

BAB II

TINJAUAN TEORI MENGENAI PERLINDUNGAN HUKUM DATA

PRIBADI DAN PERETASAN KARTU PERDANA

A. Aspek Hukum Tentang Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2024 tentang Perlindungan Data Pribadi

1. Pengertian Data Pribadi

Data pribadi merujuk pada informasi yang mencakup identitas, kode, simbol, huruf, atau angka yang digunakan untuk mengidentifikasi seseorang secara pribadi dan bersifat rahasia.¹ Data pribadi adalah segala informasi yang dapat mengenali seseorang baik secara langsung maupun tidak langsung. Hal ini mencakup, tetapi tidak terbatas pada, nama, alamat, nomor telepon, alamat surel, tanggal lahir, nomor identifikasi, informasi keuangan, dan data medis.² Kamus Besar Bahasa Indonesia mendefinisikan data ialah keterangan benar dan nyata yang dapat dijadikan dasar kajian.³ Sedangkan pribadi memiliki arti sendiri manusia sebagai perseorangan (diri manusia atau diri sendiri).⁴

Setiap negara memiliki terminologi yang berbeda terkait dengan informasi pribadi. Di Amerika Serikat, Kanada, dan Australia, istilah yang

¹ Sautunnida, L, 'Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris dan Malaysia' (2018), Vol. 20 No. 2, *Kanun Jurnal Ilmu Hukum*, Hlm. 369-384.

² Mahira, DF, Emilda Y Lisa NA, 'Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept' (2020), Vol. 3 No. 2, *Legislatif*, Hlm. 287 -302

³ <https://kbbi.web.id/data>, diakses pada hari Jumat tanggal 10 Mei 2024, Pukul 20.35 WIB.

⁴ <https://kbbi.web.id/pribadi>, diakses pada hari Jumat tanggal 10 Mei 2024, Pukul 20.35 WIB.

digunakan adalah informasi pribadi, sedangkan di negara-negara Uni Eropa dan Indonesia, istilah yang digunakan adalah data pribadi.⁵ Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.⁶ Dapat disimpulkan bahwa data pribadi merupakan informasi yang dapat mengidentifikasi individu tertentu dan dapat digunakan untuk keperluan tertentu sesuai dengan maksud dan tujuannya.

Istilah data pribadi pertama kali muncul di Jerman dan Swedia di tahun 1970-an hal ini muncul karena pada waktu itu mulai dipergunakannya komputer yang digunakan untuk menyimpan data penduduk di masa itu, ternyata berselang hanya beberapa tahun terdapatnya pelanggaran yang dilakukan oleh pelaku kejahatan maka dari itu untuk mengurangi adanya kejahatan maka dibuatnya peraturan akan hal ini. di beberapa negara maju mengistilakan data pribadi sebagai sebuah *privacy*, yang merupakan suatu hak seseorang yang harus dilindungi dan tidak dapat diganggu kehidupan pribadinya.⁷

Pasal 1 Undang-Undang Perlindungan Data Pribadi menjelaskan bahwa:

“Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau

⁵ Latumahina, R. E, ‘Aspek Hukum Perlindungan Data Pribadi di Dunia Maya’ (2014), Vol. 3 No. 2, *Jurnal Gema Aktualita*, Hlm. 35.

⁶ Mahiar DF & Emilda Y Lisa NA, *loc cit*.

⁷ Rosalinda Elsina Latumahina, ‘Aspek Hukum Perlindungan Data Pribadi di Dunia Maya’ (2014), Vol. 3 No. 2, *Jurnal Gema Aktualita*, Hlm.16-17.

dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik”

Selain itu, Pasal 1 Angka 29 Peraturan Pemerintah No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, memberikan pengertian mengenai data pribadi sebagai berikut:

“Data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi secara tersendiri dan/atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik”.

Menurut Purwanto data merupakan bahan baku informasi, yang didefinisikan sebagai kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan benda dan sebagainya. Data terbentuk dari karakter yang dapat berupa alfabet, angka, maupun simbol khusus. Data disusun untuk diolah dalam bentuk struktur data, struktur file, dan data base.⁸

Jerry Kang mendefinisikan data pribadi sesuatu yang menggambarkan informasi yang erat kaitannya dengan seseorang yang membedakan karakteristik masing-masing individu,⁹ sedangkan teori menurut Raymond Wacks, data pribadi adalah informasi pribadi seseorang yang terdiri dari fakta-fakta, komunikasi, opini yang memiliki hubungan terhadap individu dan

⁸ Sederhana Waruwu, ‘Perlindungan Hukum Terhadap Data Pribadi Pelanggan Penyedia Layanan Telekomunikasi Di Kota Medan’, (Skripsi, Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Medan Area, Medan, 2022), Hlm. 18.

⁹ *Ibid.*, Hlm. 20.

individu tersebut merasa bahwa informasi tersebut bersifat sensitif dan dibatasi atau dilarang pengumpulan, penggunaan atau peredarannya.¹⁰

Nilai data pribadi sebagai hak pribadi (*Privacy Rights*) terdiri dari sejumlah arti penting yaitu:

- a. hak pribadi adalah hak menikmati kehidupan personal dan kebebasan terlepas dari segala distraksi;
- b. hak pribadi adalah hak bersosialisasi dengan individu lain tanpa adanya tindakan pengamatan secara diam;
- c. hak pribadi adalah hak melakukan pengawasan terhadap akses informasi terkait kehidupan personal dan informasi individu.¹¹

Terkait hak pribadi sebagai hak asasi manusia dijelaskan Danrivanto Budhijanto, bahwa “Perlindungan terhadap hak-hak pribadi atau hak-hak privat akan meningkatkan nilai-nilai kemanusiaan, meningkatkan hubungan antara individu dan masyarakatnya, meningkatkan kemandirian atau otonomi untuk melakukan kontrol dan mendapatkan kepantasan, serta meningkatkan toleransi dan menjauhkan dari perlakuan diskriminasi serta membatasi kekuasaan pemerintah.”¹²

¹⁰ Bismo, ‘Perlindungan Data Pribadi Anak Di Dunia Digital Berdasarkan Ketentuan Internasional Dan Nasional’, (Skripsi, Fakultas Hukum, Universitas Lampung, 2019), Hlm.28.

¹¹ M. Jefri Maruli Tacino, ‘Perlindungan Hukum Terhadap Hak Pribadi Seseorang Di Media Sosial Menurut Undang Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik’ (2020), Vol. 26 No. 2, *Dinamika: Jurnal Ilmiah Ilmu Hukum*, Hlm. 174–84.

¹² Danrivanto Budhijanto, *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*, PT. Refika Aditama, Bandung, 2010, Hlm. 4.

