komoditi (Dalam undang-undang ini negara bertanggung jawab memastikan keamanan data dalam perdagangan berjangka komoditi. Kelemahan dalam undang-undang ini adalah fokus regulasinya hanya pada aspek ekonomi dan bisnis, tidak secara spesifik melindungi data pribadi pelaku transaksi digital).

i. Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (Dalam undang-undang ini negara memiliki tanggung jawab melindungi data kependudukan warga negara seperti NIK, kartu keluarga, akta kelahiran, dan data lainnya melalui *Dinas Kependudukan dan Pencatatan Sipil (Dukcapil)*. Kelemahan dalam undang-undang ini adalah UU ini masih berfokus pada pengelolaan data administratif secara konvensional dan kurang responsif terhadap ancaman kebocoran data di era digital dan Tidak ada mekanisme perlindungan data secara spesifik ketika data kependudukan terintegrasi dengan sistem elektronik).

j. Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Dalam undang-undang ini pemerintah

bertanggung jawab memastikan penyelenggara sistem elektronik melindungi data pribadi pengguna dan melaporkan kebocoran data dalam waktu 14 hari. Kelemahan dalam undang-undang ini adalah Tidak ada sanksi tegas bagi penyelenggara yang lalai melaporkan kebocoran data dan Prosedur pemulihan kebocoran data masih lemah dan tidak efektif).

k. Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Dalam undang-undang ini negara bertanggung jawab memastikan keamanan sistem elektronik dalam transaksi digital. Kelemahan dalam undang-undang ini adalah regulasi yang lebih fokus pada aspek penyelenggaraan sistem elektronik secara umum daripada spesifik melindungi data pribadi).

l. Peraturan Menteri Komunikasi dan Informasi Nomor 11 Tahun 2016 Tentang Klasifikasi Permainan Interaktif Elektronik (Dalam undang-undang ini Pemerintah bertanggung jawab menetapkan klasifikasi permainan elektronik untuk memastikan keamanan informasi dan melindungi data pengguna, terutama anak-anak. Kelemahan dalam undang-undang ini adalah Fokus utama regulasi adalah pada klasifikasi konten permainan, bukan pada perlindungan data pribadi pengguna dan belum ada

mekanisme pengawasan yang memadai terkait bagaimana penyelenggara permainan elektronik melindungi data pribadi pengguna).

m. Peraturan Menteri Komunikasi dan Informasi Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengaman Informasi (Dalam undang-undang ini negara bertanggung jawab memastikan penyelenggara sistem elektronik menerapkan standar manajemen keamanan informasi untuk mencegah kebocoran data pribadi. Kelemahan dalam undang-undang ini adalah Rregulasi yang masih bersifat teknis dan berfokus pada aspek keamanan sistem, tanpa pengaturan spesifik mengenai hak pengguna dan tanggung jawab pengendali data pribadi dan implementasi standar keamanan informasi belum diawasi secara ketat dan seragam di berbagai sektor).

n. Peraturan Menteri Komunikasi dan Informasi Nomor 36 Tahun 2014 Tentang Tata Cara Pendaftaran Penyelenggara Sistem Elektronik (Dalam undang-undang ini negara bertanggung jawab mengatur pendaftaran penyelenggara sistem elektronik agar dapat diawasi dalam pengelolaan data pengguna. Kelemahan dalam undang-undang ini adalah regulasi yang lebih berfokus pada aspek administratif pendaftaran penyelenggara sistem elektronik, bukan pada

mekanisme perlindungan data pribadi pengguna dan tidak ada kewajiban audit atau evaluasi berkala terkait keamanan data yang dikelola penyelenggara sistem elektronik).

o. Peraturan Menteri Komunikasi dan Informasi Nomor 11 Tahun 2010 Tentang Penyelenggaraan Layanan Televisi Protokol Internet (Internet Protocol Television / IPTV). (Dalam undang-undang ini negara bertanggung jawab memastikan penyelenggara layanan IPTV melindungi data pribadi pengguna layanan televisi berbasis internet. Kelemahan dalam undang-undang ini adalah regulasi yang lebih menekankan aspek teknis penyelenggaraan layanan IPTV dan belum mengatur secara khusus perlindungan data pribadi pengguna layanan dan tidak ada sanksi tegas bagi penyelenggara IPTV yang lalai dalam melindungi data pribadi).

Berdasarkan beberapa peraturan diatas evaluasi terhadap peraturan-peraturan tersebut adalah tidak adanya keseragaman dalam mengatur perlindungan data pribadi, mengakibatkan tumpang-tindih aturan, banyak regulasi yang belum memiliki sanksi tegas atau mekanisme pengawasan yang efektif, tidak ada badan independen khusus yang bertugas memastikan kepatuhan terhadap aturan perlindungan data pribadi, sistem keamanan siber di sektor

publik masih lemah dan rentan terhadap serangan, dan regulasi di Indonesia belum mencapai standar perlindungan seperti *GDPR* di Uni Eropa yang lebih komprehensif). Tanggung jawab negara dalam perlindungan data pribadi diatur dalam berbagai regulasi nasional, namun implementasinya masih lemah dan tidak efektif. Diperlukan harmonisasi peraturan, pembentukan lembaga pengawas independen, serta penerapan sanksi yang lebih tegas untuk memastikan perlindungan data pribadi yang lebih optimal di Indonesia.

