

LEMBAR PENGESAHAN PANITIA UJIAN SKRIPSI

Skripsi yang berjudul, "PERLINDUNGAN HUKUM TERHADAP DATA PRIBADI DALAM UU NOMOR 27 TAHUN 2022 DAN TANTANGAN IMPLEMENTASINYA DALAM ERA TEKNOLOGI INFORMASI", Oleh Ivan Hendison Samosir Npm 20600103 telah diujikan dalam sidang Meja Hijau Program Studi Ilmu Hukum Fakultas Hukum Universitas HKBP Nommensen Medan Pada tanggal 26 Maret 2024. Skripsi ini telah diterima sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu (S-1) pada Program Studi Ilmu Hukum.

PANITIA UJIAN MEJA HIJAU

1. Ketua : Dr. July Esther, S.H., M.H
NIDN. 0131077207
2. Sekretaris : Lesson Sihotang, S.H., M.H
NIDN. 0116106001
3. Pembimbing I : Lesson Sihotang, S.H., M.H
NIDN. 0116106001
4. Pembimbing II : Dr. July Esther, S.H., M.H
NIDN. 0131077207
5. Penguji I : Dr. Herlina Manullang, S.H., M.H
NIDN. 0131126303
6. Penguji II : Roida Nababan, S.H., M.H
NIDN. 0111026601
7. Penguji III : Lesson Sihotang, S.H., M.H
NIDN. 0116106001



Medan, 25 April 2024
Mengesahkan
Dekan



Dr. Janpatar Simamora, S.H., M.H
NIDN. 0114018101

BAB I

PENDAHULUAN

A. Latar Belakang

Dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyebutkan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia. Terkait hak pribadi sebagai hak asasi manusia dijelaskan Danrivanto Budhijanto, bahwa “Perlindungan terhadap hak-hak pribadi atau hak-hak privat akan meningkatkan nilai-nilai kemanusiaan, meningkatkan hubungan antara individu dan masyarakatnya, meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepantasan, serta meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi kekuasaan pemerintah.¹

Jika melihat uraian di atas maka perlindungan diri pribadi sebagaimana disebutkan dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 di atas erat kaitannya dengan perlindungan terhadap hak-hak pribadi atau hak-hak privat. Dalam Sejarah perkembangannya, privasi merupakan suatu konsep yang bersifat universal dan dikenal di berbagai negara baik tertulis dalam bentuk Undang-Undang maupun tidak

¹ Danrivanto Budhijanto, Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi, PT. Refika Aditama, Bandung, 2010, hlm. 4.

tertulis dalam bentuk aturan moral.² Hak tersebut berkaitan dengan kebutuhan spiritual manusia yaitu kebutuhan untuk dihargai perasaan, pikiran dan hak untuk menikmati kehidupannya atau disebut dengan *the right to be let alone*.³

Berkembangnya zaman pada era sekarang yang sering di sebut era revolusi 4.0 memang sangat pesat apalagi dalam hal segi teknologi, dengan teknologi yang sudah ada keberadaan internet yang dapat untuk media bersosial dan mencari informasi terkini secara cepat. Dalam bersosial dan lain sebagainya baik untuk bisnis dan lain – lain, sangatlah penting untuk era sekarang sesuai dengan perkembangannya. Baik dari semua Negara didunia pun sudah menggunakan internet itu untuk kepentingan Negara dalam segi pertahanan Negara dan keamanan masyarakatnya. Dengan semakin maraknya menggunakan internet di era sekarang tidak ada batasan nya untuk bersosial dan saling tau menau dari seseorang bersosial. Dengan perkembangan yang sangat pesat itu dapat dengan timbulnya kriminalisasi, pelecehan dan lain lain yang dapat menjadikan tindak pidana. Terkhususnya dalam *cybercrime* atau pembobolan dalam suatu akun atau media sosial seseorang untuk melakukan tindakan yang tidak sesuai norma – norma masyarakat terlebihnya di Indonesia, dengan tindakan itu pun dapat menyebabkan kebocoran suatu data pribadi seseorang yang dapat mengungkap dari pribadi seseorang dan privasinya.

Perlindungan data pribadi sendiri ialah sebagai bentuk perlindungan bagi suatu hak privasi, akan membutuhkannya pelindungan privasi seseorang atau perlindungan dari data pribadi seseorang, dan data pribadi jika mengacu pada EUGDPR (*European Union*

² <https://privacyinternational.org/>. Privacy & Human Rights, An International Survey of Privacy Laws and Developments, Electronic Privacy

³ Samuel Warren & Louis D. Brandeis, "*The Right To Privacy*", *Harvard Law Review*, Volume 4, 1890, hlm. 1

General Data Protection Regulation) ialah informasi apa pun yang berkaitan dengan orang alami yang teridentifikasi atau dapat diidentifikasi (subjek data); orang alami yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan mengacu pada pengidentifikasi seperti nama, nomor identifikasi, data lokasi, pengidentifikasi online atau satu atau lebih faktor khusus untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau sosial dari orang tersebut.⁴ Hal ini supaya dapat ngontrol dan mengatur penyebaran informasi tentang data pribadi. Data pribadi pada umumnya di bagi menjadi dua kategori : Data pribadi yang bersifat umum ialah : Nama, Alamat, Data lokasi, IP address, Data pribadi yang bersifat spesifik (sensitif) ialah : ras, etnis, agama, orientasi seksual, genetic, catatan criminal. Dimana kebutuhan dari segala hukum untuk mengayominya dalam suatu Negara dalam bentuk undang – undang dengan hukum perlindungan data pribadi.

