

BAB II

TINJAUAN PUSTAKA TINDAK PIDANA PERLINDUNGAN DATA PRIBADI DALAM UNDANG-UNDANG NOMOR 27 TAHUN 2022

A. Teori-Teori Hukum

1. Teori Tindak Pidana (*Strafbaar Feit*)

Dalam khazanah ilmu hukum pidana, teori tindak pidana merupakan fondasi fundamental untuk menentukan apakah suatu perbuatan dapat dikualifikasikan sebagai perbuatan pidana yang dapat dijatuhi sanksi. Teori ini sangat relevan dalam menganalisis ketentuan Pasal 67 sampai dengan Pasal 75 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP), karena keseluruhan pasal pidana dalam undang-undang ini dirumuskan berdasarkan konsep *strafbaar feit*.

Menurut Simons, sebagaimana dikutip oleh Moeljatno, tindak pidana adalah "suatu perbuatan yang melawan hukum yang diancam dengan pidana oleh undang-undang, dilakukan oleh seseorang yang mampu bertanggung jawab, dan dapat dipersalahkan kepadanya." Definisi ini mengandung lima unsur esensial yang harus dipenuhi secara kumulatif, yaitu: (a) adanya perbuatan manusia, baik aktif maupun pasif; (b) perbuatan tersebut bersifat melawan hukum (*wederrechtelijk*); (c) diancam pidana oleh undang-undang (asas legalitas); (d) dilakukan oleh orang yang mampu bertanggung jawab; dan (e) adanya unsur kesalahan (*schuld*), baik berupa kesengajaan (*dolus*) maupun kealpaan (*culpa*). Kelima unsur ini bersifat kumulatif, artinya jika salah satu unsur tidak terpenuhi, maka suatu perbuatan tidak dapat dikualifikasikan sebagai tindak pidana.¹⁶⁾

¹⁶⁾ Simons, *Leerboek van het Nederlandsche Strafrecht* (cet. 1937), dikutip dalam Moeljatno, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2015, hlm. 56.

Dalam konteks UU PDP, kelima unsur ini menjadi pisau analisis untuk menguji apakah perbuatan-perbuatan yang dirumuskan dalam Pasal 67 sampai dengan Pasal 75 telah memenuhi syarat sebagai tindak pidana.

Moeljatno sendiri merumuskan tindak pidana secara lebih ringkas sebagai "perbuatan yang dilarang oleh suatu aturan hukum, larangan mana disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barang siapa yang melanggar larangan tersebut."¹⁷⁾ Perbedaan mendasar antara Simons dan Moeljatno terletak pada pemisahan antara unsur perbuatan dan unsur kesalahan. Simons memisahkan secara tegas antara *daad* (perbuatan) dan *schuld* (kesalahan), sedangkan Moeljatno menggabungkan keduanya dalam pengertian "perbuatan pidana". Dalam perkembangannya, doktrin Indonesia cenderung mengikuti pendapat Simons yang membedakan kedua unsur tersebut, karena pemisahan ini memberikan kejelasan dalam proses pembuktian di pengadilan. Hakim dapat terlebih dahulu membuktikan adanya perbuatan yang dilarang, baru kemudian menilai apakah pelaku memiliki kesalahan (kesengajaan atau kealpaan). Pemisahan ini sangat penting dalam praktik peradilan pidana karena mencegah terjadinya pemidanaan tanpa adanya kesalahan yang terbukti.

Selain itu, teori tindak pidana juga mengajarkan tentang pentingnya membedakan antara *wederrechtelijkheid* (sifat melawan hukum) dalam arti formil dan materil. Sifat melawan hukum formil berarti perbuatan tersebut melanggar ketentuan undang-undang yang tertulis, sedangkan sifat melawan hukum materil berarti perbuatan tersebut bertentangan dengan kesadaran hukum masyarakat atau nilai-nilai keadilan yang hidup dalam masyarakat.¹⁸⁾ Dalam UU PDP, setiap pasal pidana secara tegas mencantumkan frasa "melawan hukum" (*expressis verbis*), sehingga unsur melawan hukum bersifat formil dan tidak memerlukan penafsiran tambahan oleh hakim. Hal ini memberikan

¹⁷⁾ *Ibid*, hlm. 61.

¹⁸⁾ Andi Hamzah, *Asas-Asas Hukum Pidana*, Rineka Cipta, Jakarta, 2017, hlm. 89.

kepastian hukum bagi aparat penegak hukum dan masyarakat tentang perbuatan apa yang dilarang dan dapat dipidana.

Dalam konteks perlindungan data pribadi, teori tindak pidana memiliki relevansi yang sangat kuat. Unsur "perbuatan" dalam UU PDP dirumuskan secara spesifik, seperti "memproses data pribadi" Pasal 67, "mengungkapkan data pribadi" Pasal 70, atau "membuat data pribadi palsu" Pasal 71. Unsur "melawan hukum" dalam UU PDP bersifat *expressis verbis* sehingga memberikan kepastian hukum. Namun, yang menjadi sorotan kritis adalah unsur "kesalahan" dalam UU PDP hanya dirumuskan dalam bentuk kesengajaan (*dolus*), dengan menggunakan kata "dengan sengaja" di setiap pasal, dan tidak mengatur kealpaan (*culpa*). Hal ini berarti bahwa perbuatan yang dilakukan karena kelalaian (misalnya lalai mengenkripsi data, lalai melakukan *update* sistem keamanan, atau lalai dalam pengawasan karyawan) tidak dapat dipidana berdasarkan UU PDP. Implikasi dari ketiadaan delik *culpa* ini sangat signifikan, terutama dalam kasus kebocoran data massal seperti yang dialami Tokopedia, di mana lebih mungkin terjadi karena kelalaian sistemik daripada kesengajaan korporasi. Dengan demikian, teori tindak pidana tidak hanya berfungsi untuk menguji unsur-unsur delik, tetapi juga untuk mengidentifikasi kelemahan-kelemahan dalam pengaturan pidana yang perlu direvisi.

Implikasi dari ketiadaan delik *culpa* ini sangat penting untuk kasus kebocoran data seperti yang dialami Tokopedia. Jika kebocoran terjadi karena kelalaian internal (misalnya server tidak di-*patch*, karyawan lalai dalam menerapkan *enkripsi*), maka perbuatan tersebut tidak memenuhi unsur kesengajaan sehingga tidak dapat dipidana berdasarkan UU PDP.¹⁹⁾ Oleh karena itu, dalam BAB IV nanti akan dianalisis apakah perbuatan kebocoran data Tokopedia (seandainya dinilai dengan UU PDP) lebih tepat dikualifikasikan sebagai tindak pidana atau sebagai kelalaian perdata.

¹⁹⁾ Edmon Makarim, *Tanggung Jawab Penyelenggara Sistem Elektronik*, Rajawali Pers, Jakarta, 2019, hlm. 215.

Selain itu, teori tindak pidana juga mengajarkan tentang klasifikasi delik menjadi delik formil dan delik materil. Delik formil adalah delik yang dianggap selesai ketika perbuatan yang dilarang telah dilakukan, tanpa perlu menimbulkan akibat tertentu. Delik materil adalah delik yang baru terwujud jika akibat yang dilarang telah terjadi. Seluruh tindak pidana dalam UU PDP merupakan delik formil, karena rumusan pasal-pasal hanya mensyaratkan adanya perbuatan (memproses, mengungkapkan, membuat palsu) tanpa mensyaratkan timbulnya kerugian. Konsekuensinya, aparat penegak hukum tidak perlu membuktikan adanya kerugian materiil atau imateriil untuk mempidana pelaku.²⁰⁾

2. Teori Pertanggungjawaban Pidana Korporasi

Perkembangan hukum pidana modern telah mengakui korporasi sebagai subjek tindak pidana yang dapat dimintai pertanggungjawaban secara mandiri. Teori ini sangat relevan dalam menganalisis Pasal 56 dan Pasal 70 UU PDP, yang secara tegas mengatur bahwa korporasi dapat menjadi pelaku tindak pidana dan dapat dikenai pidana denda dengan pemberatan.

Muladi dan Dwidja Priyatno mengemukakan bahwa pertanggungjawaban pidana korporasi didasarkan pada asas bahwa korporasi adalah *rechts persoon* (persona hukum) yang memiliki kehendak dan kemampuan untuk bertindak di luar kehendak pengurusnya.²¹⁾ Korporasi tidak hanya sekadar kumpulan individu, melainkan memiliki kebijakan, struktur organisasi, dan budaya korporasi yang dapat menjadi sumber terjadinya tindak pidana. Oleh karena itu, memidana hanya pengurus tanpa menyentuh korporasi dianggap tidak adil dan tidak efektif.²²⁾

Pasal 56 UU PDP menyatakan bahwa "dalam hal tindak pidana dilakukan oleh korporasi, pidana dijatuhkan kepada korporasi dan/atau pengurusnya." Rumusan "dan/atau" ini menunjukkan bahwa UU PDP menganut model kumulatif, di mana baik

²⁰⁾ Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana*, Kencana, Jakarta, 2008, hlm. 56.