Adapun pendapat Susan. E Gindin, berbagai informasi dapat diakses melalui Internet, dan terdapat tiga jenis data pribadi atau informasi pribadi yang dapat diambil secara tidak sah. Yang pertama disediakan dalam bentuk database online; yang kedua adalah informasi yang dapat diperoleh melalui transaksi online dan dikumpulkan melalui partisipasi pribadi dalam aktivitas jaringan; dan yang ketiga adalah dalam database yang Anda miliki.¹³

Altman menyebutkan bahwa fungsi data pribadi yaitu¹⁴

1. Pengatur dan pengontrol interaksi personal yang berarti sejauh mana hubungan dengan orang lain diinginkan, kapan waktunya menyendiri dan kapan waktunya bersama sama dengan orang lain yang dikehendaki.
2. Merencanakan dan membuat strategi untuk berhubungan dengan orang lain, yang meliputi keintiman atau jarak dalam berhubungan dengan orang lain.

2. Klasifikasi Data Pribadi

Pengaturan mengenai klasifikasi data pribadi, diatur dalam Pasal 4 UU PDP Nomor 27 Tahun 2022. Merujuk pada aturan tersebut, klasifikasi data pribadi terdiri atas:

- a. Data pribadi yang bersifat spesifik.

¹³ Edmon Makarim, *Pengantar Hukum Telematika Suatu Kompilasi Kajian*, PT. Raja Grafindo Persada, Jakarta, 2005, Hlm. 181.

¹⁴ Nova Purnama Lisa, 'Privasi Pada Pekarangan Sebagai Ruang Terbuka Privat Perkotaan Di Kawasan Hunian Jeron Beteng Kraton Yogyakarta' (2015), Vol. 5 No. 5, *Jurnal Arsitekno*, Hlm. 73.

b. Data pribadi yang bersifat umum.

Data pribadi yang bersifat spesifik merupakan data pribadi yang apabila dalam pemrosesannya dapat mengakibatkan dampak lebih besar kepada subjek data pribadi, antara lain tindakan diskriminasi dan kerugian yang lebih besar subjek data pribadi.

a. Data pribadi yang bersifat spesifik

Data pribadi yang bersifat spesifik dapat berupa data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan data lainnya sesuai dengan ketentuan pertauran perundang-undangan.

b. Data pribadi yang bersifat umum

Data pribadi yang bersifat umum dapat berupa nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan dan data yang dikombinasikan untuk mengidentifikasi seseorang.

3. Hak-Hak Subjek Data Pribadi

Hak subjek data pribadi adalah orang perseorangan yang pada dirinya melekat data pribadi, sehingga hubungannya saling terkait dengan data pribadi.

Dalam UU PDP memuat hak subjek data pribadi, meliputi:

- a. Subjek data pribadi berhak mendapatkan Informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi.

- b. Subjek data pribadi berhak melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi tentang dirinya sesuai dengan tujuan pemrosesan data pribadi.
- c. Subjek data pribadi berhak mendapatkan akses dan memperoleh salinan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.
- d. Subjek data pribadi berhak menarik kembali persetujuan pemrosesan data pribadi tentang dirinya yang telah diberikan kepada pengendali data pribadi

Pasal 13 ayat (1) dan (2) UU PDP menyebutkan, subjek data pribadi berhak untuk mengakhiri pemrosesan, berhak menghapus, memusnahkan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan, berhak menarik kembali persetujuan data pribadi, menunda pemrosesan atau berhak mengajukan keberatan atau tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis dan lainnya.

Adapun Pasal 15 ayat (1) UU PDP hak-hak subjek data pribadi dikecualikan yaitu :

- a. kepentingan pertahanan dan keamanan nasional;
- b. kepentingan proses penegakan hukum;
- c. kepentingan umum dalam rangka penyelenggaraan negara;

- d. kepentingan pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau
- e. kepentingan statistik dan penelitian ilmiah.

Pasal 15 ayat (1) UU PDP tersebut tidak secara terang dan menjelaskan secara pasti dan akurat mengenai yang dimaksud dengan kepentingan pertahanan dan keamanan nasional. Sehingga pasal *a quo* berpotensi menjadi pasal yang multitafsir dan bermasalah di kemudian hari dan digunakan sebagai justifikasi untuk mengecualikan hak-hak subjek data pribadi⁶ selain itu pasal tersebut hanya akan berpotensi pada *abuse of power*.

Selain adanya subjek data ada pula pengendali data pribadi. Definisi mengenai pengendali data pribadi diatur dalam Pasal 1 Ayat 4, UU PDP yaitu setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi.

B. Tinjauan Teori Mengenai Perlindungan Hukum Terhadap Data Pribadi Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

1. Pengertian Perlindungan Hukum

Menurut Kamus Besar Bahasa Indonesia (KBBI), perlindungan hukum didefinisikan sebagai tempat berlindung atau tindakan (dan berbagai hal

lainnya) yang bertujuan untuk melindungi.¹⁵ Sedangkan hukum adalah peraturan yang dibuat oleh pemerintah atau yang data berlaku bagi semua orang dalam masyarakat (negara).

Fitzgerald mengutip istilah teori perlindungan hukum dari Salmond bahwa hukum bertujuan mengintegrasikan dan mengkoordinasikan berbagai kepentingan dalam masyarakat karena dalam suatu lalu lintas kepentingan, perlindungan terhadap kepentingan tertentu dapat dilakukan dengan cara membatasi berbagai kepentingan di lain pihak. Kepentingan hukum adalah mengurus hak dan kepentingan manusia, sehingga hukum memiliki otoritas tertinggi untuk menentukan kepentingan manusia yang perlu diatur dan dilindungi. Perlindungan hukum harus melihat tahapan yakni perlindungan hukum lahir dari suatu ketentuan hukum dan segala peraturan hukum yang diberikan oleh masyarakat yang pada dasarnya merupakan kesepakatan masyarakat tersebut untuk mengatur hubungan perilaku antara anggota-anggota masyarakat dan antara perseorangan dengan pemerintah yang dianggap mewakili kepentingan masyarakat.¹⁶ Adapun pendapat yang dikutip dari beberapa ahli mengenai perlindungan hukum sebagai berikut:

- a. Menurut Hetty Hassanah, perlindungan hukum adalah segala upaya yang dapat menjamin kepastian hukum sehingga dapat memberikan perlindungan hukum kepada pihak yang bersangkutan atau yang melakukan tindakan hukum.¹⁷

¹⁵ Dendi Sugiyono, *loc cit.*

¹⁶ Satjipto Raharjo, *Ilmu Hukum*, PT. Citra Aditya Bakti, Bandung, 2000, Hlm. 53

¹⁷ Hetty Hassanah, *loc cit.*

- b. Menurut Satjito Rahardjo perlindungan hukum adalah adanya upaya melindungi kepentingan seseorang dengan cara mengalokasikan suatu Hak Asasi Manusia kekuasaan kepadanya untuk bertindak dalam rangka kepentingannya tersebut.