Badan Jasa Keuangan juga menerbitkan Peraturan OJK Nomor 77/POJK.01/2016 tentang Pelayanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Pasal 26 huruf a mengatur bahwa kerahasiaan, integritas, dan ketersediaan data pribadi, transaksional, dan keuangan yang dikendalikan harus dijaga sejak saat diterima hingga dimusnahkan. Selain itu, Peraturan OJK Nomor 13 Tahun 2018 tentang Inovasi Keuangan Digital di Sektor Keuangan memuat hal-hal mengenai perlindungan dan kerahasiaan data. Pasal 30 ayat (1) mengatur bahwa Penyelenggara berkewajiban menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi,

transaksi, dan keuangan yang dikuasainya sejak diterima hingga dimusnahkan.[35]

Banyaknya peraturan mengenai perlindungan data pribadi menunjukkan betapa pentingnya melindungi data pribadi. Sayangnya, aturan tersebut masih tersebar di berbagai peraturan, sehingga belum memberikan perlindungan yang optimal dan efektif terhadap data pribadi sebagai bagian dari privasi. Oleh karena itu, perlu dikembangkan undang-undang yang secara khusus menjamin perlindungan data pribadi.

B. Tinjauan Umum tentang Tanggung Jawab Negara dalam Perlindungan Data Pribadi

1. Peran dan Tanggung Jawab Negara

Dalam era digital, data pribadi menjadi komoditas yang sangat bernilai, tetapi rentan terhadap penyalahgunaan. Tanggung jawab negara dalam melindungi data pribadi warganya mencakup penyediaan regulasi, pengawasan, dan penegakan hukum yang memadai untuk menjamin keamanan data pribadi dari pelanggaran dan penyalahgunaan. Negara berperan sebagai penjamin hak privasi warga negara dalam interaksi digital, serta sebagai pengawas untuk memastikan penyelenggara sistem informasi, baik sektor publik maupun swasta, menjalankan kewajiban mereka dalam

[35] Aryani, A. P., & Susanti, L. E. (2022). Pentingnya Perlindungan Data Pribadi Konsumen dalam Transaksi Online pada Marketplace terhadap Kepuasan Konsumen. *Ahmad Dahlan Legal Perspective*, *2*(1), 20–29. https://doi.org/10.12928/adlp.v2i1.5610.

perlindungan data pribadi.[36] Dalam hal ini, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir sebagai regulasi utama di Indonesia yang mengatur kewajiban dan tanggung jawab negara dalam menjamin perlindungan data pribadi.

Peran negara dalam perlindungan data pribadi mencakup berbagai aspek, termasuk pembuatan regulasi yang melindungi privasi individu, pengembangan infrastruktur keamanan siber, dan penegakan hukum atas pelanggaran privasi. Dalam UU PDP, negara memiliki kewajiban untuk memberikan perlindungan data yang optimal dan berstandar internasional, yang bertujuan untuk menciptakan kepercayaan masyarakat terhadap penggunaan data pribadi dalam sistem elektronik.[37] Berdasarkan teori hukum privasi, perlindungan data pribadi adalah bagian dari hak asasi manusia yang harus dijamin oleh negara. Dalam *General Data Protection Regulation* (GDPR) yang berlaku di Uni Eropa, misalnya, negara bertanggung jawab atas perlindungan data pribadi melalui standar-standar yang ketat mengenai pengelolaan data, hak-hak pemilik data, dan kewajiban penyelenggara data. Meskipun belum sepenuhnya mengadopsi prinsip GDPR, Indonesia berusaha

[36] Kusumaningrum, R. (2021). *Perlindungan Hak Privasi di Era Digital.* Jakarta: PT Pustaka Rakyat.
[37] Hasibuan, A. (2022). *Undang-Undang Perlindungan Data Pribadi dan Implementasinya di Indonesia.* Jakarta: Pustaka Ilmu.

mengembangkan kebijakan yang serupa untuk menciptakan standar perlindungan data pribadi yang lebih baik.[38]

UU PDP juga mengamanatkan agar negara memiliki sistem pemantauan dan penegakan hukum yang tegas terhadap pihak-pihak yang melanggar perlindungan data pribadi. Dalam pelaksanaannya, penegakan hukum menjadi tanggung jawab pemerintah, yang mencakup penyediaan sumber daya manusia dan teknologi yang memadai untuk melindungi data pribadi di ruang digital. Hal ini sejalan dengan peran negara sebagai pengatur dan pengawas untuk memastikan bahwa penyelenggara sistem elektronik (PSE) mematuhi aturan yang berlaku dan menjaga keamanan data pribadi dengan menerapkan langkah-langkah teknis yang memadai.[39] Negara bertindak sebagai pengawas yang harus memastikan bahwa penyelenggara sistem memiliki kebijakan yang transparan dalam pengelolaan data pribadi, sesuai dengan asas transparansi dan akuntabilitas yang terkandung dalam UU PDP.[40]

Kesimpulannya, tanggung jawab negara dalam perlindungan data pribadi mencakup penyusunan aturan hukum yang rinci, penerapan sanksi tegas untuk pelanggaran, dan komitmen untuk

[38] Rinaldi, Y. (2022). *Perbandingan Perlindungan Data Pribadi di Indonesia dan Uni Eropa.* Jakarta: PT Gramedia.
[39] Priyanto, H. (2023). *Kebijakan Negara dalam Perlindungan Data Pribadi.* Jakarta: Kencana.
[40] Amin, S. (2023). *Sanksi dan Penegakan Hukum dalam UU Perlindungan Data Pribadi.* Bandung: PT Refika Aditama.

melindungi hak-hak data pribadi sebagai bagian dari hak privasi individu.