²¹⁾ Muladi dan Dwidja Priyatno, *Pertanggungjawaban Pidana Korporasi*, Kencana, Jakarta, 2012, hlm. 85

²²⁾ *Ibid.*, hlm. 90.

korporasi maupun pengurusnya dapat dipidana secara bersamaan atau salah satunya. Hal ini berbeda dengan beberapa undang-undang lain yang hanya memungkinkan salah satu (alternatif).²³⁾

Lebih lanjut dalam Pasal 79 UU PDP mengatur pemberatan pidana bagi korporasi, yaitu denda hingga 10 kali lipat dari ancaman maksimal (misalnya dari Rp6 miliar menjadi Rp60 miliar untuk Pasal 70), serta pidana tambahan berupa penghentian usaha, pembekuan usaha, perampasan aset, pencabutan izin, hingga pembubaran korporasi. Penulis menilai bahwa pidana tambahan seperti pencabutan izin atau pembubaran merupakan *ultimum remedium* yang hanya dijatuhkan untuk pelanggaran berat.

Ini menunjukkan bahwa korporasi memiliki tanggung jawab yang lebih besar dalam perlindungan data pribadi. Namun, penulis menyoroti bahwa pemberatan ini hanya berlaku untuk delik *dolus*, sehingga korporasi yang lalai tetap tidak dapat dipidana. Dalam kasus Tokopedia, penulis berpendapat bahwa PT Tokopedia hanya dapat dipidana jika terbukti ada unsur kesengajaan, misalnya jika direksi sengaja memerintahkan penjualan data. Jika kebocoran terjadi karena kelalaian sistemik, maka UU PDP tidak dapat menjerat korporasi.

Pemberatan denda hingga 10 kali lipat dari ancaman maksimal (misalnya dari Rp6 miliar menjadi Rp60 miliar untuk Pasal 70) menunjukkan bahwa pembentuk undang-undang menganggap korporasi memiliki tanggung jawab yang lebih besar dalam perlindungan data pribadi. Pidana tambahan berupa pencabutan izin usaha atau pembubaran korporasi merupakan *ultimum remedium* yang hanya dijatuhkan untuk pelanggaran berat.²⁴⁾

Dalam konteks kasus Tokopedia, teori pertanggungjawaban pidana korporasi akan digunakan untuk menilai, apakah PT Tokopedia sebagai korporasi dapat dipidana berdasarkan UU PDP jika kebocoran data terjadi karena kebijakan korporasi yang lalai (misalnya tidak mengalokasikan anggaran yang memadai untuk keamanan siber)?

²³⁾ Muladi & Priyatno, *op. cit.*, hlm. 95.

²⁴⁾ *Ibid.*

Ataukah hanya pengurus (direksi) yang bertanggung jawab secara personal? Jawaban atas pertanyaan ini sangat bergantung pada model pertanggungjawaban yang dianut dan tingkat kesengajaan yang dapat dibuktikan.)

3. Teori Pidana (Tujuan Pidana)

Teori pidana membahas alasan mengapa pidana dijatuhkan dan tujuan apa yang hendak dicapai dari penjatuhan pidana tersebut. Teori ini sangat relevan untuk mengevaluasi apakah sistem pidana dalam UU PDP (ancaman pidana penjara, denda, pemberatan untuk korporasi, delik aduan) sudah efektif dalam mencapai tujuannya.²⁵⁾

Secara garis besar, teori pidana terbagi menjadi tiga aliran utama:

a. Teori Absolut (Teori Pembalasan / *Vergeldingstheorie*)

Teori ini berpendapat bahwa pidana dijatuhkan semata-mata karena seseorang telah melakukan kejahatan. Pidana adalah pembalasan yang setimpal atas perbuatan pelaku, tanpa mempertimbangkan manfaat bagi masyarakat atau pelaku. Immanuel Kant, salah satu tokoh utama teori ini, menyatakan bahwa pidana adalah "*imperatif kategoris*" yang harus dijatuhkan karena kejahatan itu sendiri, bukan untuk tujuan lain seperti pencegahan atau rehabilitasi.²⁶⁾ Hasil analisis penulis menyatakan bahwa kelemahan teori ini adalah tidak memberikan ruang bagi perbaikan pelaku (rehabilitasi) dan tidak mempertimbangkan dampak sosial dari pidana. Dalam konteks Undang-Undang Perlindungan Data Pribadi, teori absolut hanya sedikit berpengaruh, terlihat dari ancaman pidana yang lebih berat untuk pengungkapan data (Pasal 70) yang mencerminkan pembalasan atas pelanggaran privasi yang serius.

b. Teori Relatif (Teori Tujuan / *Doelstheorie*)

Teori ini berpendapat bahwa pidana bukanlah pembalasan, melainkan sarana untuk mencapai tujuan yang bermanfaat bagi masyarakat. Jeremy Bentham, tokoh

²⁵⁾ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Kencana, Jakarta, 2017, hlm. 23-25.

²⁶⁾ Immanuel Kant, *The Philosophy of Law*, terjemahan W. Hastie, T&T Clark, Edinburgh, 1887, hlm. 195.

utilitarianisme, mengemukakan bahwa setiap tindakan termasuk pidana harus diukur berdasarkan manfaat yang dihasilkan bagi masyarakat secara keseluruhan (*the greatest happiness of the greatest number*).²⁷⁾ Feuerbach mengembangkan teori pencegahan umum (*Generalprävention*), yang menyatakan bahwa pidana bertujuan untuk menakut-nakuti masyarakat umum agar tidak melakukan kejahatan. Sementara itu, teori pencegahan khusus (*Spezialprävention*) lebih menitikberatkan pada pembinaan dan efek jera terhadap pelaku secara individual agar tidak mengulangi kejahatannya di masa depan.

Dalam konteks Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), penerapan teori relatif ini terasa sangat dominan yang dapat dibuktikan melalui beberapa indikasi nyata. Pertama, UU PDP menyediakan mekanisme sanksi administratif pada Pasal 57 sebagai instrumen utama sebelum menjatuhkan sanksi pidana (*ultimum remedium*). Hal ini menunjukkan bahwa tujuan utama hukum bukan semata-mata untuk memenjarakan pelaku, melainkan untuk memastikan kepatuhan standar pelindungan data melalui jalur yang terukur sebagai bentuk prevensi khusus. Kedua, rentang ancaman pidana penjara yang bertingkat berkisar antara 4 hingga 6 tahun serta denda maksimal miliaran rupiah memberikan ruang diskresi bagi hakim untuk menyesuaikan sanksi dengan tingkat kerugian yang ditimbulkan. Fleksibilitas pemidanaan ini mencerminkan perpaduan antara tujuan prevensi khusus untuk menjerakan pelaku dan prevensi umum yang berfungsi sebagai peringatan keras bagi publik.

Selanjutnya, keberlakuan teori relatif semakin dipertegas melalui fokus undang-undang ini pada pertanggungjawaban korporasi. Penerapan denda maksimal hingga 10 (sepuluh) kali lipat bagi korporasi, ditambah dengan ancaman pidana tambahan berupa pembekuan hingga pencabutan izin usaha sebagaimana diatur dalam Pasal 70, merupakan manifestasi nyata dari *doelstheorie*. Pidana denda yang sangat besar ini

²⁷⁾ Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation*, T. Payne, London, 1789, hlm. 170-172.

tidak hanya bertujuan melumpuhkan kemampuan finansial korporasi yang melanggar agar tidak mengulangi perbuatannya, tetapi juga menjadi instrumen *Generalprävention* yang sangat efektif untuk memaksa entitas perusahaan lain agar segera memperkuat sistem keamanan siber mereka. Di samping itu, orientasi pada kemanfaatan (*utilitarianisme*) juga terlihat jelas pada pengaturan pemulihan kerugian korban di Pasal 69. Melalui ketentuan perampasan keuntungan dan kewajiban pembayaran ganti kerugian, negara secara aktif berusaha memulihkan hak-hak subjek data pribadi yang telah dilanggar, alih-alih hanya berfokus pada penghukuman pelaku kejahatannya semata.

c. Teori Integratif (Teori Gabungan)

Teori ini mencoba menggabungkan unsur pembalasan dan unsur tujuan. Van Hammel, salah satu tokoh aliran modern, mengemukakan bahwa pidana harus memenuhi tuntutan keadilan retributif sekaligus berfungsi sebagai sarana untuk memperbaiki pelaku dan melindungi masyarakat. Sistem pemasyarakatan Indonesia pada dasarnya menganut teori gabungan, di mana pidana penjara tetap mengandung unsur pembalasan (menjalani sebagian masa pidana) sekaligus unsur pembinaan (program rehabilitasi).²⁸⁾

Dalam Undang-Undang Perlindungan Data Pribadi, Hasil analisis penulis, unsur teori integratif terlihat dari ancaman pidana yang tetap ada (pembalasan) namun dengan mekanisme delik aduan yang memungkinkan perdamaian (tujuan sosial). Selain itu, pemberatan pidana untuk korporasi hingga 10 kali lipat mencerminkan pembalasan yang lebih berat, tetapi juga bertujuan untuk memberikan efek jera yang kuat bagi entitas bisnis (*prevensi*).

Berdasarkan teori pembedaan di atas, penelitian ini akan mengevaluasi apakah ancaman pidana dalam UU PDP (maksimal 6 tahun penjara dan denda Rp6 miliar untuk perorangan, serta pemberatan 10 kali untuk korporasi) sudah memenuhi tujuan

²⁸⁾ Muladi, *Kapita Selekta Sistem Peradilan Pidana*, UNDIP Press, Semarang, 1995, hlm. 45.

pencegahan kejahatan. Selain itu, akan dikritisi kelemahan seperti ketiadaan delik *culpa* yang membuat kelalaian korporasi tidak dapat dipidana, serta pemberlakuan delik aduan yang berpotensi menghambat penegakan hukum karena korban harus melapor secara individual.²⁹⁾

4. Teori Perlindungan Hukum

Teori perlindungan hukum memiliki relevansi yang kuat dalam penelitian ini karena hak atas perlindungan data pribadi merupakan hak asasi yang harus dijamin oleh negara, termasuk melalui instrumen hukum pidana. Menurut Philipus M. Hadjon, perlindungan hukum bagi rakyat dibedakan menjadi dua macam, yaitu perlindungan hukum preventif dan perlindungan hukum represif.³⁰⁾

Perlindungan hukum preventif bertujuan untuk mencegah terjadinya sengketa atau pelanggaran hak sebelum insiden terjadi. Dalam konteks perlindungan data pribadi, perlindungan preventif diwujudkan melalui kewajiban-kewajiban yang dibebankan kepada pengendali data dalam UU PDP, seperti kewajiban memperoleh persetujuan Pasal 22, kewajiban memberitahukan tujuan pemrosesan Pasal 23, kewajiban menjamin keakuratan data (Pasal 24), serta kewajiban menerapkan sistem pengamanan yang andal Pasal 38. Dengan adanya kewajiban-kewajiban ini, diharapkan pelanggaran data pribadi dapat dicegah sejak awal. Aspek pidana dalam perlindungan preventif tercermin dari ancaman pidana bagi yang melanggar kewajiban tersebut Pasal 67-75, yang berfungsi sebagai *deterrent* (pencegah) bagi calon pelaku.

Perlindungan hukum represif diberikan setelah terjadinya pelanggaran hak, bertujuan untuk memulihkan hak yang dilanggar dan memberikan sanksi kepada pelaku. Dalam UU PDP, perlindungan represif diwujudkan melalui mekanisme gugatan ganti rugi perdata Pasal 12 huruf h, sanksi administratif Pasal 57-66, dan sanksi pidana Pasal 67 - 72. Dari ketiga mekanisme tersebut, sanksi pidana merupakan bentuk

²⁹⁾ *Ibid.*

³⁰⁾ Philipus M. Hadjon, *Perlindungan Hukum bagi Rakyat di Indonesia*, Bina Ilmu, Surabaya, 1987, hlm. 2-4.

perlindungan represif yang paling tegas karena melibatkan ancaman perampasan kemerdekaan penjara dan denda besar.

Satjipto Rahardjo mendefinisikan perlindungan hukum sebagai "memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan itu diberikan kepada masyarakat agar dapat menikmati semua hak-hak yang diberikan oleh hukum."³¹⁾ Dalam perspektif ini, negara berkewajiban memastikan bahwa hak atas perlindungan data pribadi, yang merupakan bagian dari hak privasi Pasal 28G UUD 1945, benar-benar dapat dinikmati oleh setiap warga negara. Kegagalan negara dalam menindak pelaku kebocoran data secara pidana merupakan bentuk kegagalan perlindungan hukum represif.

Teori perlindungan hukum digunakan dalam penelitian ini untuk menilai apakah sistem pidana dalam UU PDP sudah memberikan perlindungan yang memadai bagi korban kebocoran data. Secara khusus, akan dianalisis apakah delik aduan Pasal 72 tidak justru menghambat perlindungan represif karena korban harus melapor secara individual. Selain itu, akan dikaji apakah ketiadaan delik *culpa* menyebabkan korban kehilangan perlindungan pidana ketika kebocoran terjadi karena kelalaian korporasi.

B. Tinjauan Umum tentang Perlindungan Data Pribadi di Indonesia

1. Pengertian Data Pribadi

Pasal 1 angka 1 UU PDP mendefinisikan data pribadi sebagai "data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik." Definisi ini selaras dengan Pasal 4 angka 1 General Data Protection Regulation (GDPR) yang menggunakan pendekatan *identifiable natural person*, yaitu seseorang yang dapat diidentifikasi, baik secara langsung (misalnya melalui nama) maupun tidak langsung (misalnya melalui kombinasi alamat, nomor telepon, dan tanggal lahir).

³¹⁾ Satjipto Rahardjo, *Ilmu Hukum*, Citra Aditya Bakti, Bandung, 2000, hlm. 53.

Sinta Dewi Rosadi menjelaskan bahwa data pribadi bukan sekadar informasi administratif, melainkan representasi digital dari identitas dan martabat seseorang. Kebocoran data pribadi tidak hanya merugikan secara materiil, tetapi juga melukai hak privasi yang melekat sebagai hak asasi manusia.³²⁾

2. Klasifikasi Data Pribadi

Pasal 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengklasifikasikan data pribadi ke dalam dua jenis, yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Data pribadi yang bersifat spesifik merupakan data yang memiliki tingkat sensitivitas lebih tinggi karena berkaitan langsung dengan kondisi pribadi, identitas khusus, atau keadaan tertentu dari subjek data. Jenis data ini meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, serta data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Contoh data pribadi yang bersifat spesifik antara lain sidik jari, rekam medis, golongan darah, data genetik, catatan pidana, data anak, dan nomor rekening pribadi.

Adapun data pribadi yang bersifat umum merupakan data yang lazim digunakan untuk mengenali atau mengidentifikasi seseorang dalam kehidupan sehari-hari. Data ini mencakup nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang. Dalam praktiknya, data seperti alamat, alamat email, nomor telepon, tanggal lahir, serta jenis kelamin juga sering digunakan sebagai identitas seseorang dalam sistem elektronik. Meskipun dikategorikan sebagai data pribadi umum, data tersebut tetap harus dilindungi karena apabila bocor atau disalahgunakan dapat menimbulkan kerugian bagi subjek data, seperti pencurian identitas, penipuan, penyalahgunaan akun, atau tindakan lain yang merugikan.

³²⁾ Sinta Dewi Rosadi, *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital*, Refika Aditama, Bandung, 2018, hlm. 89.

Perbedaan antara data pribadi spesifik dan data pribadi umum menunjukkan bahwa UU PDP memberikan tingkat perlindungan yang berbeda sesuai dengan sifat dan risiko dari data tersebut. Data pribadi yang bersifat spesifik memerlukan perlindungan yang lebih ketat karena penyalahgunaannya dapat menimbulkan dampak yang lebih serius terhadap hak, martabat, dan keamanan subjek data. Oleh karena itu, setiap proses pengumpulan, penggunaan, penyimpanan, pengungkapan, atau pemindahan data pribadi harus dilakukan berdasarkan prinsip kehati-hatian, persetujuan yang sah, serta sesuai dengan ketentuan hukum yang berlaku.

Dalam kasus kebocoran data Tokopedia, data yang bocor meliputi nama, alamat email, nomor telepon, tanggal lahir, dan jenis kelamin yang tergolong data pribadi bersifat umum. Meskipun demikian, kebocoran data umum tetap memiliki implikasi serius karena dapat digunakan untuk *phishing*, penipuan identitas, dan serangan siber lainnya.³³⁾

3. Asas-Asas Perlindungan Data Pribadi

Pasal 3 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengatur bahwa penyelenggaraan perlindungan data pribadi didasarkan pada beberapa asas, yaitu asas pelindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan. Asas-asas tersebut menjadi pedoman utama dalam setiap kegiatan pemrosesan data pribadi agar hak subjek data tetap terlindungi dan tidak disalahgunakan oleh pihak yang tidak berwenang.

Asas pelindungan menegaskan bahwa setiap pemrosesan data pribadi harus dilakukan dengan memberikan perlindungan kepada subjek data atas data pribadinya. Perlindungan ini diperlukan agar data pribadi tidak digunakan secara melawan hukum, tidak disebarluaskan tanpa dasar yang sah, dan tidak dimanfaatkan untuk kepentingan yang merugikan pemilik data. Asas kepastian hukum menghendaki agar setiap pemrosesan data pribadi dilakukan berdasarkan landasan hukum yang jelas, sehingga

³³⁾ Laporan BSSN tentang Insiden Tokopedia, BSSN, Jakarta, 2020, hlm. 5.

hak dan kewajiban antara subjek data, pengendali data, prosesor data, serta pihak lain yang terlibat dapat ditentukan secara tegas.

Selanjutnya, asas kepentingan umum menunjukkan bahwa perlindungan data pribadi tetap harus memperhatikan kepentingan masyarakat secara luas, termasuk kepentingan penyelenggaraan negara, pelayanan publik, penegakan hukum, serta pertahanan dan keamanan nasional. Namun, penerapan asas ini tidak boleh dilakukan secara sewenang-wenang, melainkan harus tetap memperhatikan hak-hak subjek data pribadi. Asas kemanfaatan berarti bahwa pengaturan dan pemrosesan data pribadi harus memberikan manfaat bagi kepentingan nasional, masyarakat, serta subjek data pribadi itu sendiri.

Asas kehati-hatian mewajibkan setiap pihak yang terlibat dalam pemrosesan dan pengawasan data pribadi untuk memperhatikan seluruh aspek yang berpotensi menimbulkan kerugian. Asas ini sangat penting dalam konteks kebocoran data pribadi, karena kelalaian dalam menjaga keamanan sistem, lemahnya pengawasan internal, atau tidak adanya standar keamanan yang memadai dapat menyebabkan data pribadi disalahgunakan. Oleh karena itu, pengendali data pribadi wajib bertindak cermat dan bertanggung jawab dalam setiap tahap pemrosesan data.

Selain itu, asas keseimbangan menekankan perlunya keseimbangan antara hak subjek data pribadi dengan kepentingan negara yang sah berdasarkan kepentingan umum. Asas pertanggungjawaban mengharuskan setiap pihak yang melakukan pemrosesan dan pengawasan data pribadi untuk dapat mempertanggungjawabkan tindakannya sesuai dengan ketentuan hukum yang berlaku. Terakhir, asas kerahasiaan menegaskan bahwa data pribadi harus dilindungi dari pihak yang tidak berhak dan dari setiap bentuk pemrosesan yang tidak sah. Dengan demikian, asas-asas dalam UU PDP berfungsi sebagai dasar normatif untuk memastikan bahwa perlindungan data pribadi dilaksanakan secara aman, adil, bertanggung jawab, dan sesuai dengan hukum.

4. Hak-Hak Subjek Data Pribadi

Undang-Undang Perlindungan Data Pribadi memberikan 9 (sembilan) hak kepada subjek data pribadi yang diatur dalam Pasal 12 sampai dengan Pasal 16. Hak-hak tersebut meliputi:

- a. Hak untuk mendapatkan informasi (Pasal 12 huruf a)
- b. Hak untuk mengakses data (Pasal 12 huruf b)
- c. Hak untuk melengkapi, memperbarui, dan memperbaiki data (Pasal 12 huruf c)
- d. Hak untuk menghapus dan/atau memusnahkan data (*right to be forgotten*) (Pasal 12 huruf d)
- e. Hak untuk mengakhiri pemrosesan (Pasal 12 huruf e)
- f. Hak untuk membatasi pemrosesan (Pasal 12 huruf f)
- g. Hak untuk mengajukan keberatan (Pasal 12 huruf g)
- h. Hak untuk menuntut dan menerima ganti rugi (Pasal 12 huruf h)
- i. Hak untuk mendapatkan mekanisme penyelesaian sengketa (Pasal 12 huruf i)

Dari kesembilan hak tersebut, hak untuk menuntut ganti rugi (Pasal 12 huruf h) memiliki keterkaitan erat dengan hukum pidana, karena korban tindak pidana dapat mengajukan tuntutan restitusi (ganti rugi) dalam proses pidana, tanpa harus mengajukan gugatan perdata terpisah.³⁴⁾ Selain itu, hak untuk mengakhiri pemrosesan dan hak untuk menghapus data (*right to be forgotten*) juga relevan karena pelanggaran terhadap hak-hak ini dapat dikenai sanksi pidana (Pasal 74 tentang menghalangi akses subjek data).

C. Tinjauan tentang Tindak Pidana dalam UU PDP

1. Pengaturan Tindak Pidana dalam UU PDP

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi secara khusus mengatur larangan dan ancaman pidana dalam Bab XIV tentang Ketentuan Pidana. Pengaturan tersebut menunjukkan bahwa pelindungan data pribadi tidak hanya

³⁴⁾ Pasal 7C ayat (2) Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban.

ditempatkan sebagai persoalan administratif atau perdata, tetapi juga sebagai bagian dari hukum pidana apabila terdapat perbuatan yang dilakukan secara sengaja dan melawan hukum.

Pasal 67 ayat (1) UU PDP mengatur bahwa 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 bagi subjek data pribadi, dapat dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Ketentuan ini menunjukkan bahwa perbuatan memperoleh atau mengumpulkan data pribadi tanpa hak merupakan tindakan yang dilarang apabila dilakukan dengan tujuan memperoleh keuntungan dan berpotensi merugikan subjek data pribadi.

Selanjutnya, Pasal 67 ayat (2) UU PDP mengatur larangan terhadap perbuatan mengungkapkan data pribadi yang bukan miliknya secara sengaja dan melawan hukum. Terhadap perbuatan tersebut, pelaku dapat dikenai pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah). Ketentuan ini penting karena pengungkapan data pribadi tanpa dasar hukum yang sah dapat membuka peluang penyalahgunaan data, seperti penipuan, pencurian identitas, maupun kejahatan siber lainnya.

Pasal 67 ayat (3) UU PDP juga mengatur bahwa setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya dapat dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Perbuatan menggunakan data pribadi tanpa hak memiliki tingkat bahaya yang serius karena data pribadi dapat dimanfaatkan untuk memperoleh keuntungan, merugikan pemilik data, atau melakukan tindakan lain yang bertentangan dengan hukum.

Selain itu, Pasal 68 UU PDP mengatur mengenai perbuatan membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian bagi orang lain. Terhadap

perbuatan tersebut, pelaku dapat dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp6.000.000.000,00 (enam miliar rupiah). Ancaman pidana dalam pasal ini lebih berat karena pemalsuan data pribadi tidak hanya melanggar hak subjek data, tetapi juga dapat menimbulkan akibat hukum yang luas, termasuk kerugian bagi pihak lain yang menggunakan atau mempercayai data palsu tersebut.

Dengan demikian, Pasal 67 dan Pasal 68 UU PDP menunjukkan bahwa tindak pidana perlindungan data pribadi berfokus pada beberapa bentuk perbuatan utama, yaitu memperoleh atau mengumpulkan data pribadi secara melawan hukum, mengungkapkan data pribadi tanpa hak, menggunakan data pribadi tanpa hak, serta membuat atau memalsukan data pribadi. Seluruh perbuatan tersebut mensyaratkan adanya unsur kesengajaan dan sifat melawan hukum. Oleh karena itu, dalam perspektif hukum pidana, pembuktian terhadap unsur “dengan sengaja” dan “melawan hukum” menjadi bagian penting untuk menentukan dapat atau tidaknya seseorang dimintai pertanggungjawaban pidana berdasarkan UU PDP.

Selain tindak pidana pokok di atas, UU PDP juga mengatur sanksi pidana tambahan berupa perampasan perolehan atau harta kekayaan Pasal 69 serta mengatur mekanisme pertanggungjawaban pidana bagi korporasi yang dapat dijatuhi pidana denda hingga 10 (sepuluh) kali lipat dari maksimal pidana denda yang diancamkan (Pasal 70).

2. Unsur-Unsur Tindak Pidana

Semua tindak pidana dalam UU PDP Pasal 67 sampai dengan Pasal 75 memiliki kesamaan unsur, yaitu dilakukan dengan sengaja dan melawan hukum. Penggunaan frasa "dengan sengaja" secara tegas menunjukkan bahwa tindak pidana ini diklasifikasikan sebagai delik *dolus* (kesengajaan), bukan delik *culpa* (kealpaan). Penulis menilai bahwa pilihan untuk hanya mengatur delik *dolus* ini merupakan keputusan hukum yang memiliki implikasi sangat signifikan terhadap efektivitas penegakan hukum pidana di bidang perlindungan data pribadi. Dengan hanya mengakomodasi unsur kesengajaan, UU PDP secara otomatis menutup pintu bagi

penuntutan pidana terhadap perbuatan yang dilakukan karena kelalaian, meskipun kelalaian tersebut mengakibatkan kerugian yang sangat besar bagi masyarakat.

Dalam doktrin hukum pidana, kesengajaan (*dolus*) dibedakan menjadi tiga bentuk berdasarkan tingkat intensitas kehendak pelaku. Bentuk pertama adalah sengaja sebagai maksud (*oogmerk*), di mana pelaku benar-benar menghendaki tercapainya suatu tujuan tertentu. Bentuk kedua adalah sengaja dengan kesadaran kepastian (*opzet als zekerheidsbewustzijn*), di mana pelaku sadar bahwa akibat dari perbuatannya pasti akan terjadi. Bentuk ketiga adalah sengaja dengan kesadaran kemungkinan (*dolus eventualis*), di mana pelaku sadar bahwa akibat mungkin terjadi dan menerima risiko tersebut.

Dalam konteks kebocoran data, pembuktian unsur "sengaja" menjadi tantangan tersendiri dalam praktik peradilan pidana. Jika kebocoran data terjadi karena peretasan oleh pihak eksternal (seperti yang dialami Tokopedia), maka hampir mustahil untuk membuktikan bahwa pengendali data memiliki unsur kesengajaan untuk membocorkan data. Yang lebih mungkin terjadi dan dapat dibuktikan adalah adanya kelalaian (*culpa*) dalam bentuk kegagalan menerapkan standar keamanan yang memadai, kelalaian dalam melakukan *update* sistem, atau kurangnya pengawasan terhadap akses data oleh pihak internal. Namun, sayangnya kelalaian dalam bentuk apa pun tidak diatur sebagai tindak pidana dalam UU PDP.

Delik *culpa* ini merupakan kelemahan fatal yang membuat UU PDP kehilangan daya jangkau terhadap sebagian besar kasus kebocoran data yang terjadi di lapangan.

3. Klasifikasi Delik

Berdasarkan karakteristiknya, tindak pidana dalam Undang-Undang Perlindungan Data Pribadi dapat diklasifikasikan sebagai berikut:

a. Delik Formil

Seluruh tindak pidana dalam Undang-Undang Perlindungan Data Pribadi merupakan delik formil, karena rumusan pasal-pasal nya hanya mensyaratkan adanya perbuatan (memproses, mengungkapkan, membuat palsu) tanpa mensyaratkan timbulnya kerugian tertentu. Konsekuensinya, aparat penegak hukum tidak perlu

membuktikan adanya kerugian materiil atau imateriil untuk mempidana pelaku. Hal ini memudahkan proses pembuktian dan memperkuat fungsi preventif hukum pidana.³⁵⁾

b. Delik Aduan Pasal 72

Pasal 72 Undang-Undang Perlindungan Data Pribadi menyatakan bahwa semua tindak pidana dalam UU PDP merupakan delik aduan. Artinya, proses pidana hanya dapat dimulai jika ada pengaduan dari subjek data pribadi yang dirugikan atau dari kuasanya. Delik aduan ini bersifat absolut, tidak dapat diproses tanpa pengaduan, dan tidak dapat dicabut setelah pengaduan diajukan, kecuali dalam hal perdamaian di luar proses pidana.³⁶⁾

Klasifikasi sebagai delik aduan memiliki implikasi signifikan. Di satu sisi, hal ini memberikan kontrol kepada subjek data untuk menentukan apakah suatu perkara akan diproses secara pidana atau tidak. Di sisi lain, hal ini dapat menjadi penghambat penegakan hukum jika korban tidak melapor karena kurangnya kesadaran hukum, trauma, atau takut akan proses yang panjang. Dalam kasus kebocoran data Tokopedia dengan 91 juta korban, mustahil untuk memproses setiap laporan secara individual. Tidak ada mekanisme pengaduan kolektif dalam UU PDP.³⁷⁾

c. Delik Dolus

Semua tindak pidana dalam Undang-Undang Perlindungan Data Pribadi dirumuskan dengan kata "dengan sengaja", sehingga merupakan delik dolus. Ketiadaan delik *culpa* berarti bahwa kelalaian (misalnya kelalaian dalam menjaga sistem keamanan data) tidak dapat dipidana berdasarkan Undang-Undang Perlindungan Data Pribadi. Ini merupakan kelemahan signifikan, karena dalam praktiknya kebocoran data lebih sering terjadi karena kelalaian (human error, sistem tidak di-*update*) daripada kesengajaan.³⁸⁾

³⁵⁾ Barda Nawawi Arief, *Masalah Penegakan Hukum*, Op. Cit. (Note 5), hlm. 56.

³⁶⁾ Andi Hamzah, Op. Cit. hlm. 201.

³⁷⁾ Sinta Dewi Rosadi, Op. Cit. hlm. 222.

³⁸⁾ Edmon Makarim, Op. Cit. hlm. 220.

D. Tinjauan tentang Pertanggungjawaban Pidana Korporasi Pasal 56 dan 79

1. Pengaturan Korporasi sebagai Subjek Tindak Pidana

Pasal 56 UU PDP menyatakan: "Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 sampai dengan Pasal 75 dilakukan oleh korporasi, pidana dijatuhkan kepada korporasi dan/atau pengurusnya." Pasal ini menegaskan bahwa korporasi dapat menjadi subjek tindak pidana. Definisi korporasi dalam Pasal 1 angka 6 UU PDP adalah "kumpulan orang dan/atau kekayaan yang terorganisasi, baik merupakan badan hukum maupun bukan badan hukum."

Pengakuan korporasi sebagai subjek tindak pidana sejalan dengan perkembangan hukum pidana modern. Muladi menyatakan bahwa korporasi dapat dipertanggungjawabkan secara pidana karena memiliki kebijakan, struktur, dan budaya yang dapat menjadi sumber kejahatan. Dalam konteks kebocoran data, korporasi seperti PT Tokopedia dapat dipidana jika kebijakan atau kelalaian sistemiknya menyebabkan kebocoran.

2. Pidana untuk Korporasi (Pasal 70)

Pasal 70 UU PDP mengatur pidana yang dapat dijatuhkan kepada korporasi. Sebagai ilustrasi, jika suatu korporasi melanggar Pasal 70 (ancaman denda Rp6 miliar untuk perorangan), maka korporasi dapat didenda hingga Rp60 miliar. Pidana tambahan berupa pencabutan izin usaha atau pembubaran korporasi merupakan *ultimum remedium* yang hanya dijatuhkan untuk pelanggaran berat.

3. Model Pertanggungjawaban yang Dianut

Berdasarkan rumusan Pasal 56 yang menyatakan "pidana dijatuhkan kepada korporasi dan/atau pengurusnya" serta Pasal 70 yang mengatur pemberatan denda untuk korporasi, UU PDP menganut model gabungan antara *vicarious liability* dan *corporate criminal liability*. Model *vicarious liability* tercermin dari kemungkinan korporasi bertanggung jawab atas perbuatan pengurus atau karyawannya yang dilakukan dalam lingkup pekerjaan, terlepas dari apakah korporasi mengetahui atau tidak mengetahui perbuatan tersebut. Sementara itu, model *corporate criminal liability* tercermin dari kemungkinan korporasi bertanggung jawab secara mandiri

sebagai entitas yang memiliki kebijakan, struktur organisasi, dan budaya korporasi sendiri yang dapat menjadi sumber terjadinya tindak pidana. Rumusan "dan/atau" dalam Pasal 56 menunjukkan sifat kumulatif, yang berarti baik korporasi maupun pengurus dapat dipidana secara bersamaan atau salah satunya, tergantung pada tingkat kesalahan dan keterlibatan masing-masing.

Model gabungan ini memberikan fleksibilitas bagi aparat penegak hukum dalam menjerat pelaku tindak pidana perlindungan data pribadi. Apabila terbukti bahwa kebocoran data disebabkan oleh kebijakan korporasi yang lalai, seperti tidak mengalokasikan anggaran yang memadai untuk keamanan siber atau tidak menerapkan standar enkripsi yang sesuai, maka korporasi dapat dipidana berdasarkan pertanggungjawaban langsung sebagai entitas. Apabila terbukti bahwa pengurus secara personal melakukan kesengajaan, misalnya memerintahkan penjualan data pribadi kepada pihak ketiga tanpa persetujuan subjek data, maka pengurus dapat dipidana secara personal. Apabila kedua unsur tersebut terbukti, yaitu baik kebijakan korporasi yang lalai maupun kesengajaan pengurus, maka keduanya dapat dipidana secara bersamaan. Fleksibilitas ini sejalan dengan perkembangan hukum pidana modern yang mengakui korporasi sebagai subjek hukum yang dapat melakukan tindak pidana dan dapat dipertanggungjawabkan secara mandiri, terlepas dari pertanggungjawaban individu pengurusnya.

E. Tinjauan tentang Sistem Pidana dalam UU PDP

1. Pengaturan Ancaman Pidana Penjara dan Denda

Sebagaimana telah diuraikan dalam tabel pada sub-bab C, ancaman pidana penjara berkisar antara 2 tahun Pasal 72 hingga 6 tahun (Pasal 70 dan 71), sedangkan ancaman denda berkisar antara Rp2 miliar hingga Rp6 miliar untuk perorangan, dan hingga Rp60 miliar untuk korporasi (dengan pemberatan 10 kali).

Perbandingan dengan regulasi lain menunjukkan bahwa ancaman pidana dalam UU PDP relatif berat. Sebagai perbandingan, Pasal 46 UU ITE mengancam akses ilegal dengan pidana penjara 6 tahun dan denda Rp600 juta denda dalam UU PDP 10 kali

lebih besar. Hal ini menunjukkan keseriusan pembentuk undang-undang dalam melindungi data pribadi.

2. Perbandingan dengan GDPR

Meskipun GDPR tidak mengatur sanksi pidana secara langsung (diserahkan kepada negara anggota), sistem denda administratif dalam GDPR menjadi tolok ukur internasional. Pasal 83 GDPR mengatur denda maksimal €20 juta atau 4% dari pendapatan global tahunan (mana yang lebih tinggi). Jika dibandingkan, denda maksimal dalam UU PDP untuk korporasi (Rp60 miliar atau sekitar €3,5 juta) jauh lebih rendah dari GDPR. Beberapa kritik menyatakan bahwa angka ini tidak cukup memberikan efek jera bagi perusahaan multinasional yang beroperasi di Indonesia.

3. Kritik terhadap Sistem Pemidanaan UU PDP

Berdasarkan teori pemidanaan dan teori perlindungan hukum, beberapa kelemahan UU PDP dapat diidentifikasi:

Pertama, ketiadaan delik *culpa* (kealpaan). Sebagaimana dijelaskan, semua tindak pidana dalam UU PDP mensyaratkan unsur kesengajaan. Padahal, dalam praktiknya kebocoran data lebih sering terjadi karena kelalaian (misalnya human error, sistem tidak di-*update*) daripada kesengajaan.³⁹⁾ Akibatnya, banyak kasus kebocoran data tidak dapat dipidana berdasarkan UU PDP, sehingga korban kehilangan perlindungan pidana. Saran perbaikan: merevisi UU PDP dengan menambahkan pasal tentang delik *culpa* untuk kelalaian berat yang mengakibatkan kebocoran data massal.

Kedua, delik aduan Pasal 72. Ketentuan bahwa semua tindak pidana adalah delik aduan menghambat penegakan hukum, terutama untuk kasus dengan korban massal seperti Tokopedia (91 juta korban). Setiap korban harus melapor secara individual, yang tidak praktis dan membebani korban.⁴⁰⁾ Saran perbaikan: mengecualikan tindak pidana yang berdampak pada banyak korban (misalnya >1.000 orang) dari syarat delik

³⁹⁾ Edmon Makarim, Op. Cit, hlm. 220.

⁴⁰⁾ Sinta Dewi Rosadi, Op. Cit, hlm. 222.

aduan, atau memberikan kewenangan kepada otoritas pengawas untuk memulai proses pidana secara *ex officio*.

Ketiga, denda yang lebih rendah dari standar internasional. Denda maksimal Rp60 miliar untuk korporasi dinilai tidak cukup memberikan efek jera bagi perusahaan teknologi raksasa yang pendapatan tahunannya mencapai triliunan rupiah. Saran perbaikan: menaikkan batas maksimal denda menjadi persentase dari pendapatan (seperti GDPR) agar lebih proporsional.

F. Tinjauan tentang Putusan Pengadilan Negeri Jakarta Pusat Nomor 235/Pdt.G/2020/PN.Jkt.Pst

Putusan ini merupakan objek studi kasus dalam penelitian. Meskipun perkara ini adalah perkara perdata berupa gugatan ganti rugi, putusan ini memiliki relevansi pidana yang kuat karena menunjukkan kelemahan penegakan hukum sebelum berlakunya UU PDP. Perkara ini bermula dari insiden kebocoran data PT Tokopedia pada bulan Mei 2020, di mana data pribadi sekitar 91 juta pengguna berhasil dicuri dan dijual di forum gelap (*dark web*). Data yang bocor mencakup nama lengkap, alamat surel, nomor telepon, tanggal lahir, dan jenis kelamin, yang berpotensi disalahgunakan untuk kejahatan siber seperti *phishing* dan penipuan identitas.

Dalam perkara ini, Komunitas Konsumen Indonesia (KKI) bertindak sebagai penggugat yang mewakili kepentingan konsumen pengguna Tokopedia. Adapun yang menjadi tergugat adalah Menteri Komunikasi dan Informatika Republik Indonesia sebagai Tergugat I dan PT Tokopedia sebagai Tergugat II. Gugatan yang diajukan oleh KKI didasarkan pada dalil Perbuatan Melawan Hukum (PMH) karena kelalaian PT Tokopedia dalam menjaga sistem keamanan data pribadi konsumennya, serta kelalaian Menteri Kominfo dalam menjalankan fungsi pengawasan terhadap penyelenggara sistem elektronik. Para penggugat menuntut ganti rugi materiil dan pencabutan sertifikat elektronik Tokopedia.

Namun, Majelis Hakim Pengadilan Negeri Jakarta Pusat dalam putusannya mengabulkan eksepsi para tergugat dan menyatakan bahwa Pengadilan Negeri tidak

berwenang mengadili perkara tersebut dengan alasan kompetensi absolut. Hakim berpendapat bahwa sengketa ini masuk ke dalam ranah Peradilan Tata Usaha Negara (PTUN) karena substansi gugatan lebih menitikberatkan pada tindakan administrasi negara, yaitu kelalaian Menteri Kominfo dalam melakukan pengawasan dan tidak mencabut sertifikat elektronik Tokopedia. Akibat putusan ini, gugatan dinyatakan tidak dapat diterima (*niet ontvankelijke verklaard*) dan pemeriksaan terhadap pokok perkara tidak pernah dilakukan. Dari perspektif hukum pidana, putusan ini menunjukkan bahwa sebelum UU PDP berlaku, korban kebocoran data tidak memiliki akses yang jelas ke keadilan, baik melalui jalur perdata yang terhambat oleh persoalan kompetensi absolut maupun jalur pidana yang belum tersedia karena kekosongan hukum.

Dari perspektif hukum pidana, putusan ini menyisakan pertanyaan: mengapa kasus kebocoran data yang merugikan jutaan orang tidak diproses secara pidana? Jawabannya adalah karena sebelum UU PDP, tidak ada ketentuan pidana yang secara spesifik mengatur kebocoran data oleh korporasi. UU ITE hanya mengatur akses ilegal (Pasal 46) dan intersepsi (Pasal 48), yang lebih ditujukan kepada peretas eksternal, bukan kepada korporasi yang lalai.

Dengan adanya UU PDP, diharapkan kasus serupa di masa depan dapat diproses secara pidana, setidaknya untuk unsur kesengajaan (Pasal 67-75) dan untuk korporasi (Pasal 70). Namun, kelemahan delik *culpa* dan delik aduan tetap menjadi tantangan.

G. Perbandingan Pengaturan Tindak Pidana Perlindungan Data Pribadi di Indonesia dengan Negara Lain

Perbandingan dengan regulasi negara lain penting untuk melihat posisi UU PDP Indonesia dalam konteks global serta mengidentifikasi kelemahan dan kelebihan yang dapat dijadikan bahan evaluasi. Dua pembanding utama yang digunakan adalah General Data Protection Regulation (GDPR) Uni Eropa sebagai standar internasional, serta Personal Data Protection Act (PDPA) Singapura sebagai representasi negara ASEAN dengan sistem hukum yang maju.

1. Perbandingan dengan GDPR (Uni Eropa)

GDPR mulai berlaku pada 25 Mei 2018 dan dianggap sebagai *gold standard* dalam perlindungan data pribadi di dunia. Meskipun GDPR lebih berorientasi pada sanksi administratif, beberapa negara anggota UE (seperti Jerman, Prancis, dan Inggris) juga mengatur sanksi pidana dalam hukum nasionalnya untuk pelanggaran yang serius.

General Data Protection Regulation atau GDPR Uni Eropa merupakan salah satu instrumen hukum perlindungan data pribadi yang sering dijadikan rujukan internasional. Dalam hal jangkauan teritorial, GDPR memiliki sifat ekstrateritorial sebagaimana diatur dalam Pasal 3. Artinya, GDPR tidak hanya berlaku bagi pengendali atau prosesor data yang berada di wilayah Uni Eropa, tetapi juga dapat menjangkau pihak di luar Uni Eropa apabila melakukan pemrosesan data terhadap warga atau subjek data di Uni Eropa. Sementara itu, UU PDP Indonesia juga mengenal prinsip ekstrateritorial sebagaimana tercermin dalam Pasal 2, yaitu berlaku terhadap perbuatan hukum di luar wilayah Indonesia yang memiliki akibat hukum di wilayah Indonesia dan/atau bagi subjek data pribadi warga negara Indonesia di luar wilayah hukum Indonesia. Dengan demikian, baik GDPR maupun UU PDP sama-sama berupaya menjangkau pelanggaran data pribadi lintas negara, meskipun efektivitas penerapannya tetap bergantung pada mekanisme penegakan hukum masing-masing negara.

Dari segi sanksi administratif, GDPR mengatur ancaman denda yang jauh lebih tinggi dibandingkan UU PDP. Berdasarkan Pasal 83 GDPR, pelanggaran tertentu dapat dikenai denda administratif hingga €20 juta atau 4% dari total pendapatan tahunan global perusahaan pada tahun sebelumnya, dipilih mana yang lebih tinggi. Sementara itu, UU PDP mengatur sanksi administratif berupa denda administratif paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran. Perbedaan ini menunjukkan bahwa GDPR memiliki pendekatan yang lebih berat dalam memberikan efek jera kepada korporasi, khususnya perusahaan berskala besar yang memiliki pendapatan global sangat tinggi.

Dalam aspek sanksi pidana pokok, GDPR tidak mengatur sanksi pidana secara langsung dalam satu instrumen yang seragam, melainkan menyerahkan pengaturannya kepada hukum nasional masing-masing negara anggota Uni Eropa. Berbeda dengan

GDPR, UU PDP Indonesia secara tegas mengatur sanksi pidana dalam undang-undang yang sama. Pasal 67 dan Pasal 68 UU PDP mengatur pidana penjara paling lama 4 sampai 6 tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 sampai Rp6.000.000.000,00, tergantung pada jenis perbuatan yang dilakukan. Dengan demikian, kelebihan UU PDP terletak pada adanya pengaturan pidana yang lebih eksplisit dan langsung dapat digunakan sebagai dasar penegakan hukum pidana.

Selanjutnya, dari aspek sifat delik, GDPR memberikan kewenangan kepada otoritas pengawas atau Data Protection Authority untuk melakukan tindakan pengawasan dan penegakan secara aktif tanpa harus menunggu aduan dari korban. Dalam UU PDP, ketentuan pidana tidak secara tegas disebut sebagai delik aduan absolut, sehingga pada dasarnya dapat dipahami sebagai delik biasa. Hal ini berarti aparat penegak hukum dapat melakukan proses penegakan hukum tanpa harus menunggu pengaduan individual dari setiap korban. Namun, efektivitas penegakan hukum tetap sangat bergantung pada kesiapan aparat penegak hukum, pembentukan lembaga pengawas perlindungan data pribadi, serta kemampuan pembuktian dalam perkara pidana.

Dalam hal korporasi sebagai subjek tindak pidana, GDPR menyerahkan pengaturan pidana korporasi kepada hukum nasional masing-masing negara anggota. Adapun UU PDP secara tegas mengakui korporasi sebagai subjek tindak pidana. Pasal 70 UU PDP mengatur bahwa apabila tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau korporasi. Selain itu, korporasi dapat dikenai pidana denda paling banyak 10 kali dari maksimal pidana denda yang diancamkan, serta dapat dijatuhi pidana tambahan. Pengaturan ini menunjukkan bahwa UU PDP telah memberikan dasar hukum yang cukup kuat untuk meminta pertanggungjawaban pidana terhadap korporasi yang terlibat dalam pelanggaran data pribadi.

Namun, demikian, kelemahan utama UU PDP dibandingkan dengan sistem perlindungan data di beberapa negara adalah belum diaturnya delik culpa atau kelalaian dalam ranah pidana. Pasal 67 dan Pasal 68 UU PDP mensyaratkan adanya unsur

“dengan sengaja”, sehingga tindak pidana perlindungan data pribadi dalam UU PDP masih berorientasi pada kesengajaan atau dolus. Akibatnya, apabila kebocoran data terjadi karena kelalaian korporasi, seperti lemahnya sistem keamanan, tidak dilakukannya pembaruan sistem, atau kurangnya pengawasan internal, maka perkara tersebut lebih mudah dikenakan sanksi administratif daripada diproses sebagai tindak pidana. Kondisi ini menjadi salah satu kelemahan mendasar UU PDP, karena dalam praktiknya kebocoran data pribadi sering kali terjadi bukan karena kesengajaan untuk membocorkan data, melainkan karena kelalaian dalam pengelolaan dan pengamanan data.

