



# Perlindungan Hukum Bagi Pengguna Jasa Internet Terhadap Kerahasiaan Data Pribadi

Fredrik Anakotta<sup>1</sup>, Nancy Silvana Haliwela<sup>2</sup>, Marselo Valentino Geovani Pariela<sup>3</sup>

<sup>1,2,3</sup> Fakultas Hukum Universitas Pattimura, Ambon, Indonesia.

 : erickottasah@gmail.com

Corresponding Author\*



## Abstract

**Introduction:** In the current era of globalization, the internet plays a very important role in human life. In addition to playing an important role, there are also adverse impacts that harm internet service users such as personal data leaks. The confidentiality of personal data was leaked in 2022, including indihome customer data, as many as 26 million customer data were traded on BreachForms by Bjorka. The data is in the form of keyword search history, user info such as email, name, to Population Identification Number.

**Purposes of the Research:** A form of legal protection for the public regarding the security of personal data and consumer rights that are not fulfilled.

**Methods of the Research:** The research method used is normative juridical, namely by examining various laws and regulations and other literature related to the research.

**Results Originality of the Research:** The results of this study show that the form of legal protection for internet service users against the confidentiality of personal data consists of three forms, namely the form of supervision of personal data, the existence of the principle of personal data security protection, where internet service providers are obliged to maintain the security of internet service user data, the existence of personal data security from unauthorized parties, for which the Government, Internet Service Providers, Law enforcement officials are obliged to supervise and secure all forms of internet networks, for example by deleting or locking personal data if it has been used by the user, as well as strengthening legal arrangements related to the misuse of personal data confidentiality. Quickly handle various cases of abuse of the confidentiality of personal data of internet network users so that it has a deterrent effect.

**Keywords:** Legal Protection; Personal Data; Internet Users.

## Abstrak

**Latar Belakang:** Era globalisasi saat ini, internet sangat berperan penting dalam kehidupan manusia. Selain berperan penting, terdapat juga dampak buruk yang merugikan pengguna jasa internet seperti adanya kebocoran data pribadi. Kerahasiaan data pribadi bocor pada tahun 2022, diantaranya yaitu data pelanggan indihome, sebanyak 26 juta data pelanggan diperjualbelikan di BreachForms oleh Bjorka. Data tersebut berupa histori pencarian keyword, user info seperti email, nama, hingga Nomor Induk Kependudukan.

**Tujuan Penelitian:** Bentuk perlindungan hukum bagi Masyarakat mengenai keamanan data pribadi dan hak-hak konsumen yang tidak terpenuhi.

**Metode Penelitian:** Metode penelitian yang digunakan yaitu yuridis normatif, yaitu dengan menelaah berbagai peraturan perundang-undangan serta literatur lain yang berkaitan dengan penelitian.

**Hasil Penelitian:** Hasil dari penelitian ini menunjukkan bahwa bentuk perlindungan hukum bagi pengguna jasa internet terhadap kerahasiaan data pribadi terdiri atas tiga bentuk yaitu bentuk pengawasan terhadap data pribadi, adanya prinsip perlindungan keamanan data pribadi, dimana penyedia jasa internet berkewajiban untuk menjaga keamanan data pengguna jasa internet, Adanya Pengamanan data pribadi dari pihak yang tidak berhak, untuk itu Pemerintah, Penyedia Jasa Internet, Aparat Penegak Hukum wajib mengawasi dan mengamankan segala bentuk jaringan internet, misalnya dengan penghapusan atau penguncian data pribadi jika telah selesai digunakan oleh pengguna