2. Dasar Hukum yang Mengatur Tanggung Jawab Negara

Tanggung jawab negara dalam melindungi data pribadi telah diatur dalam berbagai instrumen hukum baik nasional maupun internasional. Di tingkat nasional, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) merupakan landasan hukum utama yang mengatur perlindungan data pribadi di Indonesia. UU PDP memberikan kerangka bagi perlindungan data yang mengikat pemerintah, penyelenggara sistem elektronik, dan pihak lainnya untuk memastikan bahwa data pribadi individu tidak disalahgunakan. Sebagaimana dinyatakan oleh Hasibuan, "UU PDP mencerminkan komitmen pemerintah untuk menjadikan perlindungan data pribadi sebagai salah satu prioritas dalam era digital yang penuh tantangan." UU PDP ini mengatur aspek-aspek penting seperti prinsip-prinsip dasar perlindungan data, hak-hak subjek data, dan kewajiban penyelenggara data.

Lebih lanjut, dasar hukum yang mendukung perlindungan data pribadi juga terdapat dalam Undang-Undang Dasar 1945, khususnya Pasal 28G ayat (1) yang menyebutkan bahwa "setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya." Ketentuan ini memberikan dasar konstitusional yang kuat bagi

perlindungan privasi sebagai hak asasi manusia. Selain itu, pasal ini juga mendasari adanya kewajiban negara untuk memastikan keamanan dan perlindungan data pribadi bagi setiap warga negara.

Di tingkat internasional, beberapa perjanjian seperti *Universal Declaration of Human Rights* (UDHR) dan *International Covenant on Civil and Political Rights* (ICCPR) juga menetapkan hak atas privasi sebagai hak yang harus dihormati oleh negara-negara anggota.[41] Misalnya, Pasal 17 ICCPR menyebutkan bahwa "tidak seorang pun boleh menjadi sasaran gangguan sewenang-wenang atau tidak sah atas privasi, keluarga, rumah, atau korespondensinya." Dengan demikian, Indonesia sebagai negara yang meratifikasi ICCPR memiliki kewajiban untuk menghormati dan melindungi hak privasi, termasuk data pribadi.

Selain itu, standar perlindungan data pribadi global seperti *General Data Protection Regulation* (GDPR) di Uni Eropa juga memberikan pengaruh terhadap penyusunan UU PDP di Indonesia. GDPR menetapkan standar perlindungan data yang ketat, terutama dalam hal prinsip-prinsip pemrosesan data dan hak-hak subjek data. Sebagaimana yang telah dijelaskan, “GDPR menjadi inspirasi bagi banyak negara, termasuk Indonesia, dalam menyusun regulasi perlindungan data pribadi karena standar yang ditetapkannya

[41] Saputra, W. (2023). The Right to Privacy: Tinjauan terhadap Penyalahgunaan Data Pribadi dalam Perspektif HAM. *Res Judicata*, *6*(2), 128. https://doi.org/10.29406/rj.v6i2.6145

mengacu pada transparansi, akuntabilitas, dan perlindungan hak-hak subjek data." Hal ini mencerminkan bahwa Indonesia berupaya untuk membangun standar hukum yang setara dengan negara-negara maju dalam hal perlindungan data pribadi.[42]

Dalam implementasi UU PDP, negara tidak hanya berkewajiban dalam membuat regulasi tetapi juga menjamin pelaksanaannya. Literasi digital yang ditingkatkan untuk masyarakat dan pengawasan terhadap kepatuhan penyelenggara sistem informasi adalah bagian dari upaya negara untuk mematuhi tanggung jawabnya. Tanpa pengawasan dan penegakan hukum yang efektif, regulasi tidak akan memberikan perlindungan nyata bagi warga negara.

3. Kewajiban Negara dalam Melindungi Hak Privasi

Kewajiban negara dalam melindungi hak privasi warga negara merupakan tanggung jawab konstitusional yang harus dijalankan secara efektif di era digital ini. Menurut Pasal 28G Undang-Undang Dasar 1945, setiap warga negara berhak atas rasa aman dan perlindungan terhadap privasi, termasuk dalam hal data pribadi. Hak ini menjadi dasar bagi pemerintah untuk merancang regulasi yang menjamin bahwa data pribadi tidak disalahgunakan oleh pihak yang tidak berwenang. Di tingkat internasional, hak

[42] HUKUMONLINE.COM. 12 Agustus 2019. Ini 4 Perbedaan GDPR dan Perlindungan Data Pribadi di Indonesia. Diakses pada 3 November 2024, dari https://www.hukumonline.com/berita/a/ini-4-perbedaan-gdpr-dan-perlindungan-data-pribadi-di-indonesia-lt5d513741ccedd.

privasi juga diakui dalam *Universal Declaration of Human Rights* (UDHR) dan *International Covenant on Civil and Political Rights* (ICCPR), yang menggarisbawahi pentingnya perlindungan privasi sebagai hak asasi manusia.[43]

