



Perlindungan Hukum dan Kepastian Hukum terhadap Perdagangan Data Pribadi dalam UU PDP

Muhammad Rizky^{1*}, Rini Apriyani², Nur Aripkiah³

¹⁻³ Fakultas Hukum, Universitas Mulawarman, Indonesia

*Penulis Korespondensi: mhmmmd.151.rizky@gmail.com *

Abstract: Article 20 of the Personal Data Protection Law (PDP Law) normatively regulates the protection of data subjects and constitutes a pivotal provision that underscores the principle of consent as the legal basis for the processing of personal data for commercial purposes. This normative framework safeguards individuals' right to privacy, encompassing the validity of explicit consent, the right to withdraw such consent, and the accountability of data controllers. In parallel, Articles 65 to 70 of the PDP Law substantively establish various categories of criminal offenses within the context of personal data protection. These include the unlawful acquisition, disclosure, processing, falsification, and utilization of personal data. Collectively, these provisions reflect the State's commitment to ensuring criminal legal protection against violations of personal data. This research adopts a doctrinal legal methodology with a descriptive-normative approach to address two primary issues: First, to examine and identify the scope of legal protection concerning the trade of personal data under the PDP Law; and Second, to assess and determine the degree of legal certainty afforded to the trade of personal data within the framework of the PDP Law. Notwithstanding the protective intent embodied in Article 20—particularly concerning the commercial use of personal data—this provision gives rise to legal uncertainty due to the absence of comprehensive regulatory clarity on several critical aspects. Similarly, Articles 65 to 70 continue to exhibit significant legal ambiguities, particularly with respect to the constituent elements of offenses, the definition of harm, corporate liability, regulatory overlap with other legislative instruments, and the lack of clear enforcement mechanisms and implementing institutions.

Keywords: Consent; Criminal Offenses; Data Controllers; Data Subjects; Privacy Rights.

Abstrak: Pasal 20 UU PDP mengatur perlindungan subjek data secara normatif dan merupakan pasal penting yang menekankan prinsip persetujuan sebagai dasar pemrosesan data pribadi untuk tujuan komersial. Norma ini melindungi hak privasi individu. Meliputi keabsahan persetujuan eksplisit, hak pencabutan, dan tanggung jawab pengendali data. Dan pada Pasal 65–70 UU PDP secara substantif telah mengatur berbagai bentuk pelanggaran pidana dalam konteks perlindungan data pribadi, termasuk perolehan, pengungkapan, pemrosesan, hingga pemalsuan dan penggunaan data ilegal. Menunjukkan komitmen negara dalam memberikan perlindungan hukum pidana terhadap pelanggaran data pribadi. Penelitian ini menggunakan penelitian doktrinal dengan pendekatan deskriptif-normatif untuk menjawab dua hal yaitu: Pertama, untuk mengetahui dan mengidentifikasi perlindungan hukum perdagangan data data pribadi dalam UU PDP. Kedua, untuk mengetahui dan mengidentifikasi kepastian hukum perdagangan data pribadi dalam UU PDP. Meskipun Pasal 20 UU PDP bertujuan memberikan perlindungan yang kuat terhadap penggunaan data pribadi untuk kepentingan komersial, norma tersebut masih menimbulkan ketidakpastian hukum karena banyak aspek krusial yang belum diatur secara jelas. Dan Pasal 65-70 ini masih mengandung ketidakpastian hukum yang signifikan, baik dari sisi unsur delik, bentuk kerugian, pertanggungjawaban korporasi, tumpang tindih dengan peraturan lain dan ketiadaan mekanisme penegakan dan lembaga pelaksanaan.

Kata Kunci: Hak Privasi; Pengendali Data; Persetujuan; Subjek Data; Tindak Pidana.

1. LATAR BELAKANG

Ketentuan mengenai perlindungan privasi dan data pribadi merupakan amanah Pasal 28 G Undang-Undang Dasar Republik Indonesia Tahun 1945 yang mengatur hak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya. Untuk dapat melihat ketentuan tersebut sebagai ketentuan mengenai privasi dan data pribadi, pendapat Warren dan Brandeis dalam karyanya yang berjudul “The Right to Privacy”

menyatakan bahwa privasi adalah hak untuk menikmati kehidupan dan hak untuk dihargai perasaan dan pikirannya. Perlindungan privasi berhubungan erat dengan pemenuhan hak data pribadi. Hubungan mengenai privasi dan perlindungan data pribadi ditegaskan oleh Allan Westin, mendefinisikan privasi sebagai hak orang, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain. Definisi yang dikemukakan oleh Westin disebut dengan *information privacy* karena menyangkut informasi pribadi.