Dengan demikian, perbandingan antara GDPR dan UU PDP menunjukkan bahwa UU PDP telah memiliki beberapa kelebihan, khususnya karena telah mengatur sanksi pidana dan pertanggungjawaban pidana korporasi secara langsung. Akan tetapi, UU PDP masih memiliki kelemahan dari sisi besaran denda, belum optimalnya pengaturan mengenai kelalaian korporasi dalam ranah pidana, serta tantangan kelembagaan dalam pelaksanaan pengawasan. Oleh karena itu, penguatan UU PDP perlu diarahkan pada peningkatan efektivitas sanksi, penambahan pengaturan delik culpa untuk kelalaian berat, serta pembentukan otoritas pengawas yang independen dan memiliki kewenangan kuat.

Dari data terlihat bahwa kelebihan utama UU PDP dibandingkan dengan GDPR adalah adanya pengaturan sanksi pidana yang terintegrasi secara langsung dalam undang-undang, sehingga aparat penegak hukum tidak perlu menunggu pengaturan lebih lanjut dalam hukum nasional masing-masing seperti halnya di Uni Eropa yang menyerahkan pengaturan sanksi pidana kepada negara anggota. Hal ini memberikan kepastian hukum yang lebih cepat dan terukur bagi penegak hukum di Indonesia, karena ancaman pidana penjara dan denda telah dirumuskan secara jelas dan tegas dalam setiap pasal. Namun demikian, terdapat beberapa kelemahan signifikan yang perlu dicatat. Pertama, besaran denda administratif dalam UU PDP hanya mencapai maksimal 2% dari pendapatan tahunan, jauh lebih rendah dibandingkan GDPR yang menganut 4% dari pendapatan global tahunan atau €20 juta, sehingga efektivitas efek

jera bagi korporasi besar diragukan. Kedua, UU PDP belum mengatur jangkauan ekstrateritorial, berbeda dengan GDPR yang berlaku bagi pengendali data di luar Uni Eropa yang memproses data warga UE, sehingga korporasi asing yang beroperasi di Indonesia sulit dijangkau oleh ketentuan pidana dalam UU PDP. Ketiga, pemberlakuan delik aduan absolut dalam UU PDP menjadi hambatan serius bagi penegakan hukum, karena proses pidana tidak dapat dimulai tanpa adanya pengaduan dari korban, yang sangat tidak praktis untuk kasus kebocoran data massal dengan jumlah korban yang sangat besar, seperti yang terjadi pada kasus Tokopedia. Dengan demikian, meskipun UU PDP memiliki keunggulan dalam hal pengaturan sanksi pidana yang terintegrasi, kelemahan-kelemahan tersebut perlu segera diatasi melalui revisi agar perlindungan data pribadi di Indonesia dapat setara dengan standar internasional.

2. Perbandingan dengan PDPA Singapura

Selain dibandingkan dengan GDPR Uni Eropa, pengaturan perlindungan data pribadi di Indonesia juga dapat dibandingkan dengan *Personal Data Protection Act* atau PDPA Singapura. Perbandingan ini penting karena Singapura merupakan salah satu negara di kawasan Asia Tenggara yang telah lebih dahulu memiliki regulasi khusus mengenai perlindungan data pribadi dan sistem pengawasan yang relatif mapan.

Dari aspek sanksi administratif, PDPA Singapura mengatur denda administratif maksimal sebesar SGD 1.000.000 atau 10% dari pendapatan tahunan organisasi di Singapura, dipilih mana yang lebih tinggi. Ketentuan ini menunjukkan bahwa Singapura menggunakan pendekatan denda yang bersifat proporsional terhadap skala ekonomi pelaku usaha. Sementara itu, UU PDP Indonesia mengatur sanksi administratif berupa denda paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran sebagaimana diatur dalam Pasal 57 ayat (3). Jika dibandingkan, pendekatan PDPA Singapura tampak lebih tegas terhadap korporasi besar karena besaran dendanya dapat disesuaikan dengan kemampuan ekonomi organisasi yang melakukan pelanggaran.

Dari segi sanksi pidana pokok, PDPA Singapura mengatur ancaman pidana berupa denda hingga SGD 10.000 dan/atau pidana penjara hingga 3 tahun untuk pelanggaran

tertentu, misalnya tindakan re-identification terhadap data anonim. Berbeda dengan itu, UU PDP Indonesia mengatur ancaman pidana yang lebih berat, yaitu pidana penjara maksimal 6 tahun dan/atau denda maksimal Rp6.000.000.000,00 untuk perorangan, sebagaimana diatur dalam Pasal 67 dan Pasal 68. Hal ini menunjukkan bahwa UU PDP Indonesia memiliki karakter pidana yang lebih kuat dibandingkan PDPA Singapura, terutama dari sisi ancaman pidana penjara dan besaran denda pidana.

Selanjutnya, dari aspek sifat delik, PDPA Singapura tidak secara tegas menempatkan pelanggaran perlindungan data pribadi sebagai delik aduan. Otoritas pengawas perlindungan data pribadi di Singapura, yaitu *Personal Data Protection Commission* atau PDPC, dapat bertindak secara aktif dalam melakukan pengawasan dan penegakan hukum tanpa harus menunggu pengaduan dari korban. Adapun dalam UU PDP Indonesia, ketentuan pidana juga tidak secara tegas disebut sebagai delik aduan, sehingga lebih tepat diklasifikasikan sebagai delik biasa. Dengan demikian, aparat penegak hukum pada prinsipnya dapat melakukan penegakan hukum tanpa harus menunggu pengaduan individual dari setiap subjek data pribadi yang dirugikan.

Dari aspek jangkauan teritorial, PDPA Singapura pada dasarnya berlaku secara teritorial, namun tetap dapat mengikat organisasi di luar Singapura apabila organisasi tersebut memproses data pribadi yang dikumpulkan di Singapura. Sementara itu, UU PDP Indonesia menganut prinsip ekstrateritorial sebagaimana diatur dalam Pasal 2 huruf b, yaitu berlaku terhadap perbuatan hukum di luar wilayah Indonesia yang memiliki akibat hukum di wilayah Indonesia dan/atau bagi subjek data pribadi warga negara Indonesia di luar wilayah hukum Indonesia. Dengan adanya pengaturan tersebut, UU PDP berusaha menjangkau pelanggaran data pribadi yang terjadi lintas batas negara, terutama dalam konteks perkembangan ekonomi digital yang tidak lagi terbatas oleh wilayah geografis.

Berdasarkan perbandingan tersebut, dapat disimpulkan bahwa UU PDP Indonesia memiliki keunggulan dari segi ancaman pidana yang lebih tegas, khususnya karena mengatur pidana penjara dan denda dalam jumlah besar bagi pelaku perorangan maupun korporasi. Namun, PDPA Singapura memiliki kelebihan dari sisi kelembagaan

dan efektivitas pengawasan, karena adanya otoritas khusus yaitu PDPC yang dapat bertindak secara aktif dalam menegakkan aturan perlindungan data pribadi. Oleh karena itu, Indonesia perlu memperkuat pelaksanaan UU PDP, terutama melalui pembentukan lembaga pengawas yang independen dan efektif, agar perlindungan data pribadi tidak hanya kuat secara normatif, tetapi juga dapat diterapkan secara nyata dalam praktik.

PDA Singapura memiliki ancaman pidana yang lebih ringan dibandingkan UU PDP Indonesia. Namun, kelebihan PDPA adalah tidak adanya delik aduan sehingga otoritas pengawas (Personal Data Protection Commission) dapat mengambil tindakan tanpa menunggu laporan korban.⁴¹⁾ Hal ini mempercepat proses penegakan hukum.

3. Implikasi bagi Indonesia

Perbandingan di atas, Indonesia memiliki ancaman pidana yang relatif berat (6 tahun penjara) dibandingkan Singapura (3 tahun) dan rata-rata negara anggota UE. Namun, efektivitas penegakan hukum pidana sangat tergantung pada penghapusan atau pengecualian delik aduan untuk kasus-kasus massal. Saran yang dapat diambil adalah merevisi Pasal 72 UU PDP agar otoritas pengawas yang akan dibentuk memiliki kewenangan untuk memulai proses pidana secara *ex officio* untuk kebocoran data yang berdampak pada banyak korban.

H. Kelemahan UU PDP dan Saran Perbaikan dari Perspektif Hukum Pidana

Berdasarkan uraian teori dan perbandingan di atas, dapat diidentifikasi beberapa kelemahan UU PDP yang perlu mendapat perhatian:

1. Kesiadaan Delik *Culpa* (Kealpaan)

Sebagaimana telah dijelaskan sebelumnya, seluruh tindak pidana dalam UU PDP mensyaratkan adanya unsur kesengajaan (*dolus*). Ketentuan ini tercermin dalam penggunaan frasa "dengan sengaja" pada setiap pasal pidana, mulai dari Pasal 67

⁴¹⁾ Personal Data Protection Commission, *Guide to Enforcement*, Singapura, 2021.

sampai dengan Pasal 75. Artinya, untuk dapat dipidana, pelaku harus terbukti memiliki niat atau kehendak untuk melakukan perbuatan yang dilarang tersebut.