Negara diwajibkan untuk membentuk kebijakan yang efektif untuk melindungi data pribadi sebagai bentuk perlindungan hak privasi. Kewajiban ini mencakup pembentukan undang-undang yang mengatur aspek-aspek perlindungan data pribadi secara komprehensif dan pengembangan mekanisme penegakan hukum yang efektif.[44] Undang-Undang Perlindungan Data Pribadi, misalnya, telah mewajibkan negara untuk menyediakan infrastruktur dan sistem pemantauan yang memungkinkan perlindungan data pribadi dalam setiap proses elektronik yang melibatkan pengumpulan dan pemrosesan data. Implementasi yang baik dari regulasi ini menjadi bukti kewajiban negara untuk menghormati dan melindungi hak privasi warganya.[45]

Selain itu, negara juga harus memastikan adanya edukasi dan literasi kepada masyarakat mengenai pentingnya menjaga data pribadi dan hak privasi mereka. Literasi masyarakat menjadi aspek penting untuk mengurangi risiko penyalahgunaan data pribadi, serta

[43] Sardjono, A. (2019). *Hak Asasi Manusia dan Hukum Perlindungan Data Pribadi.* Yogyakarta: Deepublish.
[44] Zainal, F. (2022). *Hak Privasi dan Perlindungan Data Pribadi.* Bandung: PT Refika Aditama.
[45] Marbun, D. (2022). *Infrastruktur Keamanan Siber untuk Perlindungan Data Pribadi.* Jakarta: Gramedia Pustaka Utama.

mendorong transparansi dalam pengelolaan data oleh penyelenggara sistem informasi.[46]

C. Pengertian Pelanggaran Perlindungan Data Pribadi dan Implikasinya

1. Jenis-Jenis Pelanggaran Perlindungan Data Pribadi

Pelanggaran perlindungan data pribadi merujuk pada setiap tindakan yang melibatkan akses, pengungkapan, atau penggunaan data pribadi secara tidak sah dan tidak sesuai dengan ketentuan hukum yang berlaku.[47] Menurut Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pelanggaran terhadap data pribadi mencakup pengumpulan, pemrosesan, penyimpanan, serta penyebaran data pribadi tanpa persetujuan dari subjek data. Pelanggaran ini dapat menyebabkan hilangnya hak privasi individu dan berpotensi merugikan subjek data dalam berbagai aspek kehidupan mereka.

Jenis-jenis pelanggaran perlindungan data pribadi dapat diklasifikasikan sebagai berikut:[48]

a. *Unauthorized Access* (Akses Tanpa Izin)
   Unauthorized access terjadi ketika data pribadi diakses oleh pihak yang tidak memiliki otoritas. UU ITE (Undang-Undang

[46] Mulyani, R. (2023). *Analisis Yuridis UU PDP dan Implikasinya terhadap Perlindungan Data Pribadi.* Jakarta: Kencana.
[47] Niffari, H. (2020). PERLINDUNGAN DATA PRIBADI SEBAGAI BAGIAN DARI HAK ASASI MANUSIA ATAS PERLINDUNGAN DIRI PRIBADI Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain. *Jurnal Hukum Dan Bisnis (Selisik)*, *6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699.
[48] Seminar, P., Fh, N., & Denpasar, U. (n.d.). *Prosiding seminar nasional fh unmas denpasar*. 119–134.

No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik) dan revisinya, UU No. 19 Tahun 2016 menegaskan bahwa akses tanpa izin terhadap data pribadi merupakan bentuk pelanggaran hukum dan dapat dikenakan sanksi pidana. Sebagai contoh, hacking atau peretasan yang menyebabkan data pengguna tersebar merupakan tindakan akses tanpa izin.

b. *Improper Data Disposal* (Pemusnahan Data yang Tidak Tepat) Pemusnahan data yang tidak tepat terjadi ketika data pribadi yang seharusnya dimusnahkan malah digunakan atau diakses kembali oleh pihak tertentu. UU PDP mengatur bahwa pemusnahan data pribadi harus dilakukan sesuai prosedur agar data tersebut tidak dapat diakses lagi oleh pihak mana pun. Menurut Suprapto (2022), pelanggaran ini sering kali terjadi akibat kurangnya kesadaran akan pentingnya keamanan dalam pemusnahan data.

c. *Unauthorized Disclosure* (Pengungkapan Tanpa Izin) Pengungkapan data tanpa izin merujuk pada situasi ketika data pribadi disebarluaskan ke publik atau ke pihak ketiga tanpa persetujuan dari pemilik data. Hal ini juga termasuk dalam pelanggaran berat menurut UU PDP. Pengungkapan data tanpa izin sering kali ditemukan dalam kasus penyebaran data pribadi di media sosial tanpa seizin pemilik data, yang dikenal juga sebagai praktik *doxing*.

2. Dampak dari Pelanggaran Perlindungan Data Pribadi

Pelanggaran terhadap data pribadi memiliki implikasi yang luas dan berpotensi menimbulkan kerugian signifikan bagi individu maupun masyarakat. Berikut beberapa dampak dari pelanggaran perlindungan data pribadi:[49]

a. Kerugian Finansial

Pelanggaran data pribadi dapat menimbulkan kerugian finansial langsung maupun tidak langsung. Misalnya, kebocoran informasi perbankan seperti nomor rekening atau informasi kartu kredit bisa menyebabkan kerugian finansial pada individu akibat pencurian identitas atau penipuan. Menurut UU PDP, kerugian finansial akibat pelanggaran data harus ditanggung oleh pihak yang melakukan pelanggaran, khususnya jika mereka adalah penyelenggara sistem elektronik.