Di bawah Pasal 28 G Undang-Undang Dasar 1945, perlindungan data pribadi di Indonesia tersebar di berbagai undang-undang. Kemudian, perlindungan data pribadi dimuatkan salah satu bentuk dari perlindungan privasi yang merupakan bagian penting dalam Konstitusi Negara Republik Indonesia yang mengatur penghormatan atas nilai-nilai HAM dan nilai-nilai persamaan serta penghargaan atas hak perseorangan sehingga perlu diberikan landasan hukum untuk lebih memberikan keamanan privasi dan data pribadi. (Prastyanti, 2025)

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi telah disahkan oleh Presiden Republik Indonesia pada 17 Oktober 2022 dengan harapan mampu untuk melindungi data pribadi masyarakat yang dikelola oleh penyelenggara sistem elektronik yaitu kominfo dan mencegah penyalahgunaan oleh individu yang tidak bertanggung jawab. Fokus utamanya harus pada pentingnya penyelesaian masalah aliran data, dan solusi yang aman dan terjamin harus segera ditemukan.

Hal ini disebabkan oleh perkembangan teknologi dan internet yang terus berkembang dan selalu dikaitkan dengan kejahatan. Perlindungan data merupakan kebutuhan masyarakat untuk menciptakan keamanan dalam berinteraksi dengan teknologi dan internet. Kejahatan dunia maya mempunyai dampak yang signifikan terhadap individu, kelompok, dan negara. Kerugian ini dapat mencakup bidang ekonomi, perbankan, politik, dan bahkan keamanan nasional. (R, 2023)

Dengan disahkannya Undang-Undang Perlindungan Data Pribadi ini diharapkan dapat menjadi solusi efektif terhadap permasalahan penyaringan data pribadi yang sering terjadi di Indonesia. Undang-Undang Data Pribadi dibuat untuk melindungi privasi. Dalam Naskah Akademik Undang-Undang Perlindungan Data Pribadi, dijelaskan bahwa “hak atas privasi melalui perlindungan data pribadi merupakan elemen kunci bagi kebebasan dan martabat individu”. Oleh karena itu, tujuan disahkannya Peraturan Perlindungan Data Pribadi ini adalah untuk melindungi kepentingan masyarakat untuk mencegah penyalahgunaan data pribadinya. (Suriaatmadja, 2023)

2. KAJIAN TEORITIS

Kajian ini membahas fenomena perdagangan data pribadi yang semakin marak di Indonesia, seiring dengan perkembangan teknologi informasi dan ekonomi digital, di mana data pribadi individu diperjualbelikan atau dimanfaatkan untuk kepentingan komersial tanpa persetujuan yang sah dari pemilik data. Praktik ini menimbulkan berbagai risiko, seperti pelanggaran hak privasi, kerugian ekonomi, serta penyalahgunaan identitas. Dari perspektif hukum nasional, perdagangan data pribadi pada prinsipnya dilarang dan harus tunduk pada ketentuan peraturan perundang-undangan, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang mengatur hak subjek data, kewajiban pengendali dan prosesor data, serta mekanisme perlindungan dan penegakan hukum.

Perlindungan hukum diberikan melalui pengaturan preventif berupa kewajiban persetujuan yang sah dan pembatasan tujuan pemrosesan data, serta perlindungan represif melalui sanksi administratif, perdata, dan pidana. Kepastian hukum tercermin dari kejelasan norma mengenai larangan pengungkapan dan penggunaan data pribadi secara melawan hukum. Perdagangan data pribadi yang dilakukan tanpa dasar hukum dan tidak memenuhi ketentuan tersebut dapat dinyatakan sebagai perbuatan melawan hukum dan dikenai sanksi sesuai dengan peraturan yang berlaku.

Secara teoritis, perlindungan hukum dan kepastian hukum terhadap data pribadi bertujuan menciptakan keseimbangan antara kepentingan individu dan kepentingan ekonomi pelaku usaha. Negara berperan sebagai regulator dan pengawas agar pemanfaatan data pribadi tidak melanggar hak asasi manusia. Dalam praktiknya, efektivitas perlindungan hukum sangat bergantung pada konsistensi penegakan hukum, kesadaran hukum masyarakat, serta kesiapan institusi pengawas data pribadi.

3. METODE PENELITIAN

Penelitian ini menggunakan Penelitian Doktrinal, adalah penelitian aturan hukum, prinsip, konsep atau doktrin. Ini melibatkan eksposisi sistematis yang teliti, analisis, dan evaluasi kritis terhadap aturan hukum, prinsip, atau doktrin, dan inter-relasinya. Hal ini berkaitan dengan tinjauan kritis terhadap legislasi dan proses pengambilan keputusan serta kebijakan yang mendasarinya. (Purwati, 2020)

Pendekatan normatif-deskriptif perundang-undangan dilakukan dengan menelaah semua undang-undang dan regulasi yang bersangkutan dengan isu hukum yang ditangani yaitu tentang Tinjauan Hukum Pidana Terkait Perdagangan Data Pribadi Di Indonesia. Dan juga

peneliti akan menghubungkan antara statute approach dan teori-teori hukum relevan yang dipakai dalam menentukan hasil penelitian.

