



BAB II

TINJAUAN UMUM

A. Tinjauan Umum tentang Tindak Pidana Pencurian Identitas Melalui Platform Digital

1. Pengertian Tindak Pidana Pencurian Identitas Melalui Platform Digital

Tindak pidana merupakan terjemah dari istilah belanda *strafbaar feit*. Kata *feit* dalam bahasa belanda berarti bagian dari suatu kenyataan (*een gedeelte van de werkelijkheid*), sedangkan *strafbaar* berarti dapat dikenai hukuman. Jika diterjemahkan secara harfiah, *strafbaar feit* dapat diartikan sebagai bagian dari kenyataan yang dapat dihukum. Namun, pengertian tersebut dianggap kurang tepat karena pada dasarnya yang dapat ditajui hukuman adalah manusia sebagai pelaku, bukan peristiwa, tindakan, ataupun kenyataan sendiri.

Di Indonesia, para ahli hukum pidana juga memiliki pandangan yang berbeda mengenai pengertian *starfbaar feit*. Moeljotno menerjemahkan istilah tersebut sebagai “perbuatan pidanan”. Menurutnya, perbuatan pidana adalah suatu perbuatan yang dilarang oleh aturan hukum dan disertai ancaman saksi pidana tertentu bagi siapa saja yang melanggarnya. Dengan demikian, yang menjadi fokus larangan adalah perbuatannya, sedangkan ancaman pidana ditujukan kepada orang yang melakukan perbuatan tersebut.⁴³

⁴³ Moch Choirul Rizal, *Buku Ajar Hukum Pidana*, Lembaga Studi Hukum Pidana (LSHP), Kediri, 2021, hlm 106-112.

1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.
Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia.
Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.



Berkaitan dengan pengertian tersebut, dalam kajian hukum pidana unsur-unsur tindak pidana dibedakan menjadi dua macam, yaitu unsur subjektif dan unsur objektif. Unsur subjektif merupakan unsur yang melekat pada diri pelaku, seperti keadaan batin, niat, maupun sikap mental ketika melakukan tindak pidana. Dengan adanya unsur tersebut, dapat diketahui adanya kesalahan atau pertanggungjawaban pidana dari pelaku atas perbuatan yang dilakukannya. Sementara itu, unsur objektif yang berkaitan dengan keadaan diluar dari pelaku, seperti situasi, kondisi, atau perbuatan yang menyertai terjadinya tindak pidana. Dengan demikian, unsur objektif menitik beratkan pada tindakan keadaan yang melingkupi perbuatan pidana tersebut.

Berdasarkan uraian tersebut, unsur-unsur pokok tindak pidana (*starfbaar feit*) dapat diuraikan sebagai berikut:

- a. Adanya tindakan yang dilakukan oleh manusia.
- b. Perbuatan tersebut telah ditetapkan sebagai perbuatan yang dapat dipidana oleh undang-undang.
- c. Tindakan yang dilakukan bertentangan dengan ketentuan hukum.
- d. Dilakukan dengan adanya unsur kesalahan (sengaja atau lalai).
- e. Dilakukan oleh pelaku yang memiliki kemampuan untuk mempertanggungjawabkan perbuatannya.⁴⁴

Pasal 362 Kitab Undang-undang Hukum pidana menjelaskan bahwa pencurian adalah perbuatan mengambil suatu barang yang seluruhnya atau sebagian merupakan milik orang lain dengan maksud untuk mengusainya secara melawan hukum. Ketentuan ini menegaskan bahwa unsur utama dalam tindak pidana pencurian terletak pada adanya tindakan mengambil, objek berupa barang milik orang lain, serta adanya niat untuk memiliki barang

⁴⁴ Sudaryono & Natangsa, Hukum Pidana Dasar-dasar Hukum pidana Berdasarkan KUHP dan RUU KUHP, Muhammadiyah University Press, Surakarta, 2017, hlm 94.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

tersebut tanpa hak yang sah. Dengan demikian, perbuatan tersebut tidak hanya dipandang sebagai pelanggaran terhadap hak kepemilikan, tetapi juga sebagai bentuk perbuatan melawan hukum yang dapat dikenakan sanksi pidana.⁴⁵

Selanjutnya identitas pribadi adalah sekumpulan informasi yang melekat pada diri seseorang dan dapat dipergunakan sebagai sarana untuk mengenali, membedakan, maupun menghubungi individu tersebut, baik secara langsung maupun melalui perantara tertentu. Informasi ini mencakup berbagai bentuk data dasar seperti nama, alamat, dan nomor identitas, hingga data yang lebih sensitif seperti rekaman, biometrik, sidik jari, pemindaian wajah, serta sistem elektronik.⁴⁶ Keberadaan Identitas ini memiliki nilai yang sangat penting bagi setiap individu. Kejahatan pencurian identitas bukanlah fenomena baru yang muncul akibat perkembangan internet semata, melainkan telah lama menjadi persoalan yang kemudian menjadi kompleks seiring kemajuan teknologi informasi.

Pencurian identitas merupakan tindakan memanfaatkan data pribadi orang lain tanpa izin, seperti nomor identitas, alamat, nomor telepon, maupun informasi penting lainnya, dengan tujuan menyamar sebagai pemilik data tersebut, yang pada akhirnya dapat menimbulkan berbagai bentuk kerugian

⁴⁵ Imron Rosyadi, dkk., Victim Precipitation dalam Tindak Pidana Pencurian (Sebuah Pendekatan Viktimologi), Duta Media Publishing, Pamekasan, (2017), hlm 25.

⁴⁶ Hasan Hiawatha Rifai & Asmak UI Hosnah, (2024), Tinjauan Yuridis Terhadap Tindak Pidana Pencurian Identitas di Bawah Ketentuan KUHP, *Jurnal Pendidikan Tambusai*, Vol. 8, No. 2, hlm 17001.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

bagi korban.⁴⁷ Tindakan ini termasuk kedalam kejahatan yang dilakukan dengan cara memperoleh serta memanfaatkan data pribadi maupun informasi keuangan seseorang untuk memalsukan identitasnya demi melakukan transaksi atau aktifitas tertentu.

Praktik pencurian identitas dapat dilakukan melalui beragam cara, terutama dengan memanfaatkan teknik yang semakin maju, seperti meretas basis perusahaan dan mengambil informasi pelanggan secara ilegal. Ketika pelaku telah berhasil memperoleh data yang dibutuhkan, dampaknya dapat merugikan korban, misalnya merusak reputasi kredit atau menyalahgunakan informasi pribadi lainnya. Kejahatan ini kerap melibatkan penyamaran identitas untuk mengakses sistem komputer atau jaringan yang bahkan dapat terjadi dalam lingkup global.⁴⁸ Seiring dengan perkembangan teknologi pencurian identitas diruang digital memiliki pola yang semakin khas. Kejahatan ini dilakukan untuk memanfaatkan teknologi untuk menyamar, mengakses sistem, dan mengeksploitasi kelemahan perlindungan data, sehingga berdampak pada kerugian finansial, pelanggaran privasi, gangguan keamanan, serta menurunkannya kepercayaan dalam lingkungan digital.

Berdasarkan uraian tersebut, dapat diidentifikasi beberapa karakteristik pencurian identitas dalam ruang digital sebagai berikut :

- Dilakukan dengan cara menyamar melalui representasi digital, seperti avatar, suara tiruan, atau manipulasi visual korban.
- Memanfaatkan kelemahan sistem keamanan untuk mengambil alih kredensial akun atau mengakses basis data secara ilegal.
- Mengeksploitasi celah perlindungan data pada platform digital.