b. Kerugian Psikologis dan Sosial

Selain kerugian finansial, pelanggaran data pribadi juga menimbulkan dampak psikologis, seperti stres dan rasa tidak aman. Pengungkapan data pribadi di ruang publik, seperti yang terjadi pada kasus *doxing*, sering kali menyebabkan tekanan psikologis yang mendalam pada korban. Menurut Kartika (2022), dampak psikologis dari pelanggaran data pribadi ini

[49] Yitawati, K., Sarjiyati, Purwati, Y., & Sukarjono, B. (2022). Implikasi Dan Sosialisasi Undang-Undang Tentang Perlindungan Data Pribadi Dalam Menjaga Kerahasiaan Data Pribadi Seseorang. *Jurnal Daya-Mas*, *7*(2), 90–95. https://doi.org/10.33319/dymas.v7i2.92.

dapat mengakibatkan rasa malu, cemas, bahkan depresi, terutama jika data yang terungkap bersifat sensitif.

c. Kerugian Reputasi

Pelanggaran data dapat merusak reputasi individu maupun organisasi. Bagi perusahaan, kehilangan data pelanggan dapat menurunkan tingkat kepercayaan publik terhadap layanan mereka. Di sisi lain, individu yang data pribadinya tersebar di publik mungkin mengalami kerugian reputasi akibat informasi tersebut disalahgunakan oleh pihak ketiga. UU PDP mengharuskan penyelenggara sistem untuk mengambil langkah-langkah keamanan guna menjaga reputasi dan kepercayaan dari para pengguna.

d. Risiko Pelanggaran Lebih Lanjut (*Secondary Violations*)

Data pribadi yang bocor sering kali dimanfaatkan oleh pihak lain untuk kejahatan lanjutan, seperti penipuan atau pencurian identitas. Data yang telah terekspos di internet dapat dengan mudah disalahgunakan untuk kejahatan siber lainnya, yang menyebabkan dampak lanjutan bagi korban. UU PDP dan UU ITE berupaya untuk mengurangi risiko pelanggaran lanjutan dengan memberlakukan sanksi tegas bagi pelaku pelanggaran.

Menurut UU No. 27 Tahun 2022, pelanggaran perlindungan data pribadi merupakan pelanggaran serius yang memerlukan tindakan hukum yang ketat untuk mencegah

dampak negatif yang lebih luas. Pelanggaran data juga melibatkan aspek etika dan moral, di mana semua pihak yang memiliki akses terhadap data pribadi diharapkan mampu menjaga kepercayaan yang diberikan oleh subjek data.

D. Perlindungan Hukum terhadap Data Pribadi di Indonesia

1. Prinsip-Prinsip Perlindungan Hukum terhadap Data Pribadi

Prinsip perlindungan data pribadi tertuang dalam ketentuan turunan UU ITE dan perubahannya yang secara khusus mengatur tentang perlindungan data pribadi. Khususnya Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Menteri Komunikasi dan Informatika. Perlindungan data pribadi dalam sistem elektronik (Permenkominfo No. 20 Tahun 2016). Perlindungan data pribadi dalam sistem elektronik mencakup perlindungan terhadap pengambilan data, pengumpulan data, pemrosesan data, analisis data, penyimpanan data, tampilan, pengungkapan, publikasi, distribusi, dan pemusnahan data pribadi. Penerapan ketentuan ini harus didasarkan pada prinsip perlindungan data pribadi yang memadai. Ini termasuk:[50]

a. Kami menghormati data pribadi sebagai privasi.

[50] Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

b. Data pribadi akan dijaga kerahasiaannya berdasarkan kontrak dan/atau sebagaimana diwajibkan oleh hukum atau peraturan.
c. Berdasarkan persetujuan;
d. Relevansi dengan tujuan dikumpulkan, dikumpulkan, diproses, dianalisis, disimpan, ditampilkan, diterbitkan, ditransmisikan, dan didistribusikan.
e. Kelayakan sistem elektronik yang digunakan.
f. dan seterusnya, jika terjadi pelanggaran terhadap perlindungan data pribadi, dengan itikad baik kami akan segera memberi tahu pemilik data pribadi secara tertulis.
g. Ketersediaan aturan internal yang mengatur perlindungan data pribadi.
h. Tanggung jawab atas data pribadi di bawah kendali Anda.
i. Kemudahan akses dan koreksi data pribadi oleh pemilik data pribadi. dan
j. Kelengkapan, keakuratan, keabsahan dan ketepatan waktu data pribadi.[51]

Segala aktivitas yang terkait dengan pemrosesan, pengelolaan, penggunaan, dan penyebaran data pribadi harus mematuhi prinsip-prinsip yang diatur dalam Kerangka Privasi APEC. Dengan kata lain: Data pribadi harus dikumpulkan, disimpan, diproses atau digunakan

[51] 7 Pasal 2 ayat (2) Perkominfo 20 Tahun 2016.

secara wajar dan sah. Apakah data pribadi dikumpulkan secara sah dapat ditentukan oleh cara data tersebut dikumpulkan, disimpan, diproses, atau digunakan.[52]

Data pribadi hanya akan dikumpulkan untuk satu atau lebih tujuan yang sah. Data pribadi hanya dapat dikumpulkan untuk tujuan yang sah. Terkait langsung dengan fungsi atau aktivitas pengontrol data yang menggunakan data pribadi untuk tujuan awal pengumpulannya. Pengumpulan data diperlukan atau berkaitan langsung dengan tujuan tertentu. Data pribadi adalah tepat, relevan, dan tidak terlalu berkaitan dengan tujuan ini.[53]