4. HASIL DAN PEMBAHASAN

Perlindungan Hukum terhadap Perdagangan Data Pribadi

Pasal 20 UU PDP dalam konteks perdagangan data pribadi

Pasal 20 UU PDP merupakan salah satu aturan penting untuk melindungi subjek data terkait data pribadinya. Karena aturan ini menekankan perlindungan terhadap data pribadi baik berupa pemrosesan ataupun pemanfaatan data pribadi subjek data untuk kepentingan apapun melalui dasar hukum persetujuan. Yang mana persetujuan memiliki perbedaan dengan perikatan dan perjanjian.

Untuk mengetahui perbedaan perikatan, perjanjian, dan persetujuan perlu memahami definisinya masing-masing. Dalam Hukum Perjanjian membedakan pengertian perjanjian dengan perikatan. Subekti menyatakan bahwa hubungan antara perikatan dan perjanjian adalah perjanjian itu menerbitkan perikatan. Kemudian, perjanjian adalah sumber perikatan, di samping sumber-sumber lain. Suatu perjanjian juga dinamakan persetujuan, karena dua pihak itu setuju untuk melakukan sesuatu.

Perjanjian dan persetujuan pada esensinya memiliki makna yang sama, yaitu peristiwa hukum di mana dua pihak atau lebih saling mengikatkan diri untuk berbuat atau tidak berbuat sesuatu, yang melahirkan adanya hubungan hukum. Dari perjanjian dan persetujuan, lahirlah sebuah perikatan. Perikatan lebih luas cakupannya dari perjanjian/persetujuan, karena perikatan terlahir tak hanya lahir dari perjanjian/persetujuan, namun perikatan juga lahir dari undang-undang.

Sehingga, persamaan dari perikatan dan perjanjian/persetujuan adalah bahwa karena telah saling mengikatkan diri, salah satu pihak berhak menuntut sesuatu hal dari pihak yang lain, dan tuntutan itu wajib dipenuhi pihak yang lain sebagaimana telah disepakati bersama. Sedangkan perbedaannya adalah pada tahapan dan implikasinya. Secara singkat, perjanjian/persetujuan/kontrak melahirkan adanya sebuah perikatan. (Subekti, 1984)

a. Persetujuan Dalam Pasal 20 UU PDP

Persetujuan Penggunaan Data Pribadi Untuk Kepentingan komersial terdapat pada pasal 20:

- 1) Penggunaan Data Pribadi oleh Pengendali Data Pribadi untuk kepentingan pelayanan publik, kepentingan komersial, dan/atau kepentingan lainnya wajib berdasarkan persetujuan eksplisit dari Subjek Data Pribadi.

- 2) Pengendali Data Pribadi wajib menghentikan Pemrosesan Data Pribadi untuk kepentingan komersial apabila Subjek Data Pribadi mencabut persetujuan sebagaimana dimaksud ayat 1.

b. Sifat dan Kekuatan Norma

Pasal 20 merupakan norma Imperatif, berupa perintah yang secara apriori harus ditaati, baik berupa suruhan maupun larangan. (Soekanto, 1982) Maka perintah hukum yang mewajibkan Pengendali Data Pribadi untuk mendapatkan persetujuan eksplisit dari subjek data sebelum menggunakan data pribadi untuk kepentingan komersial. Hal ini memperlihatkan adanya prinsip legalitas perlindungan hak individual, yang mengutamakan kendali subjek data atas pemrosesan datanya.

c. Makna dan Ruang Lingkup “Kepentingan Komersial”

Istilah kepentingan komersial dalam Pasal 20 tidak dijelaskan secara eksplisit dalam UU PDP, sehingga memerlukan tafsir sistematis. Secara umum, kepentingan komersial merujuk pada segala bentuk pemanfaatan data pribadi yang ditujukan untuk keuntungan ekonomi, seperti:

- 1) Penawaran produk atau jasa (direct marketing)
- 2) Penyusunan profil konsumen (profiling)
- 3) Personalisasi iklan atau konten digital
- 4) Penjualan data pribadi kepada pihak ketiga (data brokerage).

d. Persetujuan Eksplisit sebagai Dasar Hukum

UU PDP mensyaratkan bahwa persetujuan harus eksplisit, yaitu persetujuan yang diberikan secara tertulis, lisan, atau melalui tindakan nyata (aktif), setelah subjek data diberikan informasi secara lengkap dan jelas. Dengan demikian, persetujuan:

- 1) Tidak boleh bersifat otomatis atau tersirat
- 2) Harus diperoleh melalui tindakan sadar dari subjek data
- 3) Harus memuat informasi tentang jenis data, tujuan, dan pihak yang memproses data

Maka penggunaan metode persetujuan yang kabur seperti satu klik menyetujui semua tidak memenuhi unsur legalitas pemrosesan data pribadi menurut Pasal 20.

e. Hak Mencabut Persetujuan dan Kewajiban Pengendali

Ayat (2) Pasal 20 memberikan hak kepada subjek data untuk mencabut persetujuan kapan saja, dan mewajibkan pengendali untuk segera menghentikan pemrosesan data, namun dalam praktik, pencabutan persetujuan sering kali sulit dilakukan karena:

- 1) Tidak adanya fitur opt-out yang jelas
- 2) Prosedur yang berbelit-belit atau tidak tersedia

3) Data sudah terlanjur disebarluaskan ke pihak ketiga

UU PDP tidak merinci secara teknis bagaimana pencabutan persetujuan harus difasilitasi yang dapat menyulitkan penegakan hukum, karena tidak ada indikator pelanggaran yang objektif dan standar pembuktian persetujuan masih kabur.

f. Sanksi terhadap Pelanggaran Pasal 20

Jika pengendali memproses data untuk kepentingan komersial tanpa persetujuan eksplisit, maka:

- 1) Dapat dikualifikasikan sebagai pemrosesan data tanpa dasar hukum, yang melanggar Pasal 67 dan Pasal 70 UU PDP
- 2) Dapat dikenai sanksi pidana (penjara maksimal 5 tahun dan/atau denda maksimal Rp50 miliar)
- 3) Selain itu, juga dapat dikenai sanksi administratif berdasarkan Pasal 57–58 UU PDP, seperti teguran tertulis, penghentian sementara aktivitas, hingga denda administratif

Pasal 65–70 UU PDP dalam Konteks Perdagangan Data Pribadi

Perdagangan data pribadi merupakan praktik ilegal yang melibatkan pengumpulan, pemrosesan, dan distribusi data individu untuk tujuan komersial tanpa persetujuan yang sah. Dalam konteks hukum pidana, praktik ini tidak hanya melanggar hak privasi, tetapi juga mengandung unsur perbuatan melawan hukum yang dapat dikenai sanksi pidana.

Pasal 65 sampai dengan Pasal 70 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) mengatur sanksi pidana bagi berbagai bentuk pelanggaran terhadap perlindungan data pribadi. Pasal-pasal ini secara normatif dapat digunakan untuk menjerat pelaku perdagangan data pribadi, baik individu maupun korporasi.

Dalam segi pengertian korporasi memiliki beberapa arti itu sendiri, secara etimologi kata ini berasal dari “Corporatio” dalam bahasa latin. Pada akhirnya ”Corporation” merupakan badan yang dijadikan orang, badan yang diperoleh dengan perbuatan manusia sebagai lawan terhadap badan manusia yang terjadi menurut alam.

Berdasarkan penjabaran diatas ternyata korporasi merupakan badan hasil cipta hukum. Dimana terdiri dari corpus, yang struktur fisiknya dan ke dalam hukum memasukkan unsur animus yang artinya badan hukum itu sendiri memiliki kepribadian sendiri. Sebab produk badan hukum salah satunya adalah ciptaan hukum maka kecuali penciptaanya, kematiannya pun juga ditentukan oleh hukum. (Priyatno, 2010)

a. Pasal 65 – Perolehan atau Pengumpulan Data Tanpa Hak

Pasal 65 mengatur tentang perolehan atau pengumpulan data tanpa hak, yang berbunyi:

“Setiap orang yang dengan sengaja dan tanpa hak memperoleh atau mengumpulkan data pribadi yang bukan miliknya untuk menguntungkan diri sendiri atau orang lain dan dapat merugikan Subjek Data Pribadi...”

Ini adalah tahap awal dalam praktik perdagangan data, yaitu perolehan atau pengumpulan data pribadi yang biasanya dari peretasan, scraping, atau pembelian dari pihak ketiga. Unsur “menguntungkan diri sendiri atau orang lain” langsung mengarah pada tujuan perdagangan. Delik ini bersifat materil, delik materil adalah perbuatan pidana yang perumusannya dititik-beratkan pada akibat yang dilarang. Karena harus ada akibat (kerugian). (S, 2007)

b. Pasal 66 – Pengungkapan Data Pribadi Tanpa Hak

Pasal 66 mengatur tentang pengungkapan data pribadi tanpa hak, yang berbunyi:

“...mengungkapkan Data Pribadi yang bukan miliknya...”

Perdagangan data biasanya disertai dengan pengungkapan atau pemberian akses kepada pihak ketiga (pembeli). Tidak dibutuhkan unsur kerugian, sehingga delik ini lebih mudah dibuktikan dalam konteks transfer data ke luar sistem.

c. Pasal 67 – Pemrosesan Data Tanpa Dasar Hukum

Pasal 67 mengatur tentang pemrosesan data tanpa dasar hukum, yang berbunyi:

“...memproses Data Pribadi secara tidak sah...”

Pemrosesan data untuk diklasifikasikan, disegmentasi, atau dianalisis guna dijual merupakan bentuk pelanggaran jika tidak memiliki dasar hukum. Dalam praktik perdagangan data, pelaku sering mengolah dan memodifikasi data pribadi untuk nilai jual yang lebih tinggi.

d. Pasal 68 – Pemalsuan Data Pribadi

Pasal 68 mengatur tentang pemalsuan data pribadi, yang berbunyi:

“...memalsukan Data Pribadi...”

Dalam praktik jual beli data fiktif, pelaku bisa memalsukan data untuk mengisi form palsu, membuat akun bot, atau memanipulasi informasi untuk dijual. Meskipun tidak dominan dalam perdagangan data riil, pasal ini relevan untuk skema manipulatif berbasis data pribadi palsu.

e. Pasal 69 – Penggunaan Data dari Sumber Ilegal

Pasal 69 mengatur tentang penggunaan data dari sumber ilegal, yang berbunyi:

“...menggunakan data pribadi yang diperoleh dari sumber yang tidak sah...”

Pasal ini menjerat pembeli atau penerima data yang tahu atau patut tahu bahwa data tersebut berasal dari aktivitas ilegal. Ini sangat penting untuk menindak rantai distribusi dan penggunaan data hasil perdagangan gelap.

f. Pasal 70 – Pidana Tambahan

Pasal 70 mengatur tentang pidana tambahan, yang berbunyi:

Pidana tambahan: pengumuman identitas pelaku, perampasan keuntungan, dan penghentian aktivitas.

Dalam konteks perdagangan data, pelaku sering memperoleh keuntungan besar. Pasal 70 memungkinkan perampasan hasil keuntungan dan pemulihan hak subjek data. Yang dapat diterapkan pada korporasi atau pelaku bisnis digital.

Oleh karena itu, beberapa hal-hal penting yang luput dari perhatian, diantaranya penjelasan kepentingan komersial secara eksplisit, seperti kepada siapa data pribadi kita diberikan, bagaimana mereka akan menggunakannya, serta perlu dan pentingnya informasi tersebut kita ketahui dan atas persetujuan kita. Sehingga ketika kita tidak setuju dapat mencabut persetujuan tersebut dan mendapat perlindungan.

Maka UU PDP harus merinci secara jelas teknis pencabutan persetujuan dan bagaimana hal tersebut difasilitasi. Dengan memberi indikator pelanggaran dan standar pembuktian yang jelas. Selain itu komitmen penegakan hukum pidana terhadap pelaku maupun korporasi yang melanggar aturan sebagai bukti nyata negara dalam memberikan perlindungan hukum bagi masyarakat.

Kepastian Hukum Terhadap Perdagangan Data Pribadi

Dengan adanya kepastian hukum dalam suatu negara menjamin terdapatnya upaya pengaturan hukumnya yang terwujud disuatu perundang-undangan yang dibuat oleh pemerintah. Peraturan perundangan tersebut adalah sistem hukum yang berlaku yaitu yang tidak didasarkan pada keputusan sesaat saja. Karena kepastian hukum adalah konsep guna memastikan bahwa hukum itu telah dilaksanakan secara baik dan tidak menimbulkan kerugian bagi pihak manapun. (Syahrani, 1999)

Namun dalam UU PDP terdapat banyak ketidakpastian hukum terkait perdagangan data pribadi, yang dapat menyebabkan tidak berjalannya fungsi dan tujuan hukum pidana. Berikut ini beberapa pasal yang terdapat ketidakpastian dalam pengaturannya.

Pasal 20

Pasal 20 merupakan dasar hukum yang sangat penting dalam UU PDP untuk mengatur penggunaan data pribadi bagi kepentingan komersial, yang lazim terjadi dalam dunia digital saat ini, seperti dalam iklan online, e-commerce, atau penawaran produk berbasis data pengguna. Pasal ini mewajibkan adanya persetujuan eksplisit dari subjek data sebelum data digunakan. Namun dalam pelaksanaannya, pasal ini menimbulkan ketidakpastian hukum

karena sejumlah frasa kunci yang tidak dijelaskan secara normatif maupun teknis operasional dalam UU PDP. Berikut beberapa ketidakpastian hukum pada pasal 20 UU PDP:

a. Tidak adanya definisi “kepentingan komersial”

UU PDP tidak mendefinisikan secara jelas apa yang dimaksud dengan “kepentingan komersial”. Ketidakhadiran definisi formal “kepentingan komersial” dapat menyebabkan celah interpretasi dalam praktik, yang berpotensi disalahgunakan oleh pelaku bisnis digital. Selain itu, penggunaan data untuk analisis perilaku konsumen, iklan tertarget, atau kerja sama penjualan pihak ketiga apakah termasuk?. Dampaknya, menimbulkan ruang interpretasi yang luas bagi pengendali data. Hal ini menyulitkan penegakan hukum karena tidak ada parameter objektif untuk menentukan pelanggaran.

Ketidakjelasan bentuk “persetujuan eksplisit”

Pasal 20 mensyaratkan “persetujuan eksplisit”, namun tidak menjelaskan seperti apa bentuk sah-nya. Dan pada pasal 1 angka 25 menyebutkan bahwa persetujuan eksplisit dapat berupa tertulis, lisan, dan/atau isyarat, tetapi tidak dijelaskan format, mekanisme, maupun validitas digitalnya. Jika terdapat persetujuan apakah penggunaan ini legal?, maka UU PDP tidak melarang perdagangan data kecuali tanpa izin

Dampaknya banyak platform mengklaim telah mendapat “consent” melalui persetujuan default dengan menyetujui kebijakan privasi secara umum, padahal belum tentu memenuhi unsur eksplisit.

b. Tidak diaturnya mekanisme pencabutan persetujuan

Pasal 20 ayat (2) menyatakan bahwa pengendali harus menghentikan pemrosesan jika persetujuan dicabut, namun tidak dijelaskan bagaimana pencabutan dilakukan, dan apa kewajiban teknis pengendali setelah itu. Hal ini menimbulkan kekosongan norma prosedural, yang memerlukan pengaturan lebih lanjut melalui Peraturan Pemerintah atau peraturan teknis lainnya. Dampaknya tanpa mekanisme yang terstandardisasi, hak subjek data untuk menarik persetujuan menjadi tidak efektif, karena tidak tahu harus ke mana, melalui apa, atau apakah permintaannya diproses.

c. Tidak ada jangka waktu atau batasan teknis

Dalam pasal ini, terjadi ketidakpastian hukum karena, UU PDP tidak memberikan batas waktu diantaranya:

- 1) Kapan persetujuan harus diperbarui
- 2) Berapa lama data boleh digunakan setelah dicabut
- 3) Apakah pencabutan berlaku surut (harus hapus data) atau hanya ke depan

Dampaknya menimbulkan ketidakpastian dalam perlindungan karena subjek data tidak mengetahui apakah datanya masih disimpan, diproses, atau disebarluaskan setelah persetujuan dicabut.

d. Belum ada aturan pelaksana

Sampai saat ini, belum ada Peraturan Pemerintah atau Peraturan Otoritas PDP yang mengatur teknis pelaksanaan Pasal 20. Padahal, norma ini sangat teknis dan membutuhkan standarisasi digital, seperti dashboard privasi, log aktivitas pencabutan, dan sistem opt-in/opt-out. Dampaknya pasal ini tidak operasional, meski sudah bersifat wajib. Hal ini mengarah pada norma kosong atau declaratory norm (sekadar menyatakan, tanpa daya laku).

Pasal 65-70

Pasal 65 sampai dengan Pasal 70 UU PDP mengatur mengenai ketentuan pidana atas pelanggaran terhadap hak-hak subjek data pribadi. Ketentuan ini merupakan bentuk perlindungan hukum represif, terutama untuk menangani praktik-praktik seperti penyalahgunaan, pengungkapan tanpa izin, hingga perdagangan data pribadi. Namun, dalam praktiknya, sejumlah norma pidana tersebut menimbulkan ketidakpastian hukum baik dari sisi redaksi norma, pembuktian delik, maupun tumpang tindih dengan regulasi lain, yang pada akhirnya berpotensi menghambat penegakan hukum secara efektif.

a. Ketidakjelasan Unsur Delik dalam Pasal 65

“Setiap orang yang dengan sengaja dan tanpa hak memperoleh atau mengumpulkan data pribadi...”

Permasalahannya, Tidak dijelaskan apa yang dimaksud dengan “tanpa hak”. Apakah harus dibuktikan dengan ketiadaan izin, tidak ada kontrak, atau pelanggaran kebijakan privasi? Serta Tidak dijelaskan standar “menguntungkan diri sendiri atau orang lain”, apakah sekadar potensi keuntungan sudah cukup, atau harus ada hasil nyata?