Konsep perlindungan data sering diperlakukan sebagai bagian dari perlindungan privasi. Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan *information privacy* karena menyangkut informasi pribadi.⁵

⁴ Pasal 4 (1) GDPR

⁵ Menurut Alan Westin: *Privacy is the claim of individuals, group or institution to determine for themselves when, how, and to what extent information about them is communicated to others dalam, Allan Westin, Alan F. Westin, Privacy and Freedom, London, 1967, hlm. 7.*

Perlindungan data juga merupakan hak asasi manusia yang fundamental, sejumlah negara telah mengakui perlindungan data sebagai hak konstitusional atau dalam bentuk “habeas data” yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya. Albania, Armenia, Filipina, Timor Leste, Kolombia dan Argentina adalah negara-negara dengan perbedaan sejarah dan budaya yang telah mengakui peran dari perlindungan data yang dapat memfasilitasi proses demokrasi dan telah menjamin perlindungannya dalam konstitusi mereka.⁶

Pengumpulan dan penyebarluasan data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi. Data pribadi merupakan suatu aset atau komoditas bernilai ekonomi tinggi.⁷ Isu mengenai pentingnya perlindungan data pribadi mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Sejumlah kasus yang mencuat, terutama yang memiliki keterkaitan dengan kebocoran data pribadi seseorang dan bermuara kepada aksi penipuan atau tindak kriminal pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.⁸

Sebagaimana diketahui bahwa perihal data pribadi sebelumnya telah diatur dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

⁶ Graham Greenleaf, *76 Global Data Protection Laws, Privacy Laws & Business Special Report*, September 2011

⁷ Edmon Makarim, *Kompilasi Hukum Telematika*, PT. Raja Grafindo Perkasa, Jakarta 2003, hlm. 3.

⁸ Wahyudi Djafar dan Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci*, Elsam, Jakarta, 2014, hlm. 2

Terdapat beberapa kompleksitas yang harus dipahami pengguna media sosial di seluruh Indonesia, sebagai berikut:

1. Penghinaan dan atau pencemaran nama baik. Di media sosial seseorang tidak bisa sembarangan menjelek-jelekan individu maupun lembaga tertentu karena di dalam Pasal 45 ayat (3) U ITE sebagai pengaturan yang memuat mengenai Informasi Elektronik dan atau Dokumen Elektronik yang memiliki muatan penghinaan dan atau pencemaran nama baik.
2. Pasal 45 ayat (1) UU ITE sebagai pengaturan yang memuat mengenai Informasi Elektronik dan atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
3. Pengaturan yang mengandung perihal menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen. Keempat, pengaturan yang mengandung menyebarkan kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA). Perihal ini menjadi penting mengingat media sosial akan mempertemukan banyak orang dalam dunia maya, maka sedapat mungkin menghindari postingan hal-hal yang berbau SARA.

Sebagai negara hukum, Negara Republik Indonesia memiliki kewajiban untuk melindungi hak warga negaranya. Hak tersebut adalah bagian dari hak asasi manusia yang dijamin dalam UUD 1945. Guna menanggulangi masalah keamanan dan perlindungan data pribadi, pemerintah pun membentuk Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi

Elektronik (UU ITE). Seiring pesatnya perkembangan teknologi, saat ini ketentuan tersebut dirasa belum cukup untuk menyelesaikan permasalahan-permasalahan hukum yang terjadi, terkhusus terhadap perlindungan data pribadi pada *platform* media social, diharapkan dalam keadaan tertentu. Jika ditelisik lebih lanjut bahwa perihal data pribadi selain diatur dalam UU ITE, diatur pula pada beberapa peraturan perundang-undangan di Indonesia yang tidak secara khusus mengatur tentang data pribadi. Hal ini mengingat data pribadi dapat diberikan, disimpan, dialihkan hingga bahkan terbocorkan bukan hanya melalui sistem elektronik (dunia maya) namun juga dapat pula melalui non-elektronik. Hal ini menjadi sebab dalam ketersebaran konteks penggunaannya, beberapa peraturan perundang-undangan yang melingkupi hal tersebut dapat dipergunakan.

Hingga pada tanggal 17 Oktober 2022 Pemerintah secara resmi telah menerbitkan Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. Hal ini merupakan sebuah era baru dalam pengaturan perihal data pribadi di Indonesia seiring dengan arus teknologi dan informasi dalam dunia maya di seluruh dunia.

Penggunaan internet (interconnection networking) yang menjadi media informasi dan komunikasi elektronik yang menyediakan beragam aktivitas baik berupa jasa maupun produk seperti *e-commerce* (perdagangan/bisnis melalui media elektronik), *e-education* (pendidikan), *e-health* (kesehatan), *e-government* (pemerintahan), *e-payment* (keuangan), transportasi, pariwisata serta perkembangan cloud computing atau komputasi awan yaitu aplikasi yang menyediakan ruang penyimpanan data pengguna seperti google drive, iCloud, Dropbox, Youtube dan sebagainya. Ruang lingkup dari salah satu pembaharuan dalam bidang teknologi informasi dan komunikasi yaitu melakukan pengumpulan,

penyimpanan, pembagian, dan penganalisaan data secara efektif dan efisien antar industri/perusahaan atau masyarakat.⁹

Meningkatnya jumlah pengguna platform berbasis teknologi informasi dalam beraktivitas atau bertransaksi digital maka potensi pelanggaran hukum terhadap penyalahgunaan data pun meningkat. Adanya kasus pelanggaran atau penyalahgunaan Data Pribadi belakangan menjadi isu besar di Indonesia, diantaranya kasus kebocoran data BPJS (Badan Penyelenggara Jaminan Sosial) Kesehatan pada bulan Mei tahun 2021, data sejumlah peserta BPJS (Badan Penyelenggara Jaminan Sosial) Kesehatan dijual di Raid Forums seharga 0,15 Bitcoin.¹⁰ Demikian juga muncul kasus kebocoran data pengguna aplikasi e-HAC (Electronic Health Alert) milik Kementerian Kesehatan Republik Indonesia, kebocoran data di aplikasi e-HAC tersebut terjadi pada bulan Juli tahun 2021.

Salah satu contoh perlindungan Data Pribadi yang telah diterapkan sejak lama adalah di sektor kesehatan. Pasal 57 ayat (1) menyebutkan bahwa “Setiap orang berhak atas rahasia kondisi kesehatan pribadinya yang telah dikemukakan kepada penyelenggara pelayanan kesehatan.”¹¹ Kemudian Pasal 57 ayat (2) menambahkan bahwa “Ketentuan mengenai hak atas rahasia kondisi kesehatan pribadi sebagaimana dimaksud pada ayat (1) tidak berlaku dalam hal: a. perintah undang-undang; b. perintah pengadilan; c. izin yang bersangkutan; d. kepentingan masyarakat; atau e. kepentingan orang tersebut.

⁹ Dewi, S. “Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan *Cloud Computing* Di Indonesia DEMO 2 JURNAL, (94), 22-30, 2016 hlm. 23.

¹⁰ <https://nasional.tempo.co/read/1501790/6-kasus-kebocoran-data-pribadi-di-indonesia> (diakses 24November 2023)

¹¹ Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan

Indonesia sebagai negara berasaskan hukum maka negara menjamin perlindungan atas hak asasi manusia terhadap data pribadi warga negaranya. Maraknya kasus pelanggaran hukum terhadap penyalahgunaan data pribadi dipicu semakin meningkatnya penggunaan teknologi informasi dalam aktivitas masyarakat yang menggunakan platform digital dalam mengakses data. Melihat kasus pelanggaran data pribadi di Indonesia yang terjadi maka penelitian ini bertujuan memaparkan tentang perlindungan data pribadi dalam regulasi Undang-Undang Perlindungan Data Pribadi di Indonesia.

B. Rumusan Masalah

Adapun yang menjadi permasalahan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana Kewajiban Pemilik/Pemegang Aplikasi Jual Beli Online terhadap Perlindungan Data Pribadi di Indonesia?
2. Bagaimana Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia dalam Menjamin Keamanan dan Privasi Data Individu?
3. Bagaimana Upaya yang Dilakukan agar Tercapainya Keberhasilan Undang-Undang Perlindungan Data Pribadi

C. Tujuan Penelitian

Berdasarkan rumusan masalah yang menjadi objek pembahasan dalam penelitian ini, maka tujuan yang diharapkan peneliti dalam penelitian ini sebagai berikut:

1. Untuk mengetahui kewajiban pemilik/pemegang aplikasi jual beli online terhadap Perlindungan Data Pribadi di Indonesia
2. Untuk mengetahui dan menguraikan Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia dalam menjamin keamanan dan privasi data individu

3. Untuk mengetahui Bagaimana Upaya yang Dilakukan agar Tercapainya Keberhasilan Undang-Undang Perlindungan Data Pribadi

D. Manfaat Penelitian

Adapun yang menjadi manfaat dari penulisan skripsi ini adalah sebagai berikut:

1. Manfaat teoritis

Secara teoritis skripsi ini diharapkan dapat memberi sumbangan pengetahuan dan pemikiran dalam bidang ilmu hukum, khususnya hukum Pidana. Kemudian menjadi salah satu referensi mahasiswa dalam menyusun skripsi mengenai UU Data Pribadi dalam bidang hukum Pidana karena bahasan skripsi ini masih jarang dibahas dalam tugas akhir mahasiswa di lingkungan Fakultas Hukum Universitas HKBP Nommensen.

2. Manfaat Praktis

Adapun yang menjadi manfaat praktis dari hasil penelitian ini ialah dapat memberikan masukan-masukan kepada Aparat Penegak Hukum Khususnya Hakim, Jaksa, Polisi, dan Pengacara dalam menyelesaikan permasalahan hukum serta mengambil keputusan dan kebijakan dalam menangani kasus Perlindungan Data Pribadi

3. Manfaat Bagi Penulis

Hasil penelitian ini diharapkan lebih memperdalam wawasan Ilmu Hukum kepada penulis dan sebagai salah satu syarat untuk memperoleh gelar Sarjana Hukum Program Studi Ilmu Hukum bagian Hukum Pidana

BAB II

TINJAUAN PUSTAKA

A. Tinjauan Umum Tentang Hukum Perlindungan Data Pribadi

1. Pengertian Perlindungan Data Pribadi

Perlindungan data pribadi merupakan elemen penting dalam era digital yang terus berkembang. Kepentingan menjaga kerahasiaan informasi pribadi mencakup sejumlah dimensi yang memiliki relevansi yang substansial bagi individu dan Masyarakat. Perlindungan data pribadi melibatkan landasan dari hak privasi individu. Hak ini mencakup kontrol yang dimiliki individu atas data pribadi mereka, seperti nama, alamat, nomor telepon, dan informasi yang bersifat sensitif. Dengan keberadaan perlindungan data ini, individu dapat menjaga privasi mereka, mengendalikan penggunaan informasi mereka, dan secara efektif mencegah penyalahgunaan, penipuan, atau penggunaan data mereka untuk tujuan yang tidak dikehendaki.

Perlindungan data pribadi juga memiliki relevansi penting dalam mencegah pencurian identitas.¹² Identitas digital yang terungkap secara tidak sah dapat menjadi sarana bagi pihak yang bermaksud jahat untuk mendapatkan keuntungan pribadi, seperti melakukan penipuan keuangan, membuka rekening palsu, atau menyalahgunakan informasi pribadi lainnya. Dengan demikian, menjaga kerahasiaan data pribadi menjadi langkah pertahanan yang signifikan terhadap potensi kerentanannya identitas digital.

¹² Nurfitri, Sudirman, & Disemadi. Tiktok Phenomenon: Exoneration Clause Vs. Personal Data Protection. *Jurnal Pendidikan Kewarganegaraan Undiksha*, 10(1),2022, Hlm 441-453.

Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi. Perlindungan data pribadi ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi.

Pengertian data pribadi disebutkan dalam Pasal 1 (22) Undang-Undang Administrasi Kependudukan (UU. No. 23 tahun 2006 yang diubah dengan UU. No. 24 tahun 2013) bahwa Data pribadi adalah data yang dimiliki oleh orang yang menyimpan, merawat dan memelihara, serta dijaga kerahasiaannya. Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi Pada Sistem Elektronik No. 20 tahun 2016 juga memberikan pengertian data pribadi dengan definisi yang sama. Data perseorangan yang dimaksud dalam pengertian tersebut adalah segala keterangan yang dianggap mengandung kebenaran dan nyata menjadi satu kesatuan dengan diri seseorang serta dapat diidentifikasi secara langsung maupun tidak langsung pada setiap individu. Pengertian data pribadi yang berbeda dengan pengertian diatas disebutkan dalam Pasal 1 angka 29 Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP. No. 71 tahun 2019), yang menyatakan bahwa Data pribadi adalah data setiap orang yang secara langsung atau tidak langsung diidentifikasi melalui sistem elektronik dan atau non-elektronik dan atau diidentifikasi secara individu atau digabungkan dengan informasi lain. Kedua pengertian data pribadi tersebut mempunyai

persamaan bahwa data pribadi merupakan data atau segala informasi yang melekat pada diri seseorang yang dengannya seseorang dapat diidentifikasi.

Pembicaraan perlindungan data pribadi mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Perlindungan data pribadi berhubungan dengan konsep privasi. Konsep privasi sendiri adalah gagasan untuk menjaga integritas dan martabat pribadi. Hak privasi juga kemampuan untuk siapa yang memegang informasi tentang mereka dan bagaimana informasi tersebut digunakan.¹³ Seiring berjalannya waktu, dikarenakan perkembangan teknologi saat ini segala cara bisa dilakukan agar terpenuhinya kepentingan suatu golongan maupun individu, baik itu untuk mendapatkan keuntungan sehingga merugikan pihak lain (misalnya untuk kepentingan di perbankan (*scam*). Misalnya saja seperti adanya perbuatan peretasan data pribadi di platform Marketplace yang dilakukan pihak ketiga yang tidak bertanggungjawab. Informasi pribadi dari pengguna tersebut diretas dan diambil untuk dimanfaatkan hingga dijual ke situs web yang lainnya (saat ini sering dikenal dengan istilah *darkweb*).¹⁴

Pada zaman sekarang, informasi merupakan hal yang penting dan menentukan perkembangan ekonomi suatu negara baik negara berkembang maupun negara maju. Informasi mengenai individu selalu dikelola oleh pemerintah dan swasta, tetapi munculnya era komputer menciptakan ancaman yang lebih besar bagi privasi individu tersebut, serta kemungkinan individu menderita kerugian sebagai

¹³ Djafar, W., & Komarudin, A. Perlindungan Hak Atas Privasi Di Internet-Beberapa PenjelasanKunci. Elsam, Jakarta. 2004 Hlm 3

¹⁴ Albert Lodewyk Sentosa Siahaan, *Urgency of Personal Data Protection on MarketplacePlatforms Against Technological Advances*, Majalah Hukum Nasional Volume 52 Nomor 2 Tahun 2022

akibat dari ketidaktepatan atau pembocoran informasi jauh lebih besar.¹⁵ Era digital telah memicu ledakan pertumbuhan data pribadi yang dibuat, disimpan dan ditransmisikan pada komputer dan perangkat mobile, *broadband* dan situs internet dan media.¹⁶ Kemajuan teknologi juga menimbulkan ancaman serius bagi privasi pribadi dan keamanan informasi.

Perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi. Perlindungan diri pribadi ini tercantum dalam Pasal 28G UUD 1945. Dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyebutkan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi manusia. Perlindungan diri pribadi atau privasi ini bersifat universal, dalam arti diakui banyak negara.

Pelindungan Data Pribadi adalah keseluruhan Upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.¹⁷

¹⁵ Sinta Dewi, *Cyber Law 1 : Perlindungan Privasi Atas Informasi Pribadi Dalam E commerce* Menurut Hukum Internasional, Widya Padjajaran, Bandung 2009, Hlm 53

¹⁶ Cammeron G Shilling, "Privacy and Data Security : New Challenges of The Digital Age". *New Hampshire Bar* 2011 Hlm 1

¹⁷ Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

2. Prinsip Perlindungan Data Pribadi

Perkembangan teknologi informasi saat ini, berbagai macam kegiatan baik dalam konteks pemerintahan, transaksi bisnis, komersil ataupun komunikasi berlangsung melalui media elektronik (online). Data atau informasi yang disampaikan melalui media elektronik itu sesungguhnya merupakan hal yang berharga. Selain itu, kegiatan yang berlangsung online tersebut juga memiliki risiko karena dapat menimbulkan masalah apabila data atau informasi tersebut bocor sehingga bisa disalahgunakan oleh pihak yang tidak bertanggung jawab. Salah satu bidang yang dipengaruhi oleh perkembangan teknologi informasi adalah terjadinya interaksi yang aktif antara individu dengan pihak penyedia jasa informasi. Berbagai sektor kehidupan telah memanfaatkan system informasi seperti perdagangan berbasis digital (ecommerce), transportasi, industri, pariwisata, bidang pemerintahan (egovernment) dan industry keuangan (epayment). Cakupan dan system teknologi informasi meliputi pengumpulan (collect), penyimpanan (store), pemroses, produksi dan pengiriman, dari dan ke industri atau masyarakat secara cepat dan efektif.¹⁸

Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan information

¹⁸ Sinta, Dewi. Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia.

privacy karena menyangkut informasi pribadi. Perlindungan data juga merupakan hak asasi manusia yang fundamental, sejumlah negara telah mengakui perlindungan data sebagai hak konstitusional atau dalam bentuk ‘habeas data’ yakni hak seseorang untuk mendapatkan pengamanan terhadap datanya dan untuk pembenaran ketika ditemukan kesalahan terhadap datanya. Albania, Armenia, Filipina, Timor Leste, Kolombia dan Argentina adalah negara-negara dengan perbedaan sejarah dan budaya yang telah mengakui peran dari perlindungan data yang dapat memfasilitasi proses demokrasi dan telah menjamin perlindungannya dalam konstitusi mereka.¹⁹

Pengumpulan dan penyebaran data pribadi merupakan pelanggaran terhadap privasi seseorang karena hak privasi mencakup hak menentukan memberikan atau tidak memberikan data pribadi.²⁰ Data pribadi merupakan suatu aset atau komoditas bernilai ekonomi tinggi.²¹ Isu mengenai pentingnya perlindungan data pribadi mulai menguat seiring dengan meningkatnya jumlah pengguna telepon seluler dan internet. Sejumlah kasus yang mencuat, terutama yang memiliki keterkaitan dengan kebocoran data pribadi seseorang dan bermuara kepada aksi penipuan atau tindak kriminal pornografi, menguatkan wacana pentingnya pembuatan aturan hukum untuk melindungi data pribadi.²²

¹⁹ Greenleaf, G. *Global data privacy laws: 89 countries, and accelerating. Privacy Laws & Business International Report*, 2012 Hlm 115.

²⁰ Committee, U. H. R. *CCPR general comment No. 16: Article 17 (right to privacy), the right to respect of privacy, family, home and correspondence, and protection of honour and reputation*. April 1988.

²¹ Makarim, E. *Kompilasi hukum telematika*. Divisi Buku Perguruan Tinggi, RajaGrafindo Persada 2003 Hlm 14

²² Djafar, W., & Komarudin, A. *Perlindungan Hak Atas Privasi Di Internet-Beberapa Penjelasan Kunci*. Elsam, Jakarta. 2004 Hlm 3

Perlindungan data pribadi adalah konsep yang sangat penting dalam era digital ini di mana informasi pribadi sering kali disimpan dan diproses secara daring. Teori perlindungan data pribadi mencakup sejumlah prinsip dan praktek yang dirancang untuk melindungi privasi individu. Berikut adalah beberapa teori dan konsep utama yang terkait dengan perlindungan data pribadi:

1. Prinsip Keterbukaan (*Transparency*): Organisasi yang mengumpulkan data pribadi harus transparan mengenai cara mereka mengumpulkan, menggunakan, dan membagikan informasi tersebut. Ini termasuk memberikan informasi kepada individu mengenai tujuan pengumpulan data dan cara data tersebut akan diproses.
2. Prinsip Keterbatasan Penggunaan Tujuan (*Purpose Limitation*): Data pribadi hanya boleh dikumpulkan dan diproses untuk tujuan yang jelas dan sah. Penggunaan data sebaiknya terbatas pada tujuan awal pengumpulan dan tidak boleh digunakan secara tidak sah atau tidak relevan.
3. Prinsip Minimasi Data (*Data Minimization*): Organisasi harus mengumpulkan hanya data pribadi yang diperlukan untuk mencapai tujuan yang ditentukan. Hal ini mengurangi risiko potensial dan melindungi privasi individu.
4. Konsent (*Consent*): Pengumpulan dan penggunaan data pribadi sebaiknya didasarkan pada izin atau persetujuan dari individu terkait. Individu harus diberikan informasi yang cukup untuk membuat keputusan informasi mengenai penggunaan data pribadi mereka.
5. Keamanan Data (*Data Security*): Organisasi harus mengambil langkah-langkah yang memadai untuk melindungi data pribadi dari akses yang tidak sah,

penggunaan yang tidak sah, atau perubahan yang tidak sah. Ini mencakup keamanan teknis dan organisasi.

6. Hak Individu (*Individual Rights*): Individu memiliki hak untuk mengakses, memperbaiki, menghapus, atau membatasi penggunaan data pribadi mereka. Mereka juga memiliki hak untuk mengetahui siapa yang memiliki akses ke data mereka dan bagaimana data tersebut digunakan.
7. Pemindahan Data (*Data Portability*): Individu memiliki hak untuk mentransfer data pribadi mereka dari satu layanan atau organisasi ke layanan atau organisasi lainnya.
8. Pengawasan Otoritas (*Supervisory Authority*): Perlindungan data biasanya melibatkan otoritas pengawasan yang bertugas mengawasi implementasi dan penegakan kebijakan perlindungan data.
9. Privasi Secara Default (*Privacy by Design*): Prinsip ini mendorong pengembang dan organisasi untuk memasukkan perlindungan privasi dalam desain produk dan layanan mereka sejak awal.
10. Akuntabilitas (*Accountability*): Organisasi bertanggung jawab untuk memastikan bahwa mereka mematuhi prinsip-prinsip perlindungan data pribadi dan harus dapat membuktikan kepatuhan mereka.

Teori dan prinsip ini membentuk dasar bagi regulasi perlindungan data, seperti General Data Protection Regulation (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi (UU PDP) di beberapa negara, yang memberikan kerangka kerja hukum untuk melindungi privasi individu dalam konteks penggunaan data pribadi.

B. Tinjauan Umum Tentang Unsur-unsur dalam UU Perlindungan Data Pribadi dan Ancaman Hukuman Tindak Pidana UU Perlindungan Data Pribadi

1. Unsur-unsur dalam UU Perlindungan Data Pribadi

Data Pribadi terdiri atas: Data Pribadi yang bersifat spesifik data dan informasi kesehatan; data biometrik; data genetika; catatan kejahatan; data anak; data keterangan pribadi; dan/ atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Data Pribadi yang bersifat umum nama lengkap; jenis kelamin; kewarganegaraan agama; status perkawinan; dan/ atau data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Data Pribadi yang bersifat umum nama lengkap; jenis kelamin; kewarganegaraan agama; status perkawinan; dan/ atau data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.²³

Ada empat unsur penting dalam undang-undang no 27 tahun 2022, yaitu pemilik data, pengguna data, aliran data, dan keamanan data. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) di Indonesia memuat beberapa unsur pidana terkait data pribadi. Beberapa elemen kriminal utama dalam undang-undang ini mencakup penggunaan data pribadi yang disengaja dan melanggar hukum, kegagalan melindungi data pribadi, dan sanksi administratif atas pelanggaran data. Undang-undang mengatur bahwa penggunaan data pribadi yang disengaja dan melanggar hukum dapat mengakibatkan hukuman penjara paling lama 5 tahun dan/atau denda. Di sisi lain, kegagalan dalam melindungi data pribadi dapat mengakibatkan pengenaan sanksi administratif. Elemen-elemen

²³ Pasal 4 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

tersebut bertujuan untuk menjamin kedaulatan data pribadi dan mencegah pelanggaran data di Indonesia.

Menurut UU Pelindungan Data Pribadi, setiap orang dilarang secara melawan hukum: memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi; mengungkapkan data pribadi yang bukan miliknya; menggunakan data pribadi yang bukan miliknya; membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain.

2. Ancaman Hukuman Tindak Pidana UU Perlindungan Data Pribadi

Penggunaan teknologi informasi ini yang telah berpengaruh terhadap setiap sikap dan perilaku dari anggota masyarakat, bahkan akibatnya juga telah membentuk masyarakat dunia baru yang tidak lagi dihalangi oleh batas-batas teritorial suatu negara yang dahulu ditetapkan sangat esensial sekali, yaitu “dunia mayantara” (dunia yang tanpa batas) atau “realitas virtual” (virtual reality).²⁴

Sebagaimana diatur dalam ketentuan Pasal 1365 setiap perbuatan yang melawan hukum dan menimbulkan kerugian bagi orang lain dapat dimintakan pertanggungjawaban terhadap pelakunya. Jika kita berpedoman pada dasar hukum tersebut maka saat kita mengalami kerugian baik materiil maupun immateriil akibat adanya penyalahgunaan ataupun kebocoran terhadap data pribadi kita hal tersebut

24 Sumangat Salomo Sidauruk, July Esther, Herlina Manullang, KEBIJAKAN HUKUM PIDANASEBAGAI UPAYA MEMINIMALISIR TINDAK PIDANA BULLYING DI MEDIA ELEKTRONIK, Jurnal

merupakan hal yang legal. Pada prinsipnya seseorang yang menyimpan data pribadi wajib memastikan sistem keamanannya dengan baik dan memastikan tidak terjadinya kebocoran terhadap data pribadi seseorang yang dimilikinya. Atas dasar tersebut apabila terjadinya suatu sengketa karena adanya kebocoran data pribadi seseorang maka pihak yang dirugikan tersebut dapat menuntut pertanggungjawaban kepada Penyelenggara Sistem Elektronik atau pihak yang bertanggungjawab atas kerahasiaan data pribadi yang disimpannya. Hal tersebut merupakan implementasi ketentuan Pasal 26 Undang-Undang Informasi dan Transaksi Elektronik yang menyatakan bahwa penggunaan informasi yang menyangkut data pribadi seseorang wajib memperoleh persetujuan dari yang bersangkutan kecuali diatur sebaliknya sesuai dengan ketentuan peraturan perundang-undangan.