⁴⁷ Rifqi Mahmud, (2019), Pencurian Identitas kategori & Kasus, *Cybersecurity dan Forensik Digital*, Vol. 2, No. 1, hlm 39.

⁴⁸ Hasan Hiawatha Rifai & Asmak UI Hosnah, *Op. Cit.*, hlm 17001.



- d. Menggunakan teknik siber seperti *Phishing*, malware, serangan otomatis berbasis bot, dan manipulasi data transaksi.
- e. Bertujuan menguasai akun, data pribadi, aset, virtual, serta merusak reputasi digital korban.
- f. Terjadi dalam ruang lintas batas negara sehingga menyulitkan proses pelacakan dan penegakan hukum.
- g. Menimbulkan dampak yang hanya bersifat finansial, tetapi juga menyentuh aspek privasi, keamanan, dan kepercayaan pengguna dalam ekosistem digital.⁴⁹

Pencurian identitas di lingkungan digital memiliki sejumlah karakteristik yang menggambarkan perkembangan kejahatan siber modern. Pelaku biasanya memanfaatkan kelemahan pada sistem elektronik maupun celah keamanan teknologi untuk memperoleh akses terhadap data pribadi tanpa persetujuan pemiliknya. Tindak pidana ini bersifat *asset-less*, karena pelaku tidak harus berada ditempat yang sama atau berinteraksi langsung dengan korban. Proses pengambilan data dapat dilakukan dengan sangat cepat dan menjangkau banyak korban secara bersamaan dalam skala yang luas. Identitas yang berhasil diperoleh sering disalah gunakan untuk berbagai tindakan ilegal, seperti penipuan, pengajuan kredit atau pinjaman daring, serta pembuatan rekening atas nama pihak lain. Karakteristik tersebut menunjukkan bahwa pencurian identitas diruang digital memiliki tingkat kompleksitas yang lebih tinggi dibanding dengan pencurian identitas yang dilakukan secara konvensional.

2. Dasar Hukum Perlindungan Data Pribadi

Sebagai negara hukum, hukum ditempatkan sebagai otoritas tertinggi sehingga dikenal adanya prinsip supremasi hukum. Prinsip tersebut

⁴⁹ Zul Khaidir Kadir, (2025), Kejahatan Berbasis Digital: Menggagas Kebijakan Kriminal Untuk Dunia Metaverse, *Julia Jurnal Litigasi Amsir*, Vol. 12, No. 2, hlm. 126-130.



menghendaki agar pelaksanaan tetap memperhatikan tiga nilai pokok, yakni keadilan, kemanfaatan, dan kepastian hukum. Ketika suatu negara menganut asas negara hukum maka penyelenggaraan pemerintahannya harus bertumpuh pada konstitusi atau Undang-undang Dasar sebagai landasan utama dalam menjalankan kekuasaan.

Terkait dengan perlindungan data pribadi di Indonesia, pengaturannya secara umum telah tercantum dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kemudian mengalami perubahan melalui Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE, serta semakin dipertegas dengan hadirnya Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.⁵⁰ Pengaturan-pengaturan tersebut tampak jelas melalui ketentuan larangan penggunaan data pribadi secara elektronik sebagaimana diatur dalam pasal 1 ayat (1) undang-undang tersebut, yang secara tegas merumuskan perbuatan-perbuatan yang dilarang terkait penguasaan dan pemanfaatan data pribadi.

Adapun bunyi pasal 1 ayat (1) adalah sebagai berikut:

Pasal 1 Ayat (1)

Data pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan non elektronik.⁵¹

⁵⁰ Muhammad Khorul Umam, Perlindungan Hukum Data Pribadi di Indonesia Perspektif Hak Asasi Manusia dan Hukum Pidana Islam, *Skripsi*, Fakultas Syariah dan Hukum Universitas Islam Negeri Walisongo Semarang, 2022, hlm 29-30.

⁵¹ Pasal 1 Ayat (1) Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.



Pasal 5

Subjek data pribadi berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan ukum tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi.⁵²

Pasal 7

Subjek data pribadi berhak mendapatkan akses dan memperoleh salinan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.⁵³

Pasal 11

Subjek data Pribadi berhak menunda atau membatasi pemrosesan data pribadi secara proposional sesuai dengan tujuan pemrosesan data pribadi.⁵⁴

Pasal 12 Ayat (1)

Subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.

Ayat (2)

Ketentuan lebih lanjut mengenai pelanggaran pemrosesan data pribadi dan tata cara pengenaan ganti rugi sebagaimana dimaksud pada ayat (1) diatur dalam peraturan perundang-undangan.⁵⁵

Pasal 65 Ayat (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.

Ayat (2)

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

Ayat (3)

Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya.⁵⁶

⁵² Pasal 5 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

⁵³ Pasal 7 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

⁵⁴ Pasal 11 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

⁵⁵ Pasal 12 Ayat (1) dan (2) Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

⁵⁶ Pasal 65 Ayat (1), (2), dan (3) Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.



Ketentuan larangan tersebut kemudian diikuti dengan pengaturan mengenai ancaman pidana yang diatur dalam pasal 67 sebagaimana bentuk penegasan konsekuensi hukum terhadap pelanggaran norma tersebut.

Adapun bunyi pasal 67 adalah sebagai berikut:

Pasal 67 Ayat (1)

Setiap orang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana 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 tahun dan/atau pidana denda paling banyak Rp 5.000.000.000,00 (lima miliar rupiah).

Ayat (2)

Setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya sebagaimana 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).

Ayat (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).⁵⁷

Dalam konteks perlindungan data pribadi di Indonesia, keberadaan Undang-undang Perlindungan Data Pribadi merupakan langkah penting dalam memperkuat jaminan hukum bagi masyarakat. Meskipun demikian, penerapannya masih menghadapi berbagai tantangan. Tantangan tersebut antara lain lembaga yang mengawasi dan menyelenggarakan perlindungan data pribadi yang masih dalam tahap pembentukan, rendahnya tingkat kesadaran masyarakat mengenai pentingnya menjaga dan melindungi data

⁵⁷ Undang-undang Nomor 27 tahun 2022 Tentang Perlindungan Data Diri Pasal 67 ayat (1), (2), (3).



pribadi, serta semakin kompleksnya kejahatan siber yang dapat melintasi batas wilayah negara. Selain itu, pengaturan yang secara khusus mengakomodasi perlindungan data pribadi bagi anak-anak dan penyandang disabilitas masih memerlukan penyempurnaan.

Di sisi lain, kapasitas dan kemampuan aparat penegak hukum juga perlu terus ditingkatkan agar penanganan kasus penyalahgunaan maupun pencurian data pribadi dapat dilakukan secara lebih efektif. Walaupun masih terdapat berbagai hambatan, hadirnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memberikan kepastian hukum yang lebih jelas dan menjadi fondasi penting dalam upaya melindungi hak privasi sebagai bagian dari hak konstitusional setiap warga negara.