Namun, dalam praktik kebocoran data skala besar, penyebab utamanya lebih sering bersumber dari kelalaian (*culpa*) daripada kesengajaan. Deputi Badan Siber dan Sandi Negara (BSSN) mengungkapkan bahwa 60-70% penyebab kebocoran data pribadi berasal dari rendahnya kepatuhan sumber daya manusia terhadap regulasi dan standar keamanan yang berlaku. Kelalaian ini dapat berupa tidak dilakukannya *update* sistem keamanan secara berkala, tidak diterapkannya enkripsi data yang memadai, lemahnya pengawasan internal terhadap akses data, hingga kelalaian karyawan dalam menjaga kerahasiaan informasi. Bahkan, praktik di lapangan menunjukkan bahwa banyak kebocoran data justru berawal dari kelalaian internal akibat kurangnya standar operasional prosedur (SOP) dan rendahnya kesadaran karyawan terhadap pentingnya keamanan data.⁴²⁾

Akibat dari ketiadaan delik *culpa* ini, banyak kasus kebocoran data yang tidak dapat diproses secara pidana berdasarkan UU PDP. Sebab, untuk membuktikan adanya unsur kesengajaan dalam kasus kebocoran data yang disebabkan oleh kelalaian sistemik atau human error, aparat penegak hukum menghadapi kesulitan yang sangat besar. Unsur kesengajaan dan melawan hukum harus dibuktikan secara tegas di pengadilan, sementara korban juga harus mampu menunjukkan adanya kerugian yang dialami sebagai akibat langsung dari perbuatan tersebut. Hingga saat ini, kasus pidana yang diproses berdasarkan UU PDP masih didominasi oleh pelaku individu, dan belum ada perkara dengan terpidana korporasi yang tercatat dalam direktori putusan Mahkamah Agung.

Saran perbaikan: Menambahkan pasal baru yang mengatur delik *culpa* untuk kelalaian berat (*gross negligence*) yang mengakibatkan kebocoran data massal

⁴²⁾ Hukumonline, "Kelalaian Pelindungan Data Pribadi Berpotensi Pengurus Perusahaan Terancam Pidana", 11 Februari 2026, tersedia pada: <https://www.hukumonline.com/berita/a/kelalaian-pelindungan-data-pribadi-berpotensi-pengurus-perusahaan-terancam-pidana-lt698bf5736f816/?page=1>, diakses pada 27 Juni 2026.

(misalnya lebih dari 10.000 subjek data). Ancaman pidana dapat lebih ringan dari delik dolus, misalnya penjara maksimal 2 tahun dan denda maksimal Rp2 miliar untuk perorangan, serta pemberatan untuk korporasi.

2. Delik Aduan Absolut Pasal 72

Delik aduan absolut menghambat penegakan hukum untuk kasus dengan korban massal seperti Tokopedia (91 juta korban). Setiap korban harus melapor secara individual, yang secara praktis mustahil dilakukan. Hal ini bertentangan dengan tujuan pemidanaan (prevensi umum) karena pelaku dapat lolos dari jeratan pidana.⁴³⁾

Saran perbaikan: Merevisi Pasal 72 UU PDP dengan mengecualikan tindak pidana yang berdampak pada banyak korban (misalnya lebih dari 1.000 subjek data) dari syarat delik aduan. Selain itu, memberikan kewenangan kepada otoritas pengawas perlindungan data pribadi untuk memulai proses pidana secara *ex officio* berdasarkan temuan pengawasan atau laporan dari masyarakat tanpa harus menunggu pengaduan individual.

3. Denda yang Relatif Rendah Dibandingkan Standar Internasional

Denda administratif maksimal yang diatur dalam UU PDP untuk korporasi adalah sebesar 2% (dua persen) dari pendapatan tahunan atau penerimaan tahunan pelaku usaha terhadap variabel pelanggaran. Apabila digabungkan dengan ketentuan pidana denda bagi korporasi pada Pasal 70 ayat (2) yang memberlakukan pemberatan pidana denda paling banyak 10 (sepuluh) kali dari pidana denda maksimal masing-masing tindak pidana (yakni Rp6 miliar), maka batas maksimal pidana denda yang dapat dijatuhkan kepada korporasi adalah sebesar Rp60 miliar.

Besaran denda administratif 2% dari pendapatan tahunan ini, meskipun dapat mencapai angka yang sangat besar bagi korporasi besar, tetap dinilai tidak cukup memberikan efek jera jika dibandingkan dengan standar internasional, khususnya *General Data Protection Regulation* (GDPR) Uni Eropa. Sebagai perbandingan, GDPR menerapkan denda administratif maksimal yang jauh lebih

⁴³⁾ Sinta Dewi Rosadi, Op. Cit, hlm. 222.

tinggi, yaitu sebesar €20.000.000 (dua puluh juta euro) atau 4% (empat persen) dari total pendapatan global tahunan perusahaan pada tahun fiskal sebelumnya, mana yang lebih besar.

Perbedaan besaran denda ini memiliki implikasi yang sangat signifikan terhadap efektivitas penegakan hukum dan efek jera bagi pelaku usaha. Sebagai ilustrasi nyata, pada bulan Mei 2023, Meta Platforms Ireland Limited (Facebook) dikenakan denda sebesar €1,2 miliar (setara sekitar Rp19,3 triliun) oleh Otoritas Perlindungan Data Irlandia atas pelanggaran transfer data pribadi pengguna Eropa ke Amerika Serikat. Denda ini merupakan yang terbesar yang pernah dijatuhkan berdasarkan GDPR. Jumlah ini jauh melampaui batas maksimal denda yang dapat dijatuhkan berdasarkan UU PDP, bahkan setelah pemberatan 10 kali lipat sekalipun.⁴⁴⁾

Dengan demikian, ketentuan denda dalam UU PDP memiliki beberapa kelemahan mendasar. Pertama, batas maksimal denda administratif 2% dari pendapatan tahunan dinilai masih terlalu rendah untuk memberikan efek jera yang nyata bagi korporasi besar, terutama mengingat skala usaha perusahaan teknologi raksasa yang pendapatan tahunannya dapat mencapai triliunan rupiah. Kedua, penerapan pidana denda dengan pemberatan 10 kali lipat yang menghasilkan batas maksimal Rp60 miliar masih jauh di bawah besaran denda yang diterapkan di tingkat internasional. Ketiga, efektivitas penegakan sanksi administratif masih terhambat oleh belum terbentuknya lembaga perlindungan data pribadi sebagaimana diamanatkan oleh UU PDP.

4. Belum Adanya Lembaga Otoritas Pengawas yang Independen

Pasal 58 UU PDP mengamanatkan pembentukan lembaga otoritas pengawas perlindungan data pribadi yang independen. Namun, hingga saat penelitian ini dilakukan (April 2026), lembaga tersebut belum sepenuhnya terbentuk dan berfungsi. Tanpa otoritas pengawas yang efektif, penegakan pidana akan bergantung sepenuhnya

⁴⁴⁾ European Data Protection Board (EDPB), "1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision", 22 Mei 2023, tersedia pada: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en, diakses pada 27 Juni 2026.

pada kepolisian dan kejaksaan yang mungkin tidak memiliki keahlian teknis di bidang perlindungan data.

Saran perbaikan, mempercepat pembentukan lembaga otoritas pengawas dengan kewenangan yang kuat, termasuk kewenangan melakukan penyelidikan, mengumpulkan bukti, dan melimpahkan perkara pidana kepada kejaksaan. Otoritas pengawas juga harus memiliki unit khusus yang menangani aspek pidana.

5. Tidak Ada Pengaturan Ekstrateritorial

Salah satu kelemahan mendasar yang masih diperdebatkan dalam UU PDP adalah pengaturan mengenai prinsip ekstrateritorialitas. Pasal 56 UU PDP yang mengatur tentang transfer data pribadi ke luar wilayah hukum Indonesia seringkali ditafsirkan oleh sebagian pihak sebagai dasar keberlakuan hukum Indonesia secara ekstrateritorial.. Dalam sidang pengujian materiil di Mahkamah Konstitusi, ahli dari Fakultas Hukum Universitas Indonesia, Yu Un Oppusunggu, menyatakan bahwa norma hukum Pasal 56 ayat (1) UU PDP mengatur transfer data pribadi ke luar wilayah hukum Indonesia sebagai suatu pemrosesan yang tetap tunduk pada hukum positif Indonesia, sehingga UU PDP berlaku secara teritorial maupun ekstrateritorial.⁴⁵⁾

Penafsiran ini semakin diperkuat dengan pernyataan bahwa Pasal 56 UU PDP menunjukkan kehadiran negara dalam menjamin hak konstitusional warga negara atas perlindungan data pribadi, dan ketentuan ini tidak dapat dikesampingkan oleh kesepakatan para pihak dalam hubungan hukum perdata. Dengan demikian, secara normatif, UU PDP sebenarnya telah mengatur keberlakuan ekstrateritorial melalui mekanisme transfer data lintas negara yang tetap harus mematuhi ketentuan UU PDP.

Saran perbaikan: Menambahkan pasal yang mengatur jangkauan ekstrateritorial UU PDP, setidaknya untuk pengendali data yang memiliki kegiatan usaha di Indonesia atau yang secara aktif menargetkan konsumen Indonesia.

⁴⁵⁾ Fakultas Hukum Universitas Indonesia, "Dosen FHUI: UU PDP Berlaku Secara Teritorial dan Ekstra Teritorial", 3 November 2025, tersedia pada: <https://law.ui.ac.id/dosen-fhui-uu-pdp-berlaku-secara-teritorial-dan-ekstra-teritorial/>, diakses pada 27 Juni 2026.