Perlindungan hukum menurut Muchsin dapat dibagi menjadi 2 yaitu perlindungan hukum preventif dan perlindungan hukum represif :

- a. Perlindungan hukum preventif merupakan perlindungan yang diberikan oleh pemerintah dengan tujuan untuk mencegah terjadinya pelanggaran. Perlindungan ini tersedia di peraturan perundang undangan.
- b. Perlindungan hukum represif merupakan perlindungan yang sifatnya sudah terjadi, perlindungan berupa sanksi berupa denda, penjara serta hukuman tambahan apabila sudah terjadi suatu pelanggaran.¹⁸

2. Pengertian Upaya Hukum

Upaya hukum ialah suatu usaha setiap pribadi atau badan hukum yang merasa dirugikan haknya atau atas kepentingannya untuk memperoleh keadilan dan perlindungan atau kepastian hukum menurut cara-cara yang ditetapkan dalam undang-undang. Upaya hukum dibagi menjadi dua yaitu, upaya hukum melalui pengadilan (litigasi) dan upaya hukum di luar pengadilan (non litigasi).

- a. Upaya Hukum Litigasi

¹⁸ Muchsin, *Perlindungan dan Kepastian Hukum bagi Investor di Indonesia*, Magister Ilmu Hukum Program Pascasarjana Universitas Sebelas Maret, Surakarta, 2003, Hlm 14.

Proses penyelesaian kasus yang dilaksanakan melalui pengadilan atau yang sering disebut “litigasi” yaitu suatu penyelesaian kasus yang dilaksanakan dengan proses beracara di pengadilan dimana kewenangan untuk mengatur dan memutuskannya dilaksanakan oleh hakim.¹⁹ Upaya hukum pidana dikenal dengan istilah *ultimum remedium*. Istilah tersebut ditemukan dalam buku yang ditulis oleh Wirjono Prodjodikoro berjudul *Asas-Asas Hukum Pidana di Indonesia* menyebutkan norma-norma atau kaidah-kaidah dalam bidang hukum tata negara dan hukum tata usaha negara harus pertama-tama ditanggapi dengan sanksi administrasi. Begitu pula norma-norma dalam bidang hukum perdata pertama-tama harus ditanggapi dengan sanksi perdata. Hanya, apabila sanksi administrasi dan sanksi perdata ini belum mencukupi untuk mencapai tujuan meluruskan neraca kemasyarakatan, maka baru diadakan juga sanksi pidana sebagai pamungkas (terakhir) atau *ultimum remedium*.²⁰

b. Upaya hukum non litigasi

Upaya ini merupakan penyelesaian sengketa yang dilakukan di luar pengadilan, atau yang dikenal sebagai lembaga alternatif penyelesaian sengketa. Penyelesaian sengketa di luar pengadilan (non-litigasi) merupakan upaya tawar-menawar atau kompromi untuk memperoleh jalan keluar yang saling menguntungkan. Salah satu cara

¹⁹ Nurmaningsih Amriani, *Mediasi Alternatif Penyelesaian Sengketa di Pengadilan*, Universitas Trisakti, Jakarta, 2010, Hlm. 89

²⁰ <https://www.hukumonline.com/klinik/a/arti-ultimum-remedium-sebagai-sanksi-pamungkas-lt53b7be52bcf59/>, diakses pada hari Kamis tanggal 18 Juli 2024, Pukul 21.59 WIB.

penyelesaian sengketa yang banyak dilakukan terkait dengan kepemilikan nama domain melalui arbitrase.²¹ Kata arbitrase berasal dari kata *arbitrare* (latin), *arbitrage* (belanda), *arbitration* (inggris), *schiedspruch* (jerman), dan *arbitrage* (prancis), yang berarti kekuasaan untuk menyelesaikan sesuatu menurut kebijaksanaan atau damai oleh arbiter atau wasit²² pengertian arbitrase adalah cara-cara penyelesaian hakim partikular yang tidak terkait dengan dengan berbagai formalitas, cepat dan memberikan keputusan, karena dalam instansi terakhir serta mengikat, yang mudah untuk melaksanakan karena akan di taati para pihakUnsur-Unsur Arbitrase.²³ Semesntara Pasal 1 angka 1 Undang-Undang Nomor 30 Tahun 1999 tentang Arbitrase dan Alternatif Penyelesaian Sengketa menyebutkan bahwa:

"Arbitrase adalah cara penyelesaian suatu sengketa perdata di luar peradilan umum yang didasarkan pada perjanjian arbitrase yang dibuat secara tertulis oleh para pihak yang bersengketa."

3. Pengertian Perlindungan Data Pribadi

Kata "perlindungan" diartikan sebagai proteksi ²⁴ yaitu proses atau perbuatan yang dilakukan untuk melindungi, biasanya perlindungan itu sendiri berarti menaungi sesuatu hal yang dianggap cukup berbahaya. Sementara, Pasal 1 ayat 2 UU PDP menyebutkan bahwa pelindungan data pribadi adalah

²¹ <https://repository.unikom.ac.id/49456/1/Bahan%20Kuliah%20OL%20KH%201.docx>, diakses pada hari Kamis tanggal 18 juli 2024, Pukul 22.25 WIB.

²² R. Subekti, *kumpulan karangan hukum perakitan, Arbitrase, dan peradilan*, Alumni, Bandung, 1980, Hlm. 1.

²³ Sudargo Gautama, *Kontrak Dagang Internasional*, Alumni, Bandung, 1976, Hlm. 5.

²⁴ <https://kbbi.web.id/>, diakses pada hari Rabu tanggal 1 Mei 2024, Pukul 10.19 WIB.

keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi. Perlindungan data pribadi merujuk pada upaya melindungi informasi yang dapat mengidentifikasi individu tertentu dari pengumpulan, penggunaan, dan penyebaran yang tidak sah atau tidak diinginkan.

Terdapat dua metode yang dikenal untuk melindungi suatu data pribadi, pertama adalah pengamanan terhadap fisik data pribadi itu sendiri, kedua melalui regulasi yang bertujuan untuk memberi jaminan privasi terhadap pengguna data pribadi tersebut.²⁵

Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Alan Westin yang untuk pertama kalinya mendefinisikan data privasi atau “*information privacy*” sebagai hak individu, kelompok atau lembaga untuk menentukan sendiri mengenai kapan, bagaimana dan sampai sejauh mana informasi tentang mereka dikomunikasikan atau tidak kepada pihak lain.²⁶

Perlindungan data itu sendiri umumnya mengacu pada praktik, perlindungan, dan aturan mengikat yang diterapkan untuk melindungi informasi pribadi dan memastikan bahwa subjek data mempertahankan kendali atas informasi mereka. Singkatnya, pemilik data harus dapat memutuskan apakah akan membagikan informasi tertentu, siapa yang dapat mengaksesnya, berapa lama untuk membagikannya, untuk alasan apa, dan dapat memodifikasi

²⁵ Siti Yuniarti, ‘Perlindungan Hukum Data Pribadi Di Indonesia’ (2019), Vol. 1 No. 1, *Jurnal BECOSS*, Hlm. 152