Dampaknya membuka ruang interpretasi dan menyulitkan pembuktian pidana, terutama jika tidak ada data kuantitatif tentang kerugian subjek data.

b. Ketidakpastian pada Delik Pasal 66 dan 67

Pasal 66 mengatur tentang pengungkapan tanpa hak, dan Pasal 67 tentang pemrosesan secara ilegal, namun tidak dijelaskan secara normatif:

- 1) Bentuk pengungkapan apa yang dikriminalisasi?
- 2) Apakah melalui media sosial, forum online, atau hanya transfer data besar?
- 3) Apakah semua pemrosesan tanpa dasar hukum bisa dipidana, atau hanya yang berakibat merugikan?

Dampaknya, norma terlalu luas (*overbroad*), berpotensi melanggar asas *lex certa* (kejelasan hukum) dalam hukum pidana. Dalam kaitannya dengan hukum yang tertulis, pembuat undang-undang (*legislatif*) harus merumuskan secara jelas dan rinci mengenai perbuatan yang disebut dengan tindak pidana (*kejahatan, crimes*).

Hal inilah yang disebut dengan asas *lex certa*. Pembuat undang-undang harus mendefinisikan dengan jelas tanpa samar-samar (*nullum crimen sine lege stricta*), sehingga tidak ada perumusan yang ambigu mengenai perbuatan yang dilarang dan diberikan sanksi. Perumusan yang tidak jelas atau terlalu rumit hanya akan memunculkan ketidakpastian hukum dan menghalangi keberhasilan upaya penuntutan (*pidana*) karena warga selalu akan dapat membela diri bahwa ketentuan-ketentuan seperti itu tidak berguna sebagai pedoman perilaku.

Tidak bisanya kebiasaan menjadi dasar penghukuman bukan berarti kebiasaan tersebut tidak mempunyai peran dalam hukum pidana. Ia menjadi penting dalam menafsirkan *element of crimes* yang terkandung dalam tindak pidana yang dirumuskan oleh undang-undang tersebut. Namun demikian, dalam prakteknya tidak selamanya pembuat undang-undang dapat memenuhi persyaratan di atas. Tidak jarang perumusan undang-undang di terjemahkan lebih lanjut oleh kebiasaan yang berlaku di dalam masyarakat apabila norma tersebut secara faktual dipermasalahkan. (Rommelink, 2003)

c. Tidak Adanya Klasifikasi Delik Formil atau Materil Secara Tegas

Sebagian pasal seperti Pasal 66 dan 67 tidak mewajibkan adanya akibat (*kerugian*), namun tidak secara tegas disebut sebagai delik formil. (Ali, 2011) Dan juga pasal 65 dan 69 mencantumkan “merugikan subjek data”, tapi bentuk kerugian tidak dijelaskan, apakah harus materiel, imateriel, atau hanya potensial?

Dampaknya menimbulkan ketidakpastian dalam pembuktian unsur kerugian yang bisa membuat aparat penegak hukum enggan menindak karena tidak jelas ukuran kerugiannya.

d. Ketidaktegasaan Subjek Hukum Korporasi

Meskipun Pasal 70 membuka ruang untuk pidana tambahan terhadap badan hukum/korporasi, tidak dijelaskan secara tegas:

- Bagaimana mekanisme pembuktian pertanggungjawaban pidana korporasi?
- Apakah harus dibuktikan ada *mens rea* dari direksi?
- Apakah setiap pegawai yang membocorkan data mewakili korporasi?

Dampaknya membuat pertanggungjawaban pidana korporasi dalam kasus perdagangan data oleh perusahaan menjadi sulit diterapkan.

e. Tumpang Tindih dengan Peraturan Lain

Beberapa perbuatan pidana dalam Pasal 65–70 memiliki overlapping dengan ketentuan dalam:

- 1) UU ITE (Pasal 30 dan 32): Akses ilegal dan transmisi data
- 2) KUHP (Pasal 263 dan 378): Pemalsuan dan penipuan

Belum ada kejelasan norma prioritas atau *lex specialis* (Asas ini mengandung makna bahwa peraturan yang lebih khusus mengesampingkan peraturan yang lebih umum), (Manan, 2004) antara UU PDP dan peraturan lainnya. Dampaknya dapat terjadi konflik kewenangan dan perbedaan tafsir dalam proses penegakan hukum oleh kepolisian dan kejaksaan.

f. Ketiadaan Mekanisme Penegakan dan Lembaga Pelaksana

Sampai saat ini, belum terbentuk otoritas pengawas independen (Data Protection Authority) sebagai pelaksana pengawasan UU PDP. Menyebabkan tidak dijelaskan secara rinci siapa yang berwenang melakukan penyidikan, penyitaan data digital, atau penghentian sistem informasi. Dampaknya norma pidana dalam Pasal 65–70 menjadi kurang efektif dan tidak operasional, karena tidak didukung oleh lembaga penegak yang jelas.