Terdapat tiga prinsip penting dalam privasi, yaitu:

a. Prinsip kesendirian, prinsip dasar privasi pribadi. Ada empat jenis tindakan yang melanggar privasi seseorang, seperti menunjukkan seseorang yang tidak hadir. Misalnya, menggunakan foto seseorang untuk menggambarkan kekerasan dalam rumah tangga tanpa izin, menampilkan informasi pribadi seseorang, khususnya nama atau nomor teleponnya, untuk tujuan komersial, atau menampilkan informasi pribadi seseorang dengan cara yang memalukan tidak memberi siapa pun tempat untuk menyendiri.

[52] Mohammad Dani Pratama Huzaini. "Dosen UM Malaysia, Abu Bakar Munir, Bicara tentang Perlindungan Data Pribadi Kerangka hukum di ASEAN masih terkesan longgar", https://www.hukumonline.com/berita/baca/lt5bd074d45 f36a/dosen-um-malaysia--abu-bakar-munir--bicaratentang-perlindungan-data-pribadi/. Diakses pada 14 Oktober 2020 pukul 13.43 WIB.

[53] Sinta Dewi, "Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional Dan Implementasinya", Sosiohumaniora, Volume 19 No. 3 November 2017 : 206 – 212 hlm. 210.

b. Data pribadi ini dikumpulkan dari orang lain, seperti rekam medis, kebiasaan pribadi, informasi perpajakan, informasi asuransi, dan riwayat kriminal. Informasi ini dapat disalahgunakan oleh orang-orang yang tidak bertanggung jawab melalui pengumpulan atau pemrosesan data, yang merupakan pelanggaran terhadap hak perlindungan data Pemilik.

c. Prinsip Privasi untuk Komunikasi yang Dilakukan Secara Online.[54]

Perdebatan mengenai Undang-Undang Perlindungan Informasi Pribadi mendapat sambutan antusias di Indonesia. Salah satu hal yang paling mendasar adalah undang-undang ini sama sekali tidak menyebutkan asas. Ibarat tubuh tanpa organ. Padahal, asas-asas tersebut adalah idealisme, filsafat hukum, dan nafas peraturan perundang-undangan. Ketentuan Kebijakan diatur dalam Pasal 17, dan pengolahan data pribadi mencakup prinsip perlindungan data pribadi. Namun prinsip ini hanya berlaku pada bagian pengolahan data saja. Padahal, asas dan asas tersebut seharusnya menjadi inspirasi dalam setiap bab undang-undang tersebut. Dimulai dengan bab tentang transfer data pribadi, pemrosesan data pribadi, kewajiban pengontrol dan pemroses data, dan tahap penalti untuk transfer data pribadi. Tanpa asas dan asas maka undang-undang ini hanya dapat ditentukan secara mekanis dan teknis. Inilah gagasan dan gagasan yang patut digali dengan menangkap

[54] Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R, "Legal Protection for Urban Online-Transportation-User's Personal Data Disclosure in the Age of Digital Technology". Padjadjaran Journal of Law, 5(3), 485-505, hlm. 493. Dikutip dari Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum". Jatiswara Vol. 34 No. 3, November 2019, hlm. 243.

budaya masyarakat Indonesia, nilai-nilai luhurnya, dan perubahan zaman. Pemahaman kebarat-baratan tentang privasi juga dapat ditemukan dalam keterbatasan rumusan prinsip dan prinsip tersebut, sehingga prinsip dan prinsip ini adalah yang paling orisinal dalam hal kepedulian terhadap perlindungan data pribadi dan kebutuhan ekonomi di dunia digital menjadi sesuatu. nusantara. Asas dan asas tersebut tertuang dalam naskah akademis hukum ini, seperti asas perlindungan, kepentingan umum, keseimbangan, tanggung jawab, dan timbal balik. Asas dan asas tersebut sepertinya hanya terdapat dalam tulisan ilmiah, bukan dalam teks hukum. Prinsip dan prinsip tata kelola yang baik kini tercermin dalam GDPR. Perlindungan data pribadi harus didasarkan pada prinsip keadilan, kepastian hukum, transparansi, proporsionalitas, akurasi, persetujuan, integritas dan kerahasiaan.[55]

Prinsip-prinsip tersebut selanjutnya dijabarkan sebagai berikut:

a) Pembatasan diperlukan pada pengumpulan data pribadi. Data yang dikumpulkan harus dikumpulkan menggunakan metode yang sah dan adil dan, jika sesuai, dengan sepengetahuan dan persetujuan subjek data.
b) Data pribadi harus akurat sesuai dengan tujuan penggunaannya, dan data pribadi harus akurat dan lengkap.