²⁶ Sinta Dewi Rosadio, *Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia*, Fakultas Hukum Universitas Padjajaran, 2018, Hlm. 95.

beberapa informasi, dan lain lain.²⁷ Dalam terminologi perlindungan data pribadi, yang kerap digunakan adalah “informasi pribadi” dan “data pribadi”. Amerika Serikat menggunakan istilah informasi pribadi (*personally identifiable information*), sedangkan Eropa menggunakan istilah data pribadi (*personal data*). Dalam regulasi yang ada di Indonesia saat ini, terminologi yang digunakan adalah data pribadi.²⁸

Perlindungan data pribadi atau privasi adalah hak untuk “*right to be alone*” menurut Warren & Brandeis, sedangkan acuan produk hukum Indonesia yang melindungi tentang privasi bersumber pada Undang-Undang Teknologi Informasi yang menyatakan bahwa privasi adalah hak individu untuk mengendalikan penggunaan informasi tentang identitas pribadi baik oleh dirinya sendiri atau oleh pihak lainnya. Hak Privasi didasarkan pada prinsip umum bahwa setiap orang mempunyai hak untuk dibiarkan sendiri (*right to be alone*).²⁹

4. Asas – Asas Perlindungan Data Pribadi

Merujuk pada Undang-Undang Perlindungan Data Pribadi maka asas-asas perlindungan data pribadi adalah :

- a. Asas perlindungan, yang dimaksud asas perlindungan adalah pemerintah wajib memberikan perlindungan data pribadi warga negaranya baik didalam negeri maupun didalam negeri;

²⁷ Wahyudi Djafar, ‘Perlindungan Data Pribadi Di Indonesia: Lanskap, Urgensi, Dan Kebutuhan Pembaruan’ (2019), Vol 1 No. 1, *Jurnal Becoss*, Hlm.12.

²⁸ Siti Yuniarti, *op cit*, Hlm. 150.

²⁹ Tim Privacy Internasional dan ELSAM, *Privasi 101 Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi*, Tim ELSAM, Jakarta, 2005, Hlm. 33.

- b. Asas kepentingan umum, yang dimaksud asas kepentingan umum adalah bahwa undang-undang ini disusun untuk melindungi kepentingan masyarakat secara luas;
- c. Asas keseimbangan, yang dimaksud asas keseimbangan adalah keseimbangan antara hak privasi dengan hak negara yang sah berdasarkan kepentingan umum;
- d. Asas pertanggungjawaban, yang dimaksud asas pertanggungjawaban adalah penyelenggara data pribadi harus dapat dipertanggung jawabkan oleh penyelenggara data data pribadi.

5. Prinsip-Prinsip Perlindungan Data Pribadi Berdasarkan OECD

OECD (singkatan dalam bahasa Inggris, *Organisation for Economic Co-operation and Development*), adalah salah satu badan internasional yang berperan penting dalam mengarahkan dan mendorong kerja sama ekonomi antara negara-negara anggotanya. OECD didirikan pada tahun 1961 dan menggantikan Organisasi Kerja Sama Ekonomi Eropa (OECE) yang telah ada sejak 1948. Tujuan utama pembentukan OECD adalah untuk mempromosikan pertumbuhan ekonomi yang stabil antara negara-negara anggotanya, serta mengurangi kesenjangan ekonomi. Saat ini, OECD memiliki 38 negara anggota, yang sebagian besar merupakan negara-negara maju dan ekonomi besar di dunia.³⁰

³⁰ <https://fahum.umsu.ac.id/organisasi-untuk-kerja-sama-dan-pembangunan-ekonomi-oecd-mendorong-kemajuan-ekonomi-dan-sosial/>, diakses pada hari Kamis tanggal 30 Juli 2024, Pukul 11.12 WIB.

Secara umum, sistem perlindungan data terinspirasi oleh Pedoman OECD 1980 tentang Perlindungan Privasi dan Pengelolaan Arus Data Pribadi lintas Batas. Pedoman ini menerapkan prinsip-prinsip privasi pertama yang diakui secara internasional (OECD, 2013). Prinsip-prinsip perlindungan data pribadi yang ditetapkan oleh OECD sebagai berikut: ³¹

- a. Prinsip pembatasan pengumpulan (*collection limitation principle*), pada prinsip ini diperlukannya pembatasan dalam pengumpulan data pribadi, dan data tersebut harus diperoleh dengan cara yang sah dan adil dan dengan sepengetahuan atau persetujuan dari subjek data.
- b. Prinsip kualitas data (*quality principle*), data pribadi harus relevan dengan tujuan penggunaan, dan harus akurat, lengkap, dan mutakhir sejauh yang diperlukan untuk mencapai tujuan tersebut.
- c. Prinsip spesifikasi tujuan (*purpose specification principle*), tujuan pengumpulan data pribadi harus ditentukan selambat-lambatnya pada waktu pengumpulan data, dan penggunaan selanjutnya dibatasi pada realisasi tujuan tersebut atau tujuan lain yang tidak sesuai dan ditentukan untuk setiap perubahan tujuan.
- d. Prinsip pembatasan penggunaan (*use limitation principle*), data pribadi tidak boleh diungkapkan, disediakan atau digunakan untuk tujuan selain tujuan yang ditentukan, kecuali:
 - 1) dengan persetujuan subjek data; atau
 - 2) dilaksanakan oleh otoritas hukum.

³¹ Siti Yuniarti, *loc cit.*

- e. Prinsip perlindungan keamanan (*security safeguards principle*), data pribadi harus dilindungi dengan langkah-langkah keamanan yang wajar untuk mencegah risiko seperti kehilangan data atau akses tidak sah, perusakan, penggunaan, modifikasi, atau pengungkapan.
- f. Prinsip keterbukaan (*openness principle*), Ada kebijakan terbuka mengenai pengembangan, praktik, dan kebijakan data pribadi. Sarana tersebut harus tersedia untuk menentukan keberadaan dan sifat data pribadi, tujuan utamanya, serta identitas dan lokasi pengontrol data.
- g. Prinsip partisipasi individu (*individual participation principle*), untuk memperoleh dari pengontrol data atau mengkonfirmasi apakah pengontrol data memiliki data yang relevan;
 - 1) Berkomunikasi dengannya tentang data yang terkait dengan:
 - a) waktu yang wajar;
 - b) pengeluaran, jika ada;
 - c) alasan yang baik dan
 - d) berikan dalam bentuk yang dapat dimengerti.
 - 2) Jika permintaan yang dibuat berdasarkan (1) dan (2) ditolak, alasan diberikan dan penolakan dapat ditentang;
 - 3) Hadapi data relevan dan jika penolakan tersebut benar, hapus, perbaiki, lengkapi atau ubah data tersebut.