3. Bentuk Tindak Pidana Pencurian Identitas Melalui Platform Digital

Sebagai bentuk pencurian di era digital, *Phishing* merupakan teknik penipuan siber yang bertujuan memperoleh data sensitif milik korban dengan cara mengecoh atau memanipulasi korban agar menyerahkan informasi penting, seperti kata sandi, data kartu kredit, atau tanpa sadar mengunduh program berbahaya ke perangkatnya. Istilah *Phishing* sendiri merupakan plesetan dari kata *fishing* (memancing), yang menggambarkan cara pelaku “memancing” informasi berharga di ruang daring. Praktik ini menimbulkan kerugian ganda, karena korban tidak hanya kehilangan data pribadinya, tetapi juga berpotensi mengalami kerugian finansial akibat penyalahgunaan

1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.



informasi tersebut oleh pelaku untuk melakukan tindakan kejahatan lanjutan di lingkungan digital.⁵⁸

Phishing ini bertujuan untuk mengelabui korban agar memberikan informasi pribadinya, peretasan akun media sosial maupun surat elektronik, penyebaran perangkat lunak berbahaya yang mampu mencuri data pengguna, penyalahgunaan data hasil kebocoran sistem, serta pembuatan akun palsu dan menggunakan identitas orang lain tanpa izin. Pesatnya perkembangan teknologi informasi meningkatkan penggunaan layanan digital dalam kehidupan sehari-hari menyebabkan tindak pidana ini semakin mudah dilakukan dan sulit untuk dideteksi.⁵⁹ Selain *Phishing*, pemalsuan identitas juga merupakan salah satu bentuk pencurian di era digital yang sering digunakan untuk memperoleh keuntungan dengan cara melawan hukum.

Pemalsuan identitas merupakan salah satu bentuk kejahatan yang dapat menimbulkan kerugian nyata bagi pihak lain, karena dalam praktiknya pelaku dengan sengaja mengubah, merekayasa, atau menciptakan data identitas sedemikian rupa sehingga tampak seolah-olah benar dan sah menurut kenyataan, padahal sesungguhnya informasi tersebut tidak sesuai dengan fakta yang sebenarnya, sehingga kondisi ini dapat menyesatkan, mengecoh, dan menimbulkan kepercayaan keliru dari orang yang melihat atau menggunakannya. Istilah “palsu” sendiri mengandung makna sesuatu yang tidak asli, sedangkan “pemalsuan” merujuk pada proses atau tindakan menghasilkan sesuatu yang tidak autentik tersebut, sehingga dari setiap

⁵⁸ Devie Rahmawati, dkk., *Waspada Kejahatan Phishing Attack*, PT. Literasi Nusantara abdi Grup, Malang, 2022, hlm 25.

⁵⁹ *Ibid.*



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.

2. Penggunaan tanpa izin untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

3. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

peristiwa pemalsuan selalu terdapat unsur pelaku yang melakukan tindakan, objek yang dipalsukan, serta tujuan yang hendak dicapai dari perbuatan tersebut.

Menurut pendapat Adami Chawazi, kejahatan pemalsuan adalah suatu tindak pidana yang di dalamnya terkandung unsur ketidakbenaran terhadap suatu objek, di mana objek tersebut dari tampilan luar terlihat seolah-olah benar dan sesuai dengan kenyataan, namun pada hakikatnya bertentangan dengan kondisi yang sebenarnya, sehingga dapat menimbulkan kekeliruan pemahaman bagi orang yang mempercayainya.⁶⁰

Seiring dengan perkembangan teknologi informasi, bentuk kejahatan tersebut turut berkembang keranah digital, salah satunya melalui pencurian data pribadi yang termasuk sebagai pencurian di era digital karena dilakukan dengan mengambil dan menyalahgunakan informasi pribadi seseorang secara melawan hukum melalui media elektronik dan internet. Pencurian data pribadi merupakan suatu tindakan melawan hukum yang dilakukan dengan cara memperoleh, mengakses, mengambil, menyebarluaskan, ataupun menggunakan informasi pribadi seseorang tanpa hak dan tanpa persetujuan dari pemilik data tersebut.

Data pribadi menjadi sasaran dapat berupa nama lengkap, alamat, nomor identitas, informasi rekening bank, kata sandi akun, sehingga biometrik yang bersifat rahasia. Dalam perkembangan teknologi digital saat ini, tindak pencurian data pribadi semakin sering terjadi karena hampir seluruh aktivitas

⁶⁰ Eko Nanang Nurdyansah, *Penyelesaian Tindak Pidana Pemalsuan Identitas dalam Pinjaman Online (Studi Kasus di Kecamatan Jambi Timur)*, *Skripsi*, Fakultas hukum Universitas Batanghari, 2022, hlm 12-13.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.

2. Penggunaan tanpa izin untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan

masyarakat telah terhubung dala, sistem elektronik dan internet. Kondisi tersebut memberikan peluang yang lebih besar bagi pelaku kejahatan siber untuk memanfaatkan kelemahan sistem keamanan maupun kelalaian pengguna dalam menjaga kerahasiaan datanya.⁶¹

pencurian identitas digital dikategorikan sebagai perbuatan yang melanggar hukum dan dapat dikenakan sanksi pidana berdasarkan peraturan perundang-undangan yang mengatur perlindungan data pribadi, informasi dan transaksi elektronik, serta kejahatan siber. Perbuatan pidana berupa memperoleh, mengakses, menggunakan, atau menyebarkan data pribadi tanpa hak merupakan tindakan yang dilakukan oleh seseorang dengan cara mengambil atau mendapatkan data pribadi milik orang lain tanpa persetujuan atau dasar hukum yang sah suatu tindakan dilakukan terhadap data pribadi seseorang tanpa adanya izin dari pemilik data atau tanpa adanya kewenangan yang diberikan oleh peraturan perundang-undangan.⁶²

Dalam konteks perlindungan data pribadi, setiap individu memiliki hak untuk menentukan siapa yang dapat mengakses, menggunakan, atau mengelola data pribadinya. Oleh karena itu, apabila seseorang memperoleh atau memanfaatkan data pribadi orang lain tanpa mendapatkan persetujuan terlebih dahulu dari pemilik data, maka tindakan tersebut dapat dianggap sebagai pelanggaran hukum. Selain persetujuan, penggunaan data pribadi juga dapat dibenarkan apabila terdapat dasar hukum yang sah, misalnya untuk kepentingan penegakan hukum, pelaksanaan kewajiban hukum, pelayanan

⁶¹ Andreas Bintang Raja, (2025), Pencurian Data Pribadi: Perspektif Hukum di Indonesia, Inggris, dan singapura, *Jurnal Pendidikan Tambusai*, Vol. 9, No. 2, hlm 13719.

⁶² *Ibid.*



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

publik, atau keadaan lain yang secara tegas diatur dalam peraturan perundang-undangan. Dengan demikian, penggunaan data pribadi yang tidak didasarkan pada persetujuan pemilik data maupun ketentuan hukum yang berlaku merupakan tindakan yang tidak sah dan berpotensi menimbulkan pertanggungjawaban hukum bagi pelakunya.

Tindakan ini tidak hanya melanggar hak privasi individu, tetapi juga berpotensi menimbulkan kerugian materiil dan immateriil, seperti penipuan, pencemaran nama baik, kehilangan akses terhadap akun digital, serta penyalahgunaan identitas dalam berbagai transaksi elektronik. Oleh karena itu, perbuatan memperoleh, mengakses, menggunakan, atau menyebarkan data pribadi tanpa hak dikategorikan sebagai perbuatan yang melawan hukum dan dapat dikenakan sanksi sesuai dengan ketentuan peraturan perundang-undangan yang berlaku.

B. Tinjauan Umum tentang Perlindungan Data Pribadi

1. Pengertian Perlindungan data Pribadi

Perlindungan data pribadi merupakan suatu upaya yang dilakukan untuk menjaga keamanan sekaligus kerahasiaan informasi yang berkaitan dengan identitas seseorang agar tidak disalahgunakan oleh pihak yang tidak memiliki kewenangan.⁶³ Data pribadi memiliki peranan yang sangat penting dalam kehidupan manusia karena di dalamnya terdapat berbagai informasi yang mampu menggambarkan identitas, kondisi, hingga aktivitas seseorang. Informasi tersebut dapat berupa nama, alamat, nomor telepon, data keuangan,

⁶³ Kurniawan Tri Wibowo, dkk., *Hukum Digital dan Privasi Data*, CV. Al-Haramain Lombok, Mataram, 2022, hlm 15.



data kesehatan, hingga riwayat transaksi yang apabila jatuh ke tangan yang salah dapat menimbulkan kerugian yang besar, baik secara materiil maupun immateriil.

Dalam ketentuan Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi dijelaskan bahwa data pribadi adalah setiap data mengenai orang perseorangan yang teridentifikasi atau dapat diidentifikasi, baik secara langsung maupun tidak langsung, melalui sistem elektronik maupun non elektronik. Ketentuan ini menunjukkan bahwa perlindungan data pribadi tidak hanya terbatas pada informasi yang tersimpan dalam perangkat digital, tetapi juga mencakup dokumen fisik, arsip, serta catatan manual yang memuat identitas seseorang. Dengan demikian, Ruang lingkup perlindungan data pribadi memiliki cakupan yang sangat luas karena mencakup seluruh kegiatan yang berkaitan dengan pengumpulan, penyimpanan, pengolahan, penggunaan, pengungkapan, hingga pemusnahan informasi yang dapat mengidentifikasi seseorang.⁶⁴

Perlindungan tersebut tidak hanya berlaku terhadap data yang disimpan dalam bentuk fisik, tetapi juga terhadap data yang tersimpan dan diproses melalui sistem elektronik. Luasnya cakupan perlindungan data pribadi bertujuan untuk menjamin hak privasi setiap individu serta mencegah terjadinya penyalahgunaan data oleh pihak yang tidak berwenang, terutama di era digital yang ditandai dengan meningkatnya aktivitas pengumpulan dan pertukaran informasi secara elektronik.

⁶⁴ *Ibid.*



Perlindungan data pribadi tidak semata-mata berkaitan dengan upaya pengamanan dari ancaman data tersebut diperoleh, dikelola, diproses, disimpan, hingga dibagikan oleh pihak yang mengumpulkannya. Setiap lembaga, instansi, atau organisasi yang mengelola data pribadi memiliki tanggung jawab hukum dan moral untuk memastikan bahwa data tersebut diperlakukan dengan benar, tidak disalahgunakan, serta hanya digunakan sesuai dengan tujuan awal pengumpulannya.⁶⁵ Tanggung jawab ini sejalan dengan konsep perlindungan data pribadi.

Dalam perspektif hukum, perlindungan data pribadi memiliki dua dimensi utama, yaitu perlindungan terhadap privasi sebagai bagian dari hak asasi manusia serta perlindungan terhadap data pribadi sebagai aset yang rentan disalahgunakan oleh pihak yang tidak berwenang. Hak atas privasi telah memperoleh pengakuan konstitusional melalui pasal 28G ayat (1) Undang-undang Dasar Negara Republik Indonesia Tahun 1945 yang menjamin setiap orang atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada dalam penguasaannya. Berdasarkan ketentuan tersebut, negara berkewajiban, memastikan bahwa setiap aktivitas yang berkaitan dengan pengumpulan, penyimpanan, pemrosesan, hingga penyebaran, keadilan, dan keterbukaan. Meskipun demikian, perkembangan teknologi yang berlangsung sangat cepat sering kali melampaui kemampuan hukum untuk beradaptasi.

⁶⁵ *Op. Cit.*, hlm 17.

1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.
Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia.
Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.



Transformasi digital yang terjadi secara luas telah melahirkan berbagai ruang dan aktivitas baru yang belum sepenuhnya diakomodasi oleh peraturan perundang-undangan yang berlaku. Banyak perusahaan teknologi digital mengelola dan menyimpan data pengguna Indonesia pada server yang berlokasi di luar negeri, sehingga menimbulkan persoalan yurisdiksi dalam proses penegakan hukum. Selain itu, hadirnya teknologi mutakhir seperti big data, kecerdasan buatan (*Artificial Intelligence/AI*), dan *Internet of Things* (IoT) semakin memperumit upaya pemberian perlindungan yang efektif terhadap data pribadi masyarakat. Oleh karena itu, perlindungan data pribadi tidak hanya mengandalkan instrumen hukum semata, melainkan membutuhkan pendekatan yang bersifat multidisipliner.⁶⁶

Selain pembentukan regulasi yang memadai, diperlukan peningkatan kesadaran masyarakat melalui edukasi, penguatan kapasitas lembaga yang berwenang, serta kerja sama yang erat antara pemerintah, sektor swasta, dan masyarakat sipil. Disisi lain, peraturan yang terlalu restriktif juga perlu dihindari karena berpotensi menghambat inovasi dan perkembangan ekonomi digital yang saat ini menjadi salah satu fokus pembangunan nasional. Pada praktiknya, kepatuhan terhadap prinsip-prinsip perlindungan data pribadi masih menjadi tantangan, baik dilingkungan instansi pemerintah maupun sektor swasta. Terdapat kasus dimana data pribadi digunakan oleh lembaga tertentu untuk kepentingan kampanye maupun tujuan komersial

⁶⁶ Predderics Hockop Simanjuntak, (2024), *Perlindungan Hukum Terhadap Data Pribadi pada era Digital di Indonesia: Studi Undang-undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR)*, *Jurnal Esensi Hukum Magister Hukum Universitas Pembangunan Nasional Veteran Jakarta*, Vol. 6, No. 2, hlm 107.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

tanpa memperoleh persetujuan yang sah dari pemilik data, pada dasarnya merupakan bentuk pelanggaran terhadap norma hukum dan etika. Selain itu, tidak sedikit perusahaan teknologi yang menerapkan syarat dan ketentuan penggunaan layanan dalam bentuk kontrak yang panjang dan sulit dipahami oleh pengguna, tanpa menyediakan pilihan yang transparan dan seimbang bagi mereka dalam memberikan persetujuan atas penggunaan data pribadinya.⁶⁷

2. Ruang Lingkup Data Pribadi Umum dan Spesifik

Undang-Undang Perlindungan Data Pribadi mengatur pengelompokan data pribadi dengan berdasarkan pada tingkat sensitivitas serta potensi resiko yang dapat timbul apabila data tersebut disalahgunakan atau diakses tanpa hak. Dalam pengaturannya data pribadi tidak dipandang sebagai satu kesatuan yang seragam, melainkan diklasifikasikan ke dalam dua kategori besar agar perlindungan hukum yang diberikan dapat disesuaikan dengan karakteristik dan tingkat kerahasiaan dari masing-masing jenis data yang bersifat spesifik, yaitu data yang memiliki tingkat kerentanan tinggi dan berpotensi menimbulkan dampak serius bagi pemiliknya, serta data yang bersifat umum, yaitu data yang lazim digunakan untuk mengenali identitas seseorang dalam kehidupan sehari-hari namun tetap memerlukan perlindungan agar tidak disalahgunakan. Adapun rincian dari pembagian kedua jenis data pribadi tersebut dijabarkan sebagai berikut:

⁶⁷ Ibid., hlm 108.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.