Maka dari itu negara wajib memenuhi tugasnya untuk menyelesaikan masalah-masalah yang menyebabkan adanya ketidakpastian hukum tersebut. Mulai dari memberikan definisi kepentingan komersial, memberikan kejelasan bentuk sah dari persetujuan eksplisit baik dari segi fisik dan digitalnya. Mengatur mekanisme pencabutan persetujuan, jangka waktu persetujuan, batasan teknis penggunaan data pribadi dan aturan pelaksana dari peraturan pemerintah atau peraturan otoritas. Yang menjadi bukti bahwa perlindungan hukum tersebut memiliki kepastian hukum.

Selain adanya ketidakpastian dalam perlindungan hukum, beberapa pasal terkait aturan yang menjadi dasar penerapan dan penegakan hukum pidana juga memiliki masalah-masalah yang menyebabkan ketidakpastian hukum. Seperti ketidakjelasan unsur delik, tidak ada parameter batas kerugian subjek data, norma terlalu luas, ketidaktegasan subjek hukum koperasi, tumpang tindih dengan peraturan lain, dan terpenting belum adanya mekanisme penegakan dan lembaga pelaksana meskipun UU PDP telah mengamanatkan pembentukannya.

Karena merupakan tugas sebuah negara memberikan jaminan adanya kepastian terkait perlindungan dan penegakan hukum pidana, sehingga masyarakat dapat merasa aman terkait permasalahan perdagangan data pribadi.

5. KESIMPULAN DAN SARAN

Pertama, perlu dilakukan perluasan dan penegasan norma mengenai perdagangan data pribadi dalam UU PDP. Kedua, perlu dilakukan percepatan pembentukan Otoritas Pengawas Perlindungan Data Pribadi sebagaimana diamanatkan dalam Pasal 58 UU PDP. Ketiga, pemerintah perlu segera menyusun dan menerbitkan peraturan pelaksana berupa Peraturan Pemerintah (PP) atau peraturan otoritas terkait yang menjabarkan secara teknis penggunaan data pribadi untuk kepentingan komersial. Keempat, diperlukan penguatan mekanisme perlindungan hukum bagi subjek data pribadi sebagai pihak yang paling rentan dirugikan dalam praktik perdagangan data. Hal ini dapat dilakukan melalui penyediaan sistem pengaduan publik yang mudah diakses, pemberian hak atas ganti rugi melalui jalur hukum atau administratif, serta penguatan literasi masyarakat mengenai hak-hak atas data pribadi.

Pertama, perlu adanya penegasan secara eksplisit mengenai larangan perdagangan data pribadi dalam peraturan perundang-undangan. Kedua, diperlukan pengaturan teknis yang lebih rinci mengenai bentuk dan validitas persetujuan dalam pemrosesan data pribadi, terutama dalam konteks penggunaan untuk tujuan komersial. Ketiga, diperlukan harmonisasi regulasi antar peraturan perundang-undangan, khususnya antara UU PDP dengan peraturan sektoral lain seperti UU Informasi dan Transaksi Elektronik, UU Telekomunikasi. Keempat, penegakan hukum perlu diperkuat melalui peningkatan kapasitas aparat penegak hukum dan pembentukan unit khusus penanganan kejahatan siber yang berfokus pada eksploitasi data pribadi.

Daftar Referensi

- Ali, M. (2011). *Dasar-Dasar Hukum Pidana*. Jakarta: Sinar Grafika.
- Manan, B. (2004). *Hukum Positif Indonesia (Satu Kajian Teoritik)*. Cetakan Pertama. Yogyakarta: FH UII Press.
- Prastyanti, R. A. (2025). *Monograf Perlindungan Data Pribadi Konsumen Penggunaan Tranksaksi Elektronik*. Pekalongan: NEM.
- Priyatno, M. d. (2010). *Pertanggungjawaban Pidana Korporasi*. Jakarta: Kencana.
- Purwati, A. (2020). *Metode Penelitian Hukum Teori Dan Praktek*. Surabaya: Jakad Media Publishing.
- R, Y. M. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review*.

- Remmelink, J. (2003). *Hukum Pidana: Komentar Atas Pasal-Pasal Terpenting dari Kitab Undang Undang Hukum Pidana Belanda dan Padanannya dalam Kitab Undang-Undang Hukum Pidana Indonesia*. Jakarta: PT Gramedia.
- S, A. &. (2007). *Ilmu Perundang-Undangan* . Yogyakarta: PT. Kanisius.
- Soekanto, P. P. (1982). *Perihal Kaidah Hukum*. Bandung: Alumni.
- Subekti. (1984). *Hukum Perjanjian*. Jakarta: PT Intermedia.
- Suriaatmadja, R. d. (2023). Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Bandung Conference Series*
- Syahrani, R. (1999). *Rangkuman Intisari Ilmu Hukum*. Bandung: Citra Aditya.