C. Tinjauan Teori Mengenai Peretasan Kartu Perdana Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

1. Pengertian Peretasan Kartu Perdana

Peretasan atau bisa juga disebut dengan *hacking* adalah suatu proses menganalisis, memodifikasi, menerobos masuk ke dalam komputer maupun jaringan komputer baik untuk memperoleh keuntungan maupun dimotivasi oleh tantangan.³²

Peraturan perundang-undangan di Indonesia tidak mengenal istilah *hacking*. Secara harfiah “*hacking*” berasal dari kata “*hack*” dari bahasa Inggris yang berarti mencincang atau membacok. Namun dalam kejahatan internet *hacking* diartikan sebagai penyusupan atau merusak suatu sistem komputer.³³ *Hacking* merupakan aktivitas penyusupan ke dalam sebuah sistem komputer ataupun jaringan dengan tujuan untuk menyalahgunakan ataupun merusak sistem yang ada. Definisi dari “menyalahgunakan” memiliki arti yang sangat luas, dan dapat diartikan sebagai pencurian data rahasia, serta penggunaan email yang tidak semestinya seperti *spamming* ataupun mencari celah jaringan yang memungkinkan untuk dimasuki.³⁴

Pengertian *hacking* menurut ahli bernama Sutan Reny Syahdeinn, *Hacking* adalah perbuatan membobol sistem komputer. Dia menggunakan

³² <https://www.wikipedia.org/>, diakses pada hari Rabu tanggal 01 Mei 2024, Pukul 22.45 WIB.

³³ Tubagus Heru dan Nanda Sahputra, ‘Penerapan Sanksi Sosial Sebagai Alternatif Pemidanaan Terhadap Pelaku Tindak Pidana Kejahatan Siber(Cyber Crime)’ (2022), Vol. 5 No. 2, *Al-Qisth Law Review*, Hlm 103.

³⁴ Amarudin & Sampurna Dadi, ‘Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (VPN)’ (2019), Vol. 13 No. 2, *Jurnal Teknoinfo*, Hlm. 101.

istilah "membobol" sistem komputer karena perbuatan tersebut adalah mernasukí sistem komputer orang lain tanpa izin atau otorisasi dari pemiliknya.³⁵

Meskipun UU PDP tidak menyebutkan definisi *hacking*, Undang-Undang Nomor 1 Tahun 2024 perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menjelaskan bahwa *hacking* merupakan perbuatan setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apa pun.

Pasal 65 UU PDP mengatur tentang larangan akses dan *hacking* data pribadi secara *illegal*. Pasal ini menegaskan bahwa:

- “(1) Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
- (2) Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.
- (3) Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya”.

Pasal 67 UU PDP menerapkan sanksi pidana terhadap pelaku *hacking* sebagai berikut:

- “(1) Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
- (2) Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana

³⁵ M. Ali Pamungkas, Pertanggungjawaban Pidana Pelaku Cracking Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dan Undang-Undang Nomor 19 Taun 2016 Tentang Informasi dan Transaksi Elektronik, (Skripsi Program Studi Ilmu Hukum, Fakultas Hukum Universitas Muhammadiyah Palembang), 2023, Hlm. 22.

dimaksud dalam Pasal 65 ayat (2) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

(3) Setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).”

Kartu perdana adalah kartu SIM yang digunakan pertama kali, jadi dalam keadaan benar-benar baru dan belum pernah dipasang ke slot SIM HP lalu diaktifkan sebelumnya.³⁶ Biasanya, kartu perdana sudah dilengkapi dengan nomor telepon baru, sejumlah pulsa, dan mungkin juga paket data atau layanan tambahan lainnya. Kartu ini sering kali digunakan oleh pelanggan yang baru pertama kali menggunakan layanan dari penyedia telekomunikasi tertentu atau oleh pengguna yang ingin mengganti nomor telepon. Kartu perdana biasanya dibeli dalam kondisi siap pakai, dengan penawaran promosi yang menarik dari operator, seperti tarif panggilan yang lebih murah atau kuota data yang lebih besar pada penggunaan pertama.

SimCard (Subscriber Identity Module atau *Subscriber Identification Module*) selanjutnya disebut SIM merupakan kartu yang digunakan oleh pelanggan jasa telekomunikasi untuk dapat menggunakan jasa telekomunikasi Pascabayar atau Prabayar. SIM ini bisa digunakan lebih dari sekali dan bisa dipindahkan dari satu perangkat ke perangkat lain. Dengan kata lain, SIM adalah perangkat keras yang membawa identitas pengguna di jaringan seluler SIM ini dipergunakan dengan dua metode pembayaran yaitu pertama

³⁶ <https://www.axis.co.id/blog/apa-itu-kartu-perdana-dan-bagaimana-cara-membeli-yangpraktis>, diakses pada hari kamis tanggal 01 Agustus 2024, Pukul 22.17 WIB.

membayar terlebih dahulu sebelum penggunaan dengan saldo yang sering disebut pulsa atau di sebut Prabayar, kedua penggunaan terlebih dahulu baru membayar perbulannya berdasarkan tagihan pemakaian atau disebut juga Pascabayar.³⁷ Secara teknis, kartu perdana adalah jenis khusus dari *SimCard*, tetapi istilah ini digunakan untuk menekankan status "baru" atau "pertama kali" dari kartu tersebut. Setelah kartu perdana diaktifkan dan digunakan, ia tidak lagi dianggap "perdana" dan hanya menjadi *SimCard* biasa. Selain itu, kartu perdana sering kali dijual dalam paket yang menyertakan berbagai keuntungan awal, seperti saldo pulsa atau data bonus yang tidak tersedia untuk *SimCard* yang telah digunakan sebelumnya.

Kartu perdana merupakan salah satu produk penting yang disediakan oleh *provider* telekomunikasi, berfungsi sebagai pintu gerbang utama bagi konsumen untuk mengakses berbagai layanan komunikasi dan data yang ditawarkan oleh penyedia tersebut. *Provider* telekomunikasi seperti Telkomsel, Indosat, XL Axiata, dan lainnya, bersaing dalam menawarkan kartu perdana dengan berbagai pilihan paket data, kuota internet, dan layanan tambahan seperti panggilan gratis atau layanan *streaming*. Istilah "*provider*" dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (selanjutnya disingkat PP PSTE), merujuk pada penyelenggara sistem elektronik atau penyedia layanan yang mengelola dan menyediakan berbagai layanan berbasis teknologi informasi dan

³⁷ Fadhilah Pijar Ash Shiddiq, 'Perlindungan Data Pribadi Dalam Implementasi Kebijakan Registrasi Kartu Perdana Dikaitkan Dengan Hukum Positif Indonesia', (Skripsi, Universitas Padjajaran, Bandung, 2019), Hlm. 5-6.

komunikasi. Ini mencakup berbagai jenis penyedia, seperti penyedia layanan internet, layanan *cloud*, *platform e-commerce*, dan sistem transaksi elektronik lainnya. Berdasarkan Pasal 1 ayat 4 PP PSTE menyatakan bahwa:

“Penyelenggara sistem elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/ atau keperluan pihak lain.”

Terdapat dua persyaratan yang perlu dilengkapi dalam proses registrasi yaitu:

Apabila calon pengguna merupakan warga negara Indonesia, persyaratannya antara lain:

1. Nomor *Mobile Subscriber Integrated Services Digital Network* (“MSISDN”) atau nomor pelanggan jasa telekomunikasi yang digunakan; dan
2. Data kependudukan berupa NIK dan nomor KK atau NIK dan data kependudukan biometrik, termasuk namun tidak terbatas pada teknologi wajah, sidik jari, dan iris mata.

Setelah persyaratan dipenuhi, cara daftar *SIM card* atau cara registrasi kartunya dapat dilakukan dengan:

1. Mengunjungi gerai penyelenggara jasa telekomunikasi dengan tahapan:
 - a. Registrasi dilakukan oleh petugas gerai yang ditunjuk oleh penyelenggara jasa telekomunikasi.
 - b. Petugas gerai melakukan validasi dan/atau verifikasi terhadap

identitas calon pelanggan jasa telekomunikasi prabayar.

c. Untuk proses registrasi bagi warga negara Indonesia:

- 1) Setelah menerima data dari calon pelanggan jasa telekomunikasi prabayar, penyelenggara jasa telekomunikasi melakukan validasi;
 - 2) Dalam hal data yang dimasukkan oleh calon pelanggan jasa telekomunikasi prabayar tervalidasi, proses registrasi dinyatakan berhasil; dan
 - 3) Dalam hal data yang dimasukkan tidak tervalidasi, calon pelanggan jasa telekomunikasi prabayar diminta untuk melakukan pemadanan data ke instansi pemerintah yang menyelenggarakan urusan pemerintahan di bidang kependudukan.
2. Registrasi mandiri dengan bantuan perangkat telekomunikasi dan/atau teknologi informasi, yang dilakukan melalui:
- a. layanan pesan singkat atau pusat kontak layanan penyelenggara jasa telekomunikasi yang diakses melalui nomor MSISDN, yaitu nomor yang secara unik mengidentifikasi pelanggan pada jaringan bergerak seluler, yang akan didaftarkan; atau
 - b. situs web (*website*) milik penyelenggara jasa telekomunikasi dengan menerapkan metode pembuktian kebenaran nomor MSISDN yang didaftarkan.³⁸

³⁸ <https://www.hukumonline.com/klinik/a/cara-registrasi-kartu-seluler-dan-dasar-hukumnya-lt59f7db23b755f/>, diakses pada hari Kamis tanggal 29 Agustus 2024, Pukul 20.09 WIB.

Sebagai informasi tambahan, untuk cara registrasi kartu prabayar mandiri melalui pesan singkat, Anda dapat melakukannya dengan mengirimkan pesan singkat ke 4444, dengan format-format sebagai berikut:

- NIK#Nomor KK untuk pengguna jasa telekomunikasi Indosat, Smartfren, dan Tri;
- DAFTAR#NIK#Nomor KK untuk pengguna jasa telekomunikasi XL Axiata; dan
- REG#NIK#Nomor KK untuk pengguna jasa telekomunikasi Telkomsel.

Dapat disimpulkan bahwa peretasan kartu perdana merupakan bentuk kejahatan baru yang semakin marak seiring dengan perkembangan teknologi komunikasi. Modus operasi ini biasanya melibatkan upaya untuk mengakses atau mengeksploitasi kartu SIM yang terhubung dengan nomor telepon tertentu, dengan tujuan untuk memperoleh keuntungan finansial, informasi pribadi, atau bahkan untuk melakukan tindakan kriminal lainnya. Peretasan kartu perdana dapat dilakukan dengan berbagai cara, seperti *SIM swapping*, *cloning*, atau *social engineering*, di mana pelaku dapat mengelabui penyedia layanan seluler untuk mentransfer nomor telepon ke kartu SIM baru, menggandakan kartu SIM, atau mencuri informasi yang diperlukan untuk mengakses akun korban.

2. Peretas (*Hacker*)

Hacker adalah pelaku *hacking* itu sendiri. Pengertian dari istilah “*Hacker*” secara harfiah berarti mencincang atau membacok. Dalam arti luas

adalah orang yang menyusup atau melakukan perusakan melalui komputer. *Hacker* dapat juga didefinisikan sebagai orang-orang yang mar mempelajari seluk beluk sistem komputer dan bereksperimen dengannya.³⁹

Edmon Makarim mendefinisikan *Hacker* secara umum adalah orang yang mengakses suatu sistem komputer dengan suatu cara yang tidak sah atau salah. Perbuatan ini biasanya dilakukan dengan diawali rasa keingintahuan kekaguman dan terakhir adalah adanya suatu tantangan yang ditujukan terhadap suatu sistem komputer.⁴⁰

3. Sejarah Peretasan (*hacking*)

Pertengahan abad ke-20 tepatnya tahun 1955, *hacking* pertama kali digunakan dalam bidang teknologi oleh Technical Model Railroad Club. Sebuah kelompok mahasiswa di Laboratorium Kecerdasan Artifisial di *Massachusetts Institute of Technology* (MIT). Istilah ini dipakai untuk menggambarkan bagaimana orang tersebut memodifikasi fungsi perangkat kereta berteknologi tinggi.

Menurut Jesse Sheidlower, seorang ahli IT, *hacking* dapat diartikan sebagai pemanfaatan teknologi dengan cara yang berbeda dan lebih kreatif dibandingkan dengan yang dijelaskan dalam petunjuk manual. Pada awalnya, istilah ini memiliki konotasi positif, menggambarkan keterampilan dan inovasi dalam mengutak-atik teknologi. Namun, persepsi tersebut berubah seiring dengan meningkatnya kejadian-kejadian kriminal yang memanfaatkan

³⁹ M. Ali, *loc cit.*

⁴⁰ M. Ali, *loc cit.*

keahlian teknologi secara *illegal*. Misalnya, pada tahun 1979, Kevin Mitnick, yang sering disebut sebagai salah satu *hacker* pertama, berhasil membobol sistem komputer milik *Digital Equipment Corporation (DEC)* di Amerika Serikat. Aksi ini menandai pergeseran pandangan terhadap hacking, dari sekadar keterampilan teknis yang kreatif menjadi aktivitas yang berpotensi merugikan dan melanggar hukum.

Peretasan yang dilakukan oleh Mitnick tidak hanya mengundang perhatian publik tetapi juga menyoroti risiko besar yang terkait dengan akses tidak sah ke sistem komputer, sehingga mulai muncul urgensi untuk mengatur dan mengawasi penggunaan teknologi informasi guna mencegah kejahatan siber. Sejak saat itu, berbagai insiden peretasan yang merugikan semakin memperkuat pandangan negatif terhadap hacking, menjadikannya sinonim dengan tindakan kriminal di dunia *digital*.

Mitnick yang saat itu masih berusia 16 tahun sukses meretas perangkat lunak sistem operasi RSTS/E yang sedang mereka kembangkan. Namun, ia baru diadili pada tahun 1988 dan dijatuhi hukuman satu tahun penjara.

Hacker kriminal lainnya juga muncul pada 1983. FBI berhasil menangkap kelompok The 414s yang telah membobol 60 unit komputer. Dilansir dari DiscoverMagazine.com, mereka adalah sekelompok peretas komputer dari Milwaukee yang membobol lusinan sistem komputer terkenal, termasuk yang ada di *Los Alamos National Laboratory*, *Sloan-Kettering Cancer Center*, dan *Security Pacific National Bank*. Pada *Sloan-Kettering Cancer Center*, peretasan ini menimbulkan kerugian senilai \$1.500 karena

membuat catatan tagihan terhapus.⁴¹

Setelah tertangkap dan mendapat sanksi berupa membayar ganti rugi, para pelaku menjadi sorotan dan diundang di acara TV sebagai kelompok “muda, laki-laki, cerdas, bermotivasi tinggi, dan energik”. Aksi ini pun menjadi salah satu pelopor munculnya tren hacker yang identik dengan tindak pembobolan sistem secara *ilegal*. Sejak itu pula, sebuah glosarium untuk pemrograman komputer The Jargon File mencantumkan delapan definisi terkait *hacker*, salah satunya adalah “seorang pengganggu jahat yang mencoba menemukan informasi sensitif dengan mengaduk-aduk; peretas kata sandi, peretas jaringan”. Istilah lain untuk pengertian ini adalah *cracker*. Di Indonesia sendiri, *hacker* sudah ada sejak abad 20 saat tanah air menjadi ladang subur perkembangan internet. Beberapa kelompok *hacker* di Indonesia saat itu cukup banyak, di antaranya *hackerlink*, *anti-hackerlink*, kecoa elektronik, dan echo.

Hacker di Indonesia mencapai masa keemasan pada kisaran tahun 2000, yaitu *AntiHackerlink*. Pihaknya mampu membobol puluhan situs internet kala itu baik dari dalam dan luar negeri. Uniknya, pendiri dari *Antihackerlink* ini adalah seorang anak yang belum genap berumur 17 tahun bernama Wenas Agustiawan yang biasa dikenal dengan nama hC (*hantu Crew*).

Di Indonesia, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) secara khusus mengatur larangan bagi tindakan *hacking* dalam Pasal 30 UU ITE menggarisbawahi bahwa:

⁴¹ <https://www.merdeka.com/teknologi/sejarah-asal-mula-lahirnya-hacker-mengapa-dicap-aksi-kejahatan.html>, diakses pada hari Sabtu tanggal 25 Mei 2024, Pukul 20.31 WIB.

”Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.”

Artinya pasal tersebut melindungi hak hukum terhadap properti dan privasi seseorang dengan melarang akses tanpa izin ke komputer atau sistem elektronik orang lain adalah esensi dari peraturan ini. Komputer dan sistem elektronik, yang mengandung berbagai informasi dan dokumen elektronik yang dibuat atau diperoleh oleh pemiliknya, adalah bagian dari ruang siber yang dipisahkan dan dikendalikan oleh pemiliknya. Hanya pemilik yang memiliki hak untuk mengakses dan mengelola komputer atau sistem elektronik tersebut serta berhak memberikan atau menolak izin akses kepada orang lain. Orang lain harus menghormati privasi dan hak milik pemilik, sehingga dilarang mengakses komputer atau sistem elektronik tanpa izin. Namun, Pasal 30 ayat (1) UU ITE tidak mengatur mengenai tujuan dan motif seseorang dalam mengakses komputer dan/atau sistem elektronik. Motivasi seseorang untuk melakukan peretasan bisa beragam, tidak hanya untuk keuntungan materiil seperti uang dan informasi, tetapi juga untuk keuntungan immateriil seperti status, ego, tantangan, atau hiburan. Oleh karena itu, berdasarkan ketentuan dalam Pasal 30 ayat (1) UU ITE, melakukan peretasan tanpa hak tetap merupakan perbuatan yang dilarang.⁴²

⁴² Asfarina Oktaviani & Emmilia Rusdiana, ‘Alternatif Pidana Bagi Pelaku Tindak pidana Peretasan Di Indonesia Dalam Undang-Undang Informasi dan Transaksi Elektronik’, (Program Studi Ilmu Hukum Fakultas Ilmu Sosial dan Hukum, Universitas Negeri Surabaya), Hlm. 255.

Pada dekade 2000-an, ketika layanan seluler dan penggunaan internet mulai meningkat di Indonesia, insiden peretasan kartu perdana juga mulai menjadi perhatian. Salah satu metode peretasan yang paling umum pada saat itu adalah cloning, di mana pelaku membuat salinan kartu SIM untuk mengakses jaringan telekomunikasi secara tidak sah. *Cloning* memungkinkan pelaku untuk menggunakan layanan seluler seperti panggilan telepon dan SMS tanpa terdeteksi, menciptakan risiko keamanan yang signifikan bagi penyedia layanan dan konsumen.

Memasuki dekade 2010-an, seiring dengan maraknya penggunaan ponsel pintar dan layanan online, peretasan kartu perdana menjadi lebih kompleks dan beragam. Salah satu metode yang mulai populer adalah SIM *swapping*, di mana pelaku mengelabui penyedia layanan seluler untuk mentransfer nomor telepon ke kartu SIM baru yang mereka kuasai. Dengan SIM *swapping*, pelaku dapat mengakses akun-akun yang menggunakan nomor telepon untuk otentikasi dua faktor (2FA), seperti akun *e-commerce*, perbankan, dan media sosial. Hal ini menyebabkan peningkatan risiko penipuan, pencurian identitas, dan akses tidak sah ke data pribadi.

Peretasan kartu perdana di Indonesia menjadi lebih mencolok ketika sejumlah kasus besar dilaporkan di media, menyoroti dampak serius dari peretasan ini. Kasus-kasus ini menunjukkan bagaimana pelaku dapat menggunakan akses ilegal untuk mencuri data pribadi, melakukan transaksi tanpa izin, atau bahkan membobol rekening bank. Meningkatnya insiden ini

memicu respons dari penyedia layanan seluler dan pemerintah untuk memperkuat regulasi dan keamanan dalam industri telekomunikasi.

Pada periode ini, pemerintah Indonesia memperkenalkan undang-undang dan regulasi baru untuk mengatasi peretasan kartu perdana dan memperkuat perlindungan data pribadi. UU PDP menjadi dasar hukum untuk menangani kasus-kasus peretasan dan penyalahgunaan data pribadi. Selain itu, penyedia layanan seluler mulai meningkatkan langkah-langkah keamanan, seperti memperketat proses verifikasi untuk mencegah SIM *swapping* dan meningkatkan kesadaran konsumen tentang risiko peretasan.