2. Penggunaan tanpa izin untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

3. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan

peraturan yang berlaku di Indonesia.

a. Data pribadi yang bersifat spesifik (sensitif) terdiri atas (Pasal 4 Ayat (2) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi).⁶⁸

- 1) Data dan informasi yang berkaitan dengan kondisi kesehatan seseorang.
- 2) Data biometrik yang menunjukkan ciri fisik atau biologis khas individu, seperti sidik jari atau pemindaian wajah.
- 3) Informasi genetik yang berkaitan dengan susunan gen atau DNA seseorang.
- 4) Catatan atau riwayat keterlibatan dalam tindak pidana.
- 5) Data yang berhubungan dengan anak di bawah umur.
- 6) Keterangan pribadi yang bersifat sangat rahasia.
- 7) Data lain yang penentapannya diatur lebih lanjut dalam peraturan perundang-undangan.

b. Data pribadi yang bersifat umum terdiri atas (Pasal 4 Ayat (3) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi).⁶⁹

- 1) Nama lengkap individu.
- 2) Jenis kelamin.
- 3) Kewarganegaraan.
- 4) Agama yang dianut.
- 5) Status perkawinan.
- 6) Data pribadi lain yang apabila digabungkan dapat mengarah pada proses identifikasi seseorang.⁷⁰

Kasus-kasus seperti pelanggaran data oleh perusahaan besar, kebocoran

informasi sensitif, dan akses legal ke data pengguna telah menimbulkan kekhawatiran serius bagi masyarakat dan regulator. Ketika data pribadi jatuh ke tangan yang salah, dampaknya bisa sangat merusak karena pelaku kejahatan dapat menggunakan data ini untuk melakukan tindakan kriminal

⁶⁸ Pasal 4 Ayat (2) Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

⁶⁹ Pasal 4 Ayat (3) Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

⁷⁰ Riantika Pratiwi, dkk., (2024), Tinjauan Yuridis Perlindungan Data Pribadi dalam Transaksi E-Commerce, *Pagaruyuang Law Journal*, Vol. 7, No. 2, hlm 374-375.



seperti pencurian identitas, penipuan finansial, dan bahkan manipulasi opini publik.⁷¹

3. Prinsip-prinsip Perlindungan Data Pribadi

Perlindungan hukum merupakan upaya yang diberikan oleh negara kepada setiap subjek hukum melalui peraturan perundang-undangan yang berlaku guna menjamin terpenuhinya hak-hak mereka. Dalam praktiknya, perlindungan hukum terdiri adad dua bentuk, yaitu perlindungan preventif yang bertujuan mencegah terjadinya pelanggaran, dan perlindungan represif yang diberikan setelah terjadinya pelanggaran melalui penegakan hukum dan pemberian saksi. Perkembangan teknologi informasi dan komunikasi telah meningkatkan kebutuhan akan perlindungan data pribadi. Aktivitas masyarakat yang semakin bergantung pada layanan digital, seperti penggunaan media sosial, transaksi elektronik, dan berbagai aplikasi berbasis internet, menyebabkan data pribadi menjadi salah satu aset yang sangat bernilai sekaligus rentan terhadap penyalahgunaan. Oleh karen itu, negara memiliki kewajiban untuk membentuk regulasi yang mampu menjamin keamanan serta perlindungan data pribadi setiap warga negara.

Dalam perspektif hak asasi manusia, perlindungan data pribadi tidak hanya berkaitan dengan aspek keamanan informasi, tetapi juga menyangkut perlindungan hak privasi individu. Jaminan tersebut mencerminkan dalam pasal 28G ayat (1) dan pasal 28H ayat (4) UUD 1945 yang memberikan perlindungan terhadap diri pribadi, kehormatan, martabat, serta harta benda

⁷¹ Fara Anindita & Andi Aina Ilmih, (2024), Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber, *Aladalah: Jurnal Politik, Sosial, Hukum dan Humaniora*, Vol. 2, No.4, hlm 177.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

setiap warga negara. Dengan demikian, setiap orang berhak menentukan dan mengendalikan penggunaan data pribadinya oleh pihak lain. Urgensi perlindungan data pribadi semakin terlihat dari berbagai kasus kebocoran data yang terjadi di Indonesia. Kebocoran data pada sektor perbankan, kesehatan, perusahaan swasta, maupun instansi pemerintah menunjukkan bahwa keamanan sistem informasi masih menghadapi berbagai tantangan. Peristiwa-peristiwa tersebut berpotensi menimbulkan kerugian berupa pencurian identitas, penipuan, penyalahgunaan informasi pribadi, hingga ancaman terhadap keamanan nasional.⁷²

Data pribadi tidak boleh digunakan diolah, maupun disebarluaskan tanpa adanya persetujuan dari pemilik data. Prinsip ini menempatkan hak privasi individu sebagai aspek utama yang harus dihormati dalam setiap kegiatan pengumpulan dan pengelolaan data pribadi. Dalam konteks di Indonesia, prinsip tersebut dapat dijadikan landasan dalam penyelenggaraan perlindungan data pribadi dengan menekankan pengawasan yang mengumpulkan, menyimpan, serta memproses data masyarakat. Melalui mekanisme tersebut, risiko kebocoran data maupun penyalahgunaan informasi pribadi oleh pihak yang tidak berwenang dapat diminimalkan. Dengan demikian, penggunaan data pribadi hanya dapat dilakukan apabila pemilik data telah memberikan persetujuan yang sah sesuai dengan tujuan pengumpulan data tersebut.

⁷² Wibowo, *op. Cit.*, hlm 19-20.



Beberapa prinsip perlindungan privasi yang diterapkan dalam pengelolaan data pribadi meliputi:

a. Prinsip perlindungan privasi secara proaktif

Prinsip ini menekankan pentingnya tindakan pencegahan sebelum terjadi pelanggaran terhadap data pribadi, pemerintahan, penyelenggaraan sistem elektronik, dan masyarakat harus berperan aktif dalam mengantisipasi kemungkinan terjadinya kebocoran maupun penyalahgunaan data melalui penerapan sistem pengamanan yang memadai dan pengawasan yang berkelanjutan.

b. Prinsip prioritas terhadap kerahasiaan data

Perlindungan privasi harus ditempatkan sebagai prioritas utama dalam setiap proses pengolahan data pribadi. Oleh karena itu, sistem yang digunakan wajib menjamin bahwa kerahasiaan data terlindungi secara otomatis dan bahwa setiap informasi pribadi hanya dapat diakses oleh pihak yang memiliki kewenangan.⁷³

c. Prinsip integrasi perlindungan privasi dalam sistem

Perlindungan privasi harus menjadi bagian yang melekat dalam keseluruhan sistem pengelolaan data. Dengan mengintegrasikan aspek perlindungan data kedalam seluruh proses dan infrastruktur teknologi, pengawasan terhadap penggunaan data pribadi dapat dilakukan secara lebih efektif dan menyeluruh.

⁷³ *Ibid.*



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.

2. Penggunaan tanpa izin untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

d. Prinsip fungsionalitas dan pengurangan resiko

Prinsip ini menghendaki adanya standar dan mekanisme yang mampu meminimalkan berbagai resiko yang muncul dalam penyelenggaraan sistem elektronik. Perlindungan data tidak hanya ditujukan untuk menjaga keamanan organisasi atau perusahaan, tetapi juga untuk memastikan hak privasi pengguna tetap terlindungi.⁷⁴

e. Prinsip keamanan menyeluruh

Keamanan data pribadi harus dijamin pada setiap tahapan pengelolaan data, mulai dari pengumpulan, penyimpanan, penggunaan, hingga pemusnahan data. Dengan demikian, perlindungan terhadap data pribadi dapat berlangsung secara berkesinambungan selama siklus hidup data tersebut.

f. Prinsip transparansi

Pengelolaan data pribadi harus dilakukan secara terbuka dan dapat dipertanggungjawabkan. Pemilik data berhak mengetahui bagaimana data mereka dikumpulkan, digunakan, disimpan, dan diproses oleh penyelenggara sistem elektronik. Keterbukaan informasi ini penting untuk membangun kepercayaan serta memastikan kepatuhan terhadap peraturan yang berlaku.

g. Prinsip kehormatan terhadap hak pemilik data

⁷⁴ Alfred Yetno, (2021), Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna dalam Upaya Mewujudkan Tujuan Hukum di Indonesia, *Satya Darma: Jurnal Ilmu Hukum*, Vol. 4, No. 1.



Prinsip ini menegaskan bahwa pemilik data harus diberikan hak untuk mengendalikan informasi pribadinya. Masyarakat sebagai subjek data berhak mengakses, mengawasi, serta menentukan penggunaan data pribadinya sehingga tercipta perlindungan yang lebih efektif terhadap hak privasi individu.

Berdasarkan prinsip tersebut, perlindungan data pribadi tidak hanya berfokus pada aspek keamanan teknologi, tetapi juga pada penghormatan terhadap hak-hak individu atas informasi pribadinya. Oleh karena itu, penyelenggara sistem elektronik, pemerintah, dan masyarakat perlu bekerja sama untuk mewujudkan tata kelola data yang aman, transparan, dan bertanggung jawab.⁷⁵

C. Tinjauan Umum Tentang Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

1. Hak subjek data pribadi

Dalam Undang-undang Perlindungan Data Pribadi (PDP), data pribadi dibedakan menjadi dua kategori, yaitu data pribadi umum dan data pribadi yang bersifat spesifik. Data yang termasuk spesifik, seperti data biometrik, kesehatan, dan data genetika, memperoleh tingkat perlindungan hukum yang lebih tinggi karena memiliki tingkat sensitivitas yang lebih besar. Klasifikasi tersebut berperan penting dalam menentukan standar perlindungan yang harus diterapkan serta tanggung jawab yang wajib dipenuhi oleh pihak pengendali data. Pengaturan ini juga selaras dengan praktik perlindungan data yang

⁷⁵ *Ibid*, diakses pada, file:///C:/Users/Hype%20GLK/Downloads/761-Article%20Text-2471-1-10-20211229%20(4).pdf



berlaku secara internasional, sehingga dapat memberikan jaminan keamanan yang lebih efektif terhadap data pribadi.

Undang-undang PDP memberikan berbagai hak kepada pemilik data pribadi, antara lain hak untuk memperoleh akses terhadap data, hak untuk memperbaiki data yang tidak akurat, hak untuk meminta penghapusan data, serta hak untuk membatasi kegiatan pemrosesan data. Pemberian hak-hak tersebut menunjukkan adanya perubahan pendekatan dari perlindungan yang bersifat pasif menjadi perlindungan yang menempatkan individu sebagai pihak yang memiliki kendala atas data pribadinya. Dengan demikian, negara mengakui pentingnya kedaulatan individu terhadap informasi pribadi dalam lingkungan digital. Prinsip transparansi dan akuntabilitas juga menjadi dasar utama dalam pengelolaan data pribadi sesuai dengan ketentuan yang berlaku.⁷⁶

Pengaturan mengenai hak-hak subjek data pribadi tersebut secara lebih rinci diatur dalam Bab IV Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Didalam pasal 8 subjek data diberikan hak untuk memperoleh informasi mengenai kejelasan identitas, dasar kepentingan hukum, tujuan tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta data tersebut. Selanjutnya, pasal 9 mengatur hak subjek data untuk melengkapi, memperbaharui, dan/atau memperbaiki kesalahan maupun ketidakakuratan data pribadinya. Dan pasal 10 ayat (1) memberikan hak subjek data pribadi untuk memperoleh akses dan mendapatkan salinan data pribadi yang diproses sesuai dengan ketentuan

⁷⁶ Asep Mahbub Junaedi, (2025), Urgensi Perlindungan Data Pribadi dalam Era Digital: Analisis Undang-undang Nomor 27 Tahun 2022, *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, Vol. 5, No. 2, hlm 249.



peraturan perundang-undangan.⁷⁷ Pasal 10 memberikan hak kepada subjek data untuk menyampaikan keberatan terhadap putusan yang dihasilkan melalui proses pemrosesan data secara otomatis, termasuk kegiatan pemrofilan, apabila keputusan tersebut menimbulkan konsekuensi hukum atau memberikan dampak yang cukup besar terhadap dirinya.

Penggunaan pemrofilan dan sistem pengambilan keputusan otomatis dianggap memiliki sejumlah resiko yang perlu diperhatikan. Salah satu resiko utama adalah kurangnya transparansi dalam proses pembentukan profil, sehingga individu sering kali tidak mengetahui bagaimana data pribadinya dikumpulkan, dianalisis, dan digunakan. Selain itu, terdapat kemungkinan bahwa subjek data tidak diberikan persetujuan atau tidak menghendaki informasi pribadinya dimanfaatkan untuk keperluan pemrofilan. Permasalahan lainnya adalah keterbatasan pemahaman subjek data mengenai mekanisme kerja teknologi tersebut serta dampak yang ditimbulkannya. Kondisi ini dapat menyebabkan individu tidak menyadari bagaimana hasil pemrosesan data mempengaruhi keputusan yang berkaitan dengan dirinya. Lebih jauh lagi, keputusan yang dihasilkan secara otomatis berpotensi menimbulkan kerugian atau konsekuensi negatif yang signifikan bagi pihak tertentu.

Hal lain yang perlu diperhatikan adalah bahwa hasil analisis data yang menunjukkan adanya hubungan atau korelasi antar variabel tidak selalu dapat dijadikan dasar yang akurat untuk menarik kesimpulan. Korelasi yang ditemukan belum tentu memiliki makna yang relevan atau menverminkan

⁷⁷ *Ibid*, hlm 250.



kondisi yang sebenarnya. Oleh karena itu karena pemprofilan pada dasarnya hanya menghasilkan prediksi atau asumsi mengenai perilaku dan karakteristik seseorang, selalu terdapat kemungkinan terjadinya kesalahan. Dengan demikian, diperlukan kehati-hatian serta mekanisme pengendali yang memadai agar resiko yang muncul dari penggunaan hasil pemprofilan dapat diminimalkan dan hak-hak subjek data tetap terlindungi.⁷⁸ Sementara itu, Pasal 11 mengatur hak subjek data untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi mengenai dirinya sesuai dengan ketentuan yang berlaku.

Hak-hak tersebut perlu didukung oleh mekanisme perlindungan yang jelas agar dapat dilakukan secara efektif. Oleh karena itu, dalam pelaksanaannya Undang-undang PDP mengatur tanggung jawab yang jelas bagi pengendali data maupun prosesor data pribadi. Pengendali data memiliki kewenangan untuk menentukan tujuan serta metode pemrosesan data, sedangkan prosesor data bertugas menjalankan pemrosesan sesuai arahan yang diberikan oleh pengendali. Pengaturan ini bertujuan untuk memastikan bahwa setiap pihak memiliki kewajiban hukum yang tegas dan tidak dapat melepaskan tanggung jawabnya kepada pihak lain secara sepihak. Selain itu, ketentuan tersebut mendorong penetapan tata kelola data yang lebih profesional, terstruktur, dan sesuai dengan standar perlindungan data yang diakui secara global.⁷⁹

2. Perlindungan terhadap hak subjek data pribadi

⁷⁸ Heru Tjatur, dkk., *Perlindungan Data Pribadi Dalam Jurnalisme dan Media*, Asosiasi Media Siber Indonesia (AMSI), Jakarta Selatan, 2024, hlm 26.

⁷⁹ Junaedi, *op.cit*, hlm 251.



Dalam kerangka hukum perlindungan data pribadi, subjek data menempati posisi yang sangat penting karena menurupkan pihak yang memiliki hak dan kewenangan atas diri pribadinya. Pengakuan terhadap kedudukan subjek data tersebut bertujuan untuk memastikan bahwa setiap individu tetap memiliki kontrol terhadap pengumpulan, penyimpanan, pengungkapan, maupun penghapusan data pribadinya oleh pihak lain. Pengelolaan data pribadi tidak dapat dilakukan secara sewenang-wenang tanpa memperhatikan hak-hak yang melekat pada pemilik data. Hak subjek data merupakan perwujudan dari prinsip-prinsip dasar perlindungan data pribadi yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Prinsip-prinsip tersebut menekankan bahwa pemrosesan data pribadi harus dilakukan secara sah, transparan, dan bertanggung jawab. Selain itu, subjek data juga diberikan hak untuk memperoleh informasi yang jelas mengenai penggunaan data pribadinya, melakukan perbaikan apabila terdapat kesalahan atau ketidakakuratan data, serta meminta pembatasan terhadap pemrosesan data dalam kondisi tertentu. Pemberian hak-hak tersebut bertujuan untuk menciptakan keseimbangan antara kepentingan pengendali data dalam mengelola informasi dan hak individu untuk melindungi privasinya.⁸⁰

Pengaturan mengenai hak subjek data diatur secara khusus dalam Bab IV Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

⁸⁰ *Ibid.*

1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.



Ketentuan tersebut memberikan jaminan hukum bagi setiap individu agar dapat mengetahui, mengawasi, dan mengendalikan penggunaan data pribadinya. Secara keseluruhan, Bab IV Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memuat sepuluh jenis hak yang tersebar dalam pasal 5 hingga pasal 15. Berbagai hak tersebut mencakup hak untuk memperoleh informasi tentang kejelasan identitas pihak yang memproses data, hak untuk mengakses dan memperoleh salinan data pribadi, hak untuk melengkapi, memperbarui, dan memperbaiki data, hak untuk mengakhiri pemrosesan data, serta hak untuk menghapus atau memusnahkan data pribadi sesuai dengan ketentuan peraturan perundang-undangan.⁸¹

Menurut teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon, perlindungan hukum merupakan upaya untuk menjamin penghormatan terhadap harkat dan martabat manusia serta pengakuan atas hak-hak yang dimiliki oleh setiap subjek hukum. Perlindungan tersebut diberikan berdasarkan ketentuan hukum yang berlaku sebagai instrumen yang sah untuk menjaga kepentingan hukum seseorang dari berbagai bentuk ancaman maupun pelanggaran. Dalam teorinya, Philipus M. Hadjon membedakan perlindungan hukum menjadi dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif.

a. Perlindungan Hukum Preventif

Perlindungan hukum preventif merupakan langkah-langkah yang dilakukan untuk mencegah terjadinya pelanggaran hukum sebelum

⁸¹ Khalda Alivia Azzahra, (2025), Perlindungan Hak Subjek Data Pribadi dalam Kebijakan Penggunaan Ulang Nomor Telepon Seluler Ditinjau Menurut Hukum Positif Indonesia, *Jurnal Hukum, Politik dan Ilmu Sosial (JHPIS)*, Vol. 4, No. 2, hlm 141.

1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.
Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.
2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.
3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.

2. Penggunaan tanpa izin untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

3. Universitas hanya dilarang dan dapat dikenakan sanksi. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

peraturan yang berlaku di Indonesia.

muncul sengketa. Tujuan utama perlindungan preventif adalah meminimalkan resiko terjadinya kerugian melalui penaturan, pengawasa, dan tindakan penvegahan yang efektif. Dalam konteks perlindungan data pribadi, bentuk perlindungan preventif yang seharusnya diterapkan meliputi:

1) Penerapan Sistem Keamanan Data yang Andal dan Bertanggung Jawab

Berdasarkan pasal 39 ayat (2) Undang-undang Perlindungan Data Pribadi, pengendali data pribadi melalui sistem keamanan yang aman, andal, dan dapat dipertanggungjawabkan. Implementasi kewajiban tersebut dapat dilakukan melalui berbagai langkah teknis, seperti penggunaan teknologi enkripsi, firewall, sistem deteksi dan pencegahan intrusi, serta pembaruan sistem secara berkala. Langkah-langkah tersebut bertujuan untuk mengurangi resiko kebocoran maupun penyalahgunaan data pribadi.⁸²

2) Pembentukan Peraturan Pemerintah sebagai Aturan Pelaksana Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Undang-undang Perlindungan Data Pribadi masih memerlukan sejumlah peraturan pelaksana yang dituangkan dalam bentuk peraturan pemerintah. Keberadaan aturan pelaksana tersebut sangat penting untuk memberikan penjelasan yang lebih rinci mengenai

⁸² Nabiha Khansa Rusyda, (2025), Perlindungan Hukum Terhadap Subjek Data Kebocoran Data oleh Badan Publik Menurut UU Nomor 27 Tahun 2022, *Desentralisasi: Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, Vol. 2, No. 3, hlm 258



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang.

Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

mekanisme penerapan ketentuan yang terdapat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Mengingat sifat Undang-undang yang umumnya mengatur hal-hal secara umum, diperlukan pedoman teknis yang dapat dijadikan acuan oleh para pemangku kepentingan dalam melaksanakan kewajiban dan hak yang diatur dalam undang-undang.

3) Pembentukan Lembaga Perlindungan Data Pribadi

Dalam ketentuan Bab IX Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi mengenai kelembagaan, diatur pentingnya pembentukan lembaga yang bertugas melakukan pengawasan terhadap penyelenggaraan perlindungan data pribadi serta mendukung penegakan hukum atas pelanggaran yang terjadi. Lembaga tersebut memiliki berbagai kewenangan yang berkaitan dengan penyusunan kebijakan dan strategi perlindungan data pribadi.⁸³

b. Perlindungan Hukum Represif

Perlindungan hukum represif merupakan bentuk perlindungan yang diberikan setelah terjadinya pelanggaran hukum dengan tujuan menyelesaikan sengketa serta memulihkan hak pihak yang dirugikan. Dalam konteks pelanggaran perlindungan data pribadi, perlindungan represif dapat diwujudkan melalui beberapa langkah, salah satunya sebagai berikut:

⁸³ *Ibid*, hlm 259.



1) Keterbukaan Informasi atas Kejadian Kebocoran Data

Apabila terjadi insiden kebocoran atau kegagalan perlindungan data pribadi, badan publik maupun pengendali data wajib memberikan informasi secara terbuka kepada pihak yang berdampak. Kewajiban tersebut diatur dalam pasal 46 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengharuskan pengendali data pribadi menyampaikan pemberitahuan tertulis kepada subjek data pribadi dan lembaga yang berwenang paling lambat dalam waktu 3 kali 24 jam sejak diketahui terjadinya kegagalan perlindungan data.⁸⁴

3. Ketentuan Pidana terhadap Pelanggaran terhadap Hak Subjek Data Pribadi

Ketentuan pidana terhadap pelanggaran hak subjek data pribadi merupakan salah satu bentuk perlindungan hukum yang diberikan oleh negara untuk menjamin keamanan dan kerahasiaan data pribadi setiap individu. Dalam hukum pidana, pertanggung jawaban pidana pada dasarnya mengandung makna bahwa setiap orang yang melakukan perbuatan yang dilarang oleh undang-undang harus mempertanggung jawabkan tindakannya sesuai dengan tingkat kesalahan yang dilakukan. Seseorang dapat dikenakan sanksi pidana apabila terbukti melakukan suatu perbuatan yang bertentangan dengan hukum dan memenuhi unsur-unsur tindak pidana yang telah ditetapkan. Dengan demikian, pelaku pelanggaran tidak hanya bertanggung

⁸⁴ *Ibid*, hlm 260



1. Dilarang memperbanyak atau mendistribusikan dokumen ini untuk tujuan komersial tanpa izin tertulis dari penulis atau pihak berwenang. Penggunaan untuk kepentingan akademik, penelitian, dan pendidikan diperbolehkan dengan mencantumkan sumber.

2. Penggunaan tanpa izin untuk kepentingan komersial atau pelanggaran hak cipta dapat dikenakan sanksi sesuai dengan UU Hak Cipta di Indonesia. Plagiarisme juga dilarang dan dapat dikenakan sanksi.

3. Universitas hanya berhak menyimpan dan mendistribusikan dokumen ini di repositori akademik, tanpa mengalihkan hak cipta penulis, sesuai dengan peraturan yang berlaku di Indonesia.

jawab secara moral, tetapi juga secara hukum atas akibat yang ditimbulkan oleh perbuatannya.

Penggunaan data pribadi milik orang lain secara melawan hukum untuk kepentingan tertentu tanpa persetujuan yang sah dari subjek data juga merupakan perbuatan yang dapat dipidana. Terhadap pelanggaran tersebut, pelaku dapat dikenakan pidana paling lama lima tahun dan/atau denda paling banyak Rp5 miliar. Sementara itu, bagi pihak yang dengan sengaja membuat atau memalsukan data pribadi dengan tujuan memperoleh keuntungan bagi dirinya sendiri maupun pihak lain sehingga menimbulkan kerugian bagi orang lain, dapat dikenakan pidana penjara paling lama 6 tahun dan/atau pidana denda paling banyak Rp6 miliar. Selain pidana pokok, pelaku juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan atau harta kekayaan yang diperoleh dari hasil tindak pidana serta kewajiban membayar ganti kerugian kepada pihak yang dirugikan. Pengaturan mengenai saksi tersebut menunjukkan keseriusan negara dalam memberikan perlindungan hak-hak subjek data pribadi dan mencegah terjadinya penyalahgunaan data yang dapat merugikan masyarakat, dalam pelaksanaannya sendiri.⁸⁵

Penegakan sanksi merupakan salah satu instrumen penting dalam menjamin terlaksananya perlindungan data pribadi secara efektif. Setiap pengendali data pribadi yang terbukti tidak memenuhi kewajibannya dalam menjaga keamanan, kerahasiaan, dan integritas data pribadi milik subjek data harus dimintai pertanggungjawaban sesuai dengan ketentuan yang di atur

⁸⁵ Shafa Salsabila, dkk., (2025), Pertanggungjawaban Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-undang Perlindungan Data Pribadi Indonesia, *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Komunikasi*, Vol. 2, No. 2, hlm 150-152.



dalam Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Kegagalan dalam menerapkan langkah-langkah perlindungan yang memadai, baik yang disebabkan oleh kelalaian maupun kesengajaan, dapat menimbulkan kerugian bagi subjek data pribadi dan berpotensi mengancam hak-hak privasi yang dijamin oleh hukum. Oleh karena itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah mengatur mekanisme penegakan hukum melalui pemberian saksi administratif sebagaimana tercantum dalam Bab VII serta sanksi pidana yang diatur dalam Bab XIV.⁸⁶

Pengenaan sanksi tersebut bertujuan tidak hanya untuk memberikan efek jera kepada pelaku pelanggaran, tetapi juga untuk mendorong terciptanya tata kelola data pribadi yang bertanggung jawab dan sesuai dengan prinsip-prinsip perlindungan data. Selain itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga memberikan perlindungan yang lebih kuat melalui pengaturan ketentuan pidana terhadap berbagai bentuk pelanggaran yang mengakibatkan terlanggarnya hak-hak subjek data pribadi. Ketentuan pidana tersebut ditujukan kepada setiap orang yang dengan sengaja dan tanpa hak memperoleh, mengakses, mengungkapkan, menggunakan, memindahtangankan, atau memalsukan data pribadi milik orang lain sehingga menimbulkan kerugian bagi subejk data yang bersangkutan. Pengaturan mengenai saksi pidana ini menunjukkan bahwa hak data pribadi merupakan bagian dari hak privasi yang dapat perlindungan hukum yang serius.

⁸⁶ Rusyda, *op.cit*, hlm 260



Pengaturan mengenai sanksi pidana, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga mengatur penerapan sanksi administratif sebagai instrumen penegakan hukum terhadap pelanggaran dalam pengelolaan data pribadi. Bentuk sanksi yang dapat dikenakan meliputi teguran tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi yang diperoleh atau diproses secara tidak sah, serta pengenaan denda administratif. Untuk memastikan efektifitas pelaksanaan ketentuan tersebut, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi juga mengatur adanya lembaga yang memiliki kewenangan dalam melakukan pengawasan terhadap penyelenggaraan perlindungan data pribadi. Lembaga ini bertugas mengawasi pelaksanaan ketentuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, menerima dan menindaklanjuti pengaduan masyarakat, menyelesaikan sengketa yang berkaitan dengan pelanggaran data pribadi, serta memastikan bahwa seluruh pihak yang mengumpulkan, menyimpan, menggunakan, dan memproses data pribadi telah mematuhi standar perlindungan data yang diterapkan oleh peraturan perundang-undangan.⁸⁷

⁸⁷ Winda Agustina, dkk., (2025), Upaya Perlindungan Hak Pivasi Terhadap Data Pribadi dan Kejahatan Peretasan, *Media Hukum Indonesia (MHI)*, Vol. 2, No. 6, hlm 121.