[55] Awaludin Marwan, "Perlindungan Data Pribadi Tanpa Asas: Tubuh Tanpa Organ". https://cyberthreat.id/read/7634/Perlindungan-DataPribadi-Tanpa-Asas-Tubuh-Tanpa-Organ, diakses pada tanggal 6 Oktober 2020 pukul 18.33 WIB.

c) Tujuan pengumpulan data harus spesifik dan penggunaan data lebih lanjut harus dibatasi hanya untuk menentukan tujuan tersebut.
d) Data ini hanya boleh dipublikasikan, dipublikasikan atau digunakan untuk tujuan selain tujuan yang ditentukan dengan persetujuan pemilik data atau otoritas kehakiman.
e) Data ini harus dilindungi dengan tindakan pengamanan yang tepat untuk melindunginya dari kehilangan, kerusakan, penggunaan, modifikasi dan pengungkapan.
f) Harus ada kebijakan umum mengenai pengungkapan data pribadi.
g) Setiap orang harus mempunyai hak untuk mengakses datanya dan hak untuk menghapus atau memperbaiki data yang tidak akurat.
h) Pengendali data bertanggung jawab untuk mematuhi prinsip-prinsip ini.

Dalam Pasal 14 UU Perlindungan data pribadi disebutkan terkait prinsip-prinsip dan hak-hak pemilik data pribadi dalam hal:[56]

a) Keamanan nasional,
b) Kepentingan proses penegakan hukum;

[56] Kosegeran, G., & Rumimpunu, D. (2021). Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin. *Lex Privatum*, *IX*(12), 89–98. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/38447.

c) Kepentingan pers sepanjang data pribadi diperoleh dari informasi yang sudah dipublikasikan dan disepakati oleh pemilik;

d) Kepentingan penelitian ilmiah dan statistik sepanjang data pribadi diperoleh dari informasi yang sudah dipublikasikan (konfirmasi kembali untuk kepentingan penelitian).

2. Peraturan Perundang-Undangan yang Mengatur Perlindungan Data Pribadi

a. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)

PP PSTE merupakan pelaksanaan dari UU ITE yang memperjelas tanggung jawab penyelenggara sistem elektronik dalam melindungi data pribadi. Peraturan ini memberikan kewajiban bagi penyelenggara untuk memastikan keamanan data dan menyusun langkah-langkah mitigasi terhadap pelanggaran keamanan data. Pasal 14 PP PSTE menyatakan bahwa penyelenggara sistem elektronik harus menjaga kerahasiaan, integritas, dan ketersediaan data pribadi pengguna. Pendapat dari Bagir Manan mengindikasikan bahwa PP ini menjadi landasan penting dalam memastikan keamanan data pribadi melalui pendekatan teknis yang lebih rinci, meskipun implementasinya di lapangan masih membutuhkan peningkatan.

b. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)

UU PDP menjadi tonggak utama dalam perlindungan data pribadi di Indonesia, karena mencakup berbagai aspek terkait dengan pengumpulan, pemrosesan, penyimpanan, dan penghapusan data pribadi. Undang-undang ini memuat ketentuan hak-hak subjek data serta kewajiban pengendali data dan prosesor data, yang bertujuan untuk melindungi privasi individu. UU PDP mengatur perizinan, pengelolaan, serta sanksi bagi pelanggaran yang melibatkan data pribadi, sehingga menjadi langkah penting dalam regulasi perlindungan data di Indonesia.

c. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

UU ITE merupakan landasan hukum utama di Indonesia yang mengatur aktivitas di ruang siber, termasuk perlindungan data pribadi. Setelah revisi melalui Undang-Undang Nomor 19 Tahun 2016, UU ITE mencakup ketentuan perlindungan data pribadi pengguna di internet, meskipun tidak secara mendetail. Pasal 26, misalnya, mengatur tentang persetujuan pemilik data untuk setiap penggunaan data pribadi oleh pihak lain, sehingga menegaskan pentingnya informed consent dalam perlindungan data pribadi di ranah digital. Menurut pendapat Ahmad Sofian, ketentuan dalam UU ITE tersebut mencerminkan upaya pemerintah untuk

mengantisipasi penyalahgunaan data, tetapi masih kurang dalam aspek teknis pelaksanaannya, sehingga memerlukan regulasi pendukung.

d. Regulasi Internasional sebagai Rujukan: General Data Protection Regulation (GDPR)

GDPR di Uni Eropa sering dijadikan rujukan dalam penyusunan kebijakan perlindungan data pribadi di berbagai negara, termasuk Indonesia. GDPR memberikan standar tinggi dalam perlindungan data dengan prinsip-prinsip yang ketat terkait hak-hak individu, transparansi, dan akuntabilitas pengendali data. Beberapa prinsip dalam GDPR diadopsi dalam UU PDP, seperti hak akses, hak perbaikan data, dan hak untuk dilupakan. Menurut Rosadi Iskandar, pendekatan GDPR menjadi inspirasi utama bagi UU PDP di Indonesia, meskipun terdapat tantangan dalam penerapan standar GDPR di Indonesia yang memiliki kondisi teknis dan sosial yang berbeda.