Mengacu pada UU Nomor 27 Tahun 2022, Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi dipidana penjara paling lama 5 tahun dan/atau pidana denda paling banyak Rp5 miliar.²⁵ Sementara bagi orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya, diancam dengan pidana penjara maksimal empat tahun dan/atau denda paling banyak Rp 4 miliar.²⁶ Adapun untuk orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya akan dipidana

²⁵ Pasal 67 ayat 1 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

²⁶ Pasal 67 ayat 2 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

paling lama lima tahun penjara dan/atau denda paling banyak Rp 5 miliar.²⁷ Setiap orang yang dengan sengaja membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain dipidana penjara paling lama 6 tahun dan/atau pidana denda paling banyak Rp6 miliar.²⁸ Penyalahgunaan wewenang dapat di sebut melakukan sesuatu diluar batas kekuasaan atau wewenang. Adanya perilaku menyimpang yang tidak selaras dalam melaksanakan tugas dan fungsi dengan maksud menguntungkan diri sendiri atau orang lain.²⁹

Jeratan pidana juga mengincar orang yang dengan sengaja memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain. Pelaku yang melakukan hal ini dapat dipidana paling lama enam tahun penjara dan/atau denda paling banyak Rp 6 miliar.

Selain dijatuhi pidana-pidana ini, pelaku juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian. Jika perbuatan tersebut dilakukan oleh korporasi maka pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/ atau korporasi. Pidana

²⁷ Pasal 67 ayat 3 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

²⁸ Pasal 68 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

²⁹ Togu Oktavianus Simbolon, July Esther, Jinner Sidauruk, PERTANGGUNGJAWABAN PIDANA

KOMITE SEKOLAH YANG MENYALAHGUNAKAN WEWENANG SEHINGGA TERJADINYATINDAK PIDANA KORUPSI YANG DILAKUKAN SECARA BERSAMA-SAMA, Jurnal Hukum, Volume

yang dapat dijatuhkan terhadap korporasi hanya pidana denda yang besarnya paling banyak sepuluh kali dari maksimal pidana denda yang diancamkan. Selain itu, korporasi juga dapat dijatuhi pidana tambahan berupa:

1. perampasan keuntungan dan/ atau harta kekayaan yang diperoleh atau hasil dari tindak pidana;
2. pembekuan seluruh atau sebagian usaha korporasi;
3. pelarangan permanen melakukan perbuatan tertentu;
4. penutupan seluruh atau sebagian tempat usaha dan/ atau kegiatan korporasi; melaksanakan kewajiban yang telah dilalaikan;
5. pembayaran ganti kerugian;
6. pencabutan izin; dan/atau
7. pembubaran korporasi.³⁰

C. Tinjauan Umum Tentang Dampak UU Perlindungan Data Pribadi dalam Era Teknologi Informasi

1. Dampak Positif UU Perlindungan Data Pribadi dalam Era Teknologi Informasi

Undang-Undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP) telah resmi ditandatangani Presiden Joko Widodo. UU PDP mengatur berbagai ketentuan dari jenis-jenis data pribadi, pemrosesan hingga sanksi tercantum dalam UU PDP.

³⁰ Pasal 70 ayat 4 Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

Kehadiran UU PDP sangat dibutuhkan mengingat transaksi data yang saat ini sudah bersifat lintas batas. Sehingga, tidak hanya pemangku kepentingan Indonesia saja yang tersentuh UU PDP. Melainkan pihak asing khususnya swasta yang menghimpun data pribadi di Indonesia juga berkepentingan terhadap UU ini.

Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika, Semuel Abrijani Pangerapan, memaparkan terdapat beragam manfaat penting yang hadir dengan UU PDP. Ragam manfaat penting UU PDP antara lain dapat memberi perlindungan hak fundamental masyarakat, sebagai payung hukum yang komprehensif, berperan mendorong reformasi praktik pemrosesan data pribadi baik sektor publik dan privat, sebagai upaya tingkatkan standar industri.

Undang-undang ini dimaksudkan untuk mengatur pengumpulan, penyimpanan, pembagian, penggunaan, dan perlindungan data pribadi oleh lembaga pemerintah dan organisasi swasta di Indonesia. Ini juga bertujuan untuk memberikan transparansi tentang bagaimana data pribadi dikumpulkan, disimpan, dilindungi, dan dibagikan. Ini juga melindungi hak dan kepentingan individu sehubungan dengan data pribadi mereka. Undang-undang tersebut menguraikan data mana yang harus dilindungi oleh undang-undang, serta pihak mana yang bertanggung jawab untuk melakukannya. Ini juga menguraikan hukuman untuk ketidakpatuhan dengan persyaratan ini. Penerapan undang-undang tersebut akan mengarah pada tata pemerintahan yang lebih baik di Indonesia, yang pada akhirnya akan bermanfaat bagi rakyatnya.

Undang-Undang Perlindungan Data Pribadi (PDP) memiliki dampak positif yang signifikan dalam era Teknologi Informasi. Beberapa dampak positif utamanya termasuk:

1. **Perlindungan Privasi Individu:** UU PDP memberikan perlindungan yang lebih baik terhadap privasi individu. Dengan mengatur cara pengumpulan, pemrosesan, dan penyimpanan data pribadi, undang-undang ini membantu mencegah penyalahgunaan informasi pribadi oleh pihak ketiga.
2. **Mendorong Keamanan Data:** UU PDP mendorong organisasi untuk mengimplementasikan tindakan keamanan data yang lebih baik. Ini mencakup penggunaan langkah-langkah keamanan teknologi informasi, enkripsi, dan kontrol akses untuk melindungi data pribadi dari akses yang tidak sah atau kebocoran.
3. **Kepercayaan Publik:** Dengan memberikan jaminan terhadap privasi dan keamanan data pribadi, UU PDP dapat meningkatkan kepercayaan publik terhadap layanan dan produk yang memanfaatkan data pribadi. Kepercayaan ini penting untuk perkembangan ekosistem bisnis dan inovasi teknologi.
4. **Pengendalian Hak Individu:** UU PDP memberikan kontrol lebih kepada individu terkait data pribadinya. Hak-hak seperti hak untuk mengakses, memperbarui, dan menghapus data mereka memberikan individu kendali atas informasi pribadi mereka.
5. **Promosi Inovasi:** Dengan memberikan kerangka kerja hukum yang jelas dan terinci untuk pengelolaan data, UU PDP dapat merangsang inovasi dalam

pengembangan teknologi. Penggunaan data yang sah dan etis didorong, membuka pintu untuk pengembangan teknologi yang bermanfaat.

6. Pemberdayaan Individu untuk Keputusan yang Berinformasi: Hak individu untuk mendapatkan informasi tentang pengumpulan dan penggunaan data mereka memungkinkan mereka membuat keputusan yang lebih informasional dan memiliki kontrol atas data pribadi mereka.

Pada dasarnya, UU Perlindungan Data Pribadi membantu menciptakan lingkungan yang sehat dan aman dalam pengelolaan data pribadi di era Teknologi Informasi, menciptakan keseimbangan antara inovasi teknologi dan perlindungan hak privasi individu. Di zaman digital yang sekarang, terdapat banyak tindak kejahatan yang menggunakan data pribadi sebagai alat atau sasaran, sehingga perlindungannya perlu ditingkatkan. Sayangnya, banyak orang tidak menyadari bahwa informasi pribadi mereka rentan disalahgunakan oleh pihak yang tidak bertanggung jawab. Di Indonesia, kurangnya upaya perlindungan data telah mengakibatkan serangkaian insiden peretasan dan kebocoran data yang meluas. Kejadian-kejadian semacam ini merupakan bentuk kejahatan di dunia digital, seperti peretasan akun media sosial dan pencurian identitas, yang memiliki potensi untuk mengakibatkan pelanggaran data pribadi, pemerasan, dan penipuan online. Kesadaran akan pentingnya regulasi yang mengatur perlindungan data pribadi secara bertahap mulai diperhatikan oleh

pemerintah, yang tercermin dalam upaya mereka untuk menyusun dan mengesahkan Undang-Undang Nomor 27 tahun 2022.³¹

2. Dampak Negatif UU Perlindungan Data Pribadi dalam Era Teknologi Informasi

Pada masa ini adanya kemajuan internet dan teknologi telah terintegrasi dalam semua bidang kehidupan manusia. Dampak positif dari adanya kemajuan teknologi tersebut adalah dunia menjadi seolah-olah tanpa sekat. Setiap individu dapat melakukan kegiatannya dengan lebih praktis dan sistematis. Namun dari sekian banyak dampak positif tentu adanya bayang-bayang dampak negatif yang timbul akibat adanya kemajuan teknologi di Indonesia. Karena dunia ini menjadi seolah-olah tanpa batasan, salah satu dampak negatif yang timbul adalah adanya kemungkinan untuk terbukanya informasi yang bersifat rahasia berkaitan dengan data pribadi yang dimiliki oleh masing-masing individu dan membawa kerugian secara materiil dan immateriil. Data pribadi merupakan informasi tunggal atau sekumpulan informasi baik yang bersifat rahasia ataupun tidak yang diberikan oleh pemilik data pribadi/konsumen dan dihimpun ke dalam sistem elektronik yang diproses oleh penyelenggara sistem elektronik untuk dipergunakan sesuai tujuan dan kegunaannya serta apabila disalahgunakan maka pemilik dapat

³¹ Albert Lodewyk Sentosa Siahaan, "Urgensi Perlindungan Data Pribadi Di Platform Marketplace Terhadap Kemajuan Teknologi," *Majalah Hukum Nasional* 52, no. 2 (2022): 210–22, <https://doi.org/10.33331>.

menyelesaikannya melalui jalur hukum baik administrasi, perdata, maupun pidana.³²

Perkembangan teknologi informasi yang pesat dewasa ini memberikan pengaruh yang luar biasa terhadap kehidupan manusia. Perkembangan teknologi informasi tersebut kemudian mempunyai dampak negatif disamping juga mempunyai dampak positif. Dampak positif yang ditimbulkan oleh teknologi informasi antara lain memudahkan orang untuk berinteraksi secara langsung melalui media internet. Akan tetapi kemudahan tersebut telah menciptakan efek negatif berupa penyalahgunaan data pribadi. Perlindungan hukum terhadap data pribadi penting untuk dipikirkan mengingat begitu cepatnya pertumbuhan teknologi telah memberikan kemudahan bagi para pihak dalam melakukan pengumpulan, analisa maupun menyebarkan informasi dengan berbagai cara.³³ Sebuah data akan dikategorikan sebagai data pribadi manakala data tersebut berkaitan dengan seseorang yang dengannya orang tersebut dapat diidentifikasi sebagai pemilik data.³⁴

Meskipun Undang-Undang Perlindungan Data Pribadi bertujuan untuk melindungi privasi individu dalam era teknologi informasi, terdapat beberapa dampak negatif yang mungkin muncul. Berikut adalah beberapa dampak potensial:

1. Ketidaknyamanan Bisnis:

³² Rizky P.P. Karo-karo Pengaturan Perlindungan Data Pribadi di Indonesia Perspektif Teori Keadilan Bermartabat, Nusamedia. 2020 hal.185.

³³ Sinta Dewi, Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia, Jurnal Yustisia, Volume 5 No. 1 2016, Hal. 22 – 30, DOI: <https://doi.org/10.20961/yustisia.v5i1.8712>

³⁴ Sugeng, Hukum Telematika Indonesia, Kencana, Jakarta, 2020, Hal. 56

UU Perlindungan Data Pribadi dapat menimbulkan beban administratif tambahan bagi perusahaan. Mereka harus mengimplementasikan kebijakan dan prosedur yang ketat untuk memastikan kepatuhan dengan undang-undang tersebut.

2. Biaya Tinggi:

Penerapan kebijakan keamanan data yang ketat dan pemenuhan persyaratan undang-undang dapat memerlukan investasi yang signifikan dalam sumber daya teknologi, pelatihan, dan keamanan data. Hal ini dapat menjadi beban keuangan bagi bisnis, terutama yang kecil dan menengah.

3. Pembatasan Inovasi:

Beberapa perusahaan mungkin merasa terbatas dalam pengumpulan dan pengolahan data untuk inovasi produk dan layanan baru. Pembatasan ini dapat menghambat kemampuan bisnis untuk memanfaatkan potensi penuh data yang mereka miliki.

4. Ketidakjelasan Hukum:

Dalam beberapa kasus, interpretasi undang-undang yang tidak jelas atau ambigu dapat menyebabkan ketidakpastian hukum. Ini dapat membuat perusahaan kesulitan memahami persyaratan undang-undang dengan benar dan menerapkannya dengan konsisten.

5. Peningkatan Biaya Keamanan:

Perusahaan mungkin perlu meningkatkan infrastruktur keamanan mereka untuk melindungi data pribadi pelanggan. Hal ini bisa termasuk investasi dalam keamanan jaringan, enkripsi data, dan solusi keamanan lainnya.

6. Penurunan Efisiensi:

Penerapan langkah-langkah keamanan tambahan untuk mematuhi undang-undang dapat menyebabkan penurunan efisiensi operasional. Proses-proses yang sebelumnya lebih cepat dan mudah bisa menjadi lebih rumit dan lambat.

7. Kesulitan Penyelesaian Perselisihan:

Proses penyelesaian perselisihan terkait pelanggaran privasi dapat menjadi rumit dan mahal. Ini dapat memberikan beban tambahan pada sistem peradilan dan berpotensi memperlambat proses penegakan hukum.

8. Pengumpulan Data yang Terbatas:

Seiring dengan upaya melindungi privasi, UU Perlindungan Data Pribadi dapat membatasi kemampuan perusahaan untuk mengumpulkan data yang diperlukan untuk meningkatkan pengalaman pengguna atau menyediakan layanan yang lebih personal.

Data pribadi yang melekat pada diri seseorang merupakan salah satu hak yang harus dilindungi. Data pribadi merupakan bagian dari privasi seseorang. Secara umum terdapat tiga aspek dalam privasi, yaitu privasi yang terkait dengan diri seseorang, privasi tentang data seseorang dan privasi atas komunikasi seseorang.³⁵

Penggunaan data oleh seseorang oleh pemerintah maupun swasta, badan usaha maupun perseorangan tanpa ijin merupakan pelanggaran privasi seseorang.³⁶ Oleh karenanya data pribadi harus dilindungi.

³⁵ Edmon Makarim, Pengantar Hukum Telematika, Raja Grafindo Persada, Jakarta, 2005, Hal. 160

³⁶ Harun Mukhtar, Kriptografi Untuk Keamanan Data, Deepublish, Sleman, 2018, Hal. 8

BAB III

METODOLOGI PENELITIAN

A. Ruang Lingkup Penelitian

Penelitian hukum pada dasarnya merupakan suatu kegiatan ilmiah yang didasarkan pada metode, sistematika, dan pemikiran tertentu yang bertujuan untuk mempelajari suatu atau beberapa gejala hukum tertentu dengan cara menganalisa, maka juga diadakan pemeriksaan yang mendalam terhadap fakta hukum tersebut untuk demikian mengusahakan suatu pemecahan atas permasalahan-permasalahan yang timbul dalam gejala bersangkutan.³⁷

Ruang lingkup ini adalah bertujuan untuk membatasi permasalahan yang akan dibahas dalam penelitian ini. Adapun ruang lingkup penelitian dalam penulisan ini adalah mengenai ketentuan hukum dalam uu data pribadi dan tantangan implementasinya dalam era teknologi informasi.

B. Jenis Penelitian

Adapun jenis penelitian ini yang digunakan peneliti adalah Yuridis Normatif. Penelitian yuridis normatif adalah metode penelitian di bidang hukum yang berfokus pada analisis norma-norma hukum, dokumen hukum, dan teori hukum. Tujuan dari penelitian ini adalah untuk memahami dan mengevaluasi norma-norma hukum yang berlaku serta untuk mengembangkan konsep-konsep hukum.

³⁷ Bambang Sunggono, *Metode Penelitian Hukum*, Ed. 11, Rajawali Pers, Jakarta, 2013, hal, 38.

C. Metode Pendekatan

Metode pendekatan masalah yang digunakan dalam penelitian hukum adalah pendekatan perundang-undangan (*statue approach*). Metode pendekatan perundang-undangan (*statue approach*) yang dilakukan dengan menelaah ketentuan perundang-undangan yang berlaku yaitu Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi

D. Sumber Bahan Hukum

Penelitian ini menggunakan data sekunder yang terdiri dari bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier sebagai berikut:

a. Bahan Hukum Primer, terdiri dari:

- 1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945
- 2) Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.
- 3) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
- 4) Undang-Undang Nomor 36 Tahun 2009 Tentang Kesehatan

b. Bahan Hukum Sekunder Bahan hukum sekunder, yaitu bahan hukum yang memberikan penjelasan mengenai bahan hukum primer seperti buku-buku, karya tulis para ahli hukum, skripsi, jurnal, makalah, dan media elektronik yang relevan dengan penelitian ini khususnya pembahasan mengenai hukum pidana yang akan memberikan petunjuk kemana penelitian ini diarahkan.

c. Bahan Hukum Tersier Bahan hukum tersier yaitu bahan-bahan yang digunakan guna menunjang dan memberikan petunjuk maupun penjelasan atas bahan hukum primer dan bahan hukum sekunder, seperti kamus, wikipedia, dan ensiklopedia.

E. Metode Penelitian

Penelitian ini menggunakan metode penelitian normatif, Metode penelitian normatif digunakan untuk menganalisis dan mengevaluasi norma-norma hukum, peraturan, dan dokumen hukum lainnya. Metode penelitian ini dapat disebut juga sebagai penelitian hukum doktriner atau penelitian perpustakaan. Dinamakan sebagai penelitian hukum doktriner dikarenakan penelitian ini hanya ditujukan pada peraturan-peraturan tertulis sehingga penelitian ini sangat erat hubungannya pada perpustakaan karena akan membutuhkan data-data yang bersifat sekunder pada perpustakaan.

F. Analisis Bahan Hukum

Dalam penelitian ini analisis data yang digunakan adalah analisis data kualitatif yaitu dengan menganalisa Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, yang selanjutnya diuraikan dalam bentuk kalimat-kalimat yang tersusun secara sistematis, kemudian dilakukan pembahasan dan penafsiran yang pada akhirnya dapat ditarik kesimpulan tentang masalah-masalah yang diteliti