4. Ketentuan Hukum Peretasan Data Pribadi

Kamus Besar Bahasa Indonesia (KBBI) mendefinisikan peraturan sebagai ketentuan yang mengikat warga kelompok masyarakat dipakai sebagai panduan, tatanan dan pengendali tingkah laku yang sesuai dan dapat diterima. Setiap masyarakat harus menaati aturan yang berlaku atau ukuran, kaidah yang dipakai sebagai tolak ukur untuk menilai dan membandingkan sesuatu. Menurut Brownlee, peraturan sendiri diartikan sebagai seperangkat norma-norma yang mengandung perintah dan larangan yang didalamnya mengatur tentang bagaimana individu seharusnya berperilaku apa yang harus dilakukan dan apa yang seharusnya tidak dilakukan.⁴³

Adanya regulasi-regulasi yang menetapkan hak perlindungan data pribadi sebagai hak asasi manusia yang fundamental mencerminkan bahwa

⁴³

Ngainun Naim, *Character Building: Optimalisasi Peran Pendidikan dalam Pengembangan Ilmu & Pembentukan Karakter Bangsa*, Ar-ruzz Media, Jogjakarta, 2012, Hlm. 142-143.

negara hadir untuk melindungi setiap warganya, termasuk perlindungan terhadap jiwa, raga, dan perlindungan pada data pribadinya.⁴⁴ Hal ini mengartikan bahwa data pribadi merupakan hak yang harus dilindungi oleh negara. Pelindungan data pribadi sudah diamanatkan dalam Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD 1945) yang menyatakan bahwa :

“Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

Ketentuan mengenai peretasan sudah diamanatkan oleh konstitusi, peretasan kemudian juga diatur dalam beberapa peraturan perundang-undangan, seperti:

a. Pasal 406 KUHPidana yang menegaskan bahwa:

”Barang siapa dengan sengaja dan tanpa hak menghancurkan, merusak, membuat tidak dapat dipakai, atau menghilangkan barang yang seluruhnya atau sebagian milik orang lain, diancam dengan pidana penjara paling lama dua tahun delapan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah”.

b. Pasal 332 KUHPidana baru menyebutkan bahwa:

- (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik milik orang lain dengan cara apa pun, dipidana dengan pidana penjara paling lama 6 (enam) tahun atau pidana denda paling banyak kategori V.
- (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/ atau sistem elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/

⁴⁴

Denico Doly, ‘Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru (Establishment of a Personal Data Protection Supervisory Agency in the Perspective of the Establishment of a New State Institution)’ (2021), Vol. 12 No. 2, *Negara Hukum: Membangun Hukum untuk Keadilan dan Kesejahteraan*, Hlm. 227.

atau dokumen elektronik, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun atau pidana denda paling banyak kategori V.

- (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI.”

c. Pasal 22 UU telekomunikasi secara tegas menyebutkan bahwa:

”Setiap orang dilarang melakukan perbuatan tanpa hak, tidak sah, atau memanipulasi:

- a. akses ke jaringan telekomunikasi; dan atau
- b. akses ke jasa telekomunikasi; dan atau
- c. akses ke jaringan telekomunikasi khusus”.

d. Pasal 30 UU ITE yang berbunyi sebagai berikut:

“(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik.

(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan”.

e. Pasal 65 UU PDP menegaskan bahwa:

“(1) Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.

(2) Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.

(3) Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya”.

Perbuatan melawan hukum adalah suatu bentuk perikatan yang lahir

dari undang-undang sebagai akibat dari perbuatan manusia yang melanggar

hukum, yang diatur dalam Kitab Undang-Undang Hukum Perdata.⁴⁵ Menurut Hetty Hassanah, Perbuatan melawan hukum/ *onrechtmatigedaad*, berdasarkan Pasal 1365 KUHPerdata adalah setiap perbuatan hukum, yang melanggar, yang membawa kerugian kepada seorang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut.⁴⁶

Menurut Munir Faudy, perbuatan melawan hukum adalah sebagai suatu kumpulan dari prinsip-prinsip hukum yang bertujuan untuk mengontrol atau mengatur perilaku bahaya, untuk memberikan tanggung jawab atas suatu kerugian yang terbit dari interaksi sosial, dan untuk menyediakan ganti rugi terhadap korban dengan suatu gugatan yang tepat.⁴⁷

Pasal 1365 KUHPerdata menyatakan bahwa:

”Tiap perbuatan melanggar hukum yang membawa kerugian kepada orang lain, mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut.”

Merujuk pada Pasal 1365 KUHPerdata tersebut, seseorang dikatakan Perbuatan Melawan Hukum (PMH) apabila terpenuhi syarat-syarat atau unsur-unsur sebagai berikut :

- a. Perbuatan melawan hukum (*Onrechtmatige daad*), yaitu perbuatan yang dianggap kesusilaan undang-undang, kewajiban hukum pelaku, kesusilaan dan kepatutan yang berlaku dalam masyarakat tersebut sehingga menimbulkan kerugian.

⁴⁵ Gunawan Widjaja dan Kartini Muljadi, *Seri Hukum Perikatan-Perikatan Yang Lahir Dari Undang-Undang*, PT.Raja Grafindo Persada, Jakarta, 2017, Hlm 81.

⁴⁶ Hetty Hassanah, *Aspek hukum perdata di Indonesia*, Depublish, Yogyakarta, 2014, Hlm. 81.

⁴⁷ Munir Faudi, *Perbuatan Melawan Hukum*, PT. Citra Aditya Bakti, Bandung, 2002, Hlm. 3.

- b. Kesalahan, apabila terbukti adanya kesengajaan dalam perbuatan yang dianggap perbuatan melanggar hukum tersebut.
- c. Kerugian, meliputi kerugian secara materil maupun kerugian secara immateril.
- d. Hubungan kausal antara butir 1,2,3, maksudnya adalah hubungan sebab akibat antara perbuatan melawan hukum, kesalahan dan kerugian, sehingga kerugian yang timbul harus merupakan akibat dari perbuatan melawan hukum seseorang yang mengandung unsur kesalahan. Terdapat dua teori yang mengatur hubungan kausalitas ini yaitu teori *conditio sine qua non* dari Von Buri yang mengatakan bahwa suatu hal adalah sebab dari suatu akibat, akibat tidak akan terjadi apabila sebab itu tidak ada, teori lain adalah teori *adequate veroorzaking* dari Von Kries yang mengatakan bahwa suatu hal baru dapat dikatakan sebagai sebab dari suatu akibat apabila menurut pengalaman masyarakat dapat diduga bahwa sebab yang dimaksud dapat menimbulkan akibat tersebut.⁴⁸

⁴⁸ Wirjono Prodjodikoro, *Hukum Perdata Tentang Hak-Hak Atas Benda*, Pembimbing Masa, Jakarta, 1980, Hlm. 29.