3. Konsep Perlindungan Hukum

UU PDP mengatur tentang perlindungan hukum terhadap pemilik data pribadi (subjek data) yang meliputi hak-hak subjek data, kewajiban pengendali dan prosesor data, serta mekanisme penegakan hukum apabila terjadi pelanggaran.

a) Hak Subjek Data

Pasal 4 UU PDP menyatakan bahwa setiap individu memiliki hak-hak terkait data pribadinya, antara lain: 1) Hak atas informasi (Pasal 5); 2) Hak untuk mengakses data pribadi (Pasal 6); 3) Hak untuk memperbaiki dan memperbarui data pribadi (Pasal 7); 4) Hak untuk menghapus dan/atau memusnahkan data pribadi (Pasal 8); 5) Hak untuk menarik persetujuan pemrosesan data pribadi (Pasal 9); 6) Hak untuk mengajukan keberatan terhadap pemrosesan data pribadi (Pasal 10). Hak-hak ini merupakan bentuk perlindungan hukum preventif guna memastikan bahwa subjek data memiliki kendali atas data pribadinya.

b) Kewajiban Pengendali dan Prosesor Data

Pasal 20 UU PDP menetapkan bahwa pengendali data wajib memastikan pemrosesan data dilakukan secara sah, transparan, dan bertanggung jawab. Adapun kewajiban pengendali dan prosesor data mencakup:

1) Memastikan adanya persetujuan dari subjek data (Pasal 21)
2) Menjaga keamanan data pribadi dari akses ilegal (Pasal 22)
3) Memberitahukan adanya kebocoran data kepada subjek data dan pemerintah (Pasal 23)

Hal ini merupakan bagian dari perlindungan hukum preventif, di mana pengendali dan prosesor data diwajibkan menerapkan prinsip kehati-hatian dalam pemrosesan data.

c) Mekanisme Penegakan Hukum

Ketika terjadi pelanggaran terhadap perlindungan data pribadi, UU PDP memberikan mekanisme perlindungan hukum represif melalui:

a. Sanksi administratif (Pasal 57) bagi pengendali atau prosesor data yang melanggar ketentuan UU PDP.
b. Sanksi pidana bagi pelanggaran serius, seperti penyalahgunaan data pribadi tanpa persetujuan, yang dapat dikenakan hukuman penjara hingga 6 tahun atau denda hingga Rp.6 miliar (Pasal 67-70).

Dengan demikian, UU PDP memberikan perlindungan hukum yang bersifat komprehensif, baik secara preventif melalui pengaturan hak-hak subjek data dan kewajiban pengendali data, maupun secara represif melalui mekanisme sanksi bagi pelanggar.

E. Pengertian Konsep Kekosongan Hukum dan Asas-Asas Hukum terkait Perlindungan Data Pribadi

1. Konsep Kekosongan Hukum

Pengertian kekosongan atau kehampaan hukum secara harfiah dapat diartikan sebagai berikut : Hukum atau rect menurut kamus hukum, rect secara objektif berarti undang-undang atau hukum. Grotius dalam bukunya De Jure Belli ac Pacis (1625) menyatakan, bahwa hukum adalah peraturan tentang perbuatan moral yang menjamin keadilan. Adapun Van Vollenhoven dalam ”Het Adatrecht van Ned Indie” mengungkapkan bahwa “hukum adalah suatu gejala dalam

pergaulan hidup yang bergejolak terus-menerus dalam keadaan bentur dan membentur tanpa henti-hentinya dengan gejala-gejala lainnya."

Penyebab terjadinya kekosongan hukum yaitu, dalam penyusunan peraturan perundang-undangan baik dari legislatif maupun eksekutif pada kenyataan memerlukan waktu yang lama, sehingga pada saat peraturan perundang-undangan itu dinyatakan berlaku maka hal-hal atau keadaan yang hendak diatur oleh peraturan tersebut telah berubah. Selain itu, kekosongan hukum dapat terjadi karena hal-hal atau keadaan yang terjadi belum dapat diatur dalam suatu peraturan perundang-undangan, atau sekalipun telah diatur dalam suatu peraturan perundang-undangan namun tidak jelas atau bahkan tidak lengkap. Hal ini sebenarnya selaras dengan pameo yang menyatakan bahwa "terbentuknya suatu peraturan perundang-undangan senantiasa tertinggal atau terbelakang dibandingkan dengan kejadian-kejadian dalam perkembangan masyarakat.

Perlu dipahami juga bahwa hukum atau peraturan perundang-undangan yang dibentuk tidak dapat mencakup semua permasalahan di masyarakat. Kondisi inilah yang kemudian dapat mengakibatkan terjadinya kekosongan di bidang hukum tadi.

Kekosongan atau kehampaan ilmu hukum dapat terjadi karena berbagai penyebab disamping tradisi penemuan hukum kita yang mendasarkan kepada tardisi jurisprudence dimana tidak termasuk dalam alur legal science sehingga perkembangannya sangat lambat juga

disebabkan oleh karena pesatnya kemajuan dan pertumbuhan dinamika masyarakat yang tidak dapat diimbangi oleh pengisian atau penambahan hukum dengan tardisi jurisprudence yang saat ini terjadi.

Adapun solusi apabila terjadi kekosongan hukum sebagaimana telah diungkapkan sebelumnya, bahwa perkembangan masyarakat selalu lebih cepat dari perkembangan peraturan perundang-undangan. Peraturan perundang-undangan sebenarnya dibuat sebagai panduan bersikap bagi masyarakat yang dapat menentukan mana yang boleh dan mana yang tidak boleh. Hukum yang stabil dapat menjadi ukuran yang pasti di masyarakat, namun hukum yang jalan di tempat pada kenyataannya akan menjadi hukum yang usang dan tertinggal jauh oleh perkembangan masyarakat. Untuk itu,sangat diperlukan perkembangan masyarakat.

2. Asas-Asas Hukum terkait Perlindungan Data Pribadi

Berdasarkan ketentuan Pasal 3 Undang-Undang Nomor 27 Tahun 27 Tahun 2022 tentang Perlindungan Data Pribadi, ada delapan asas yang menjadi landasan, yakni asas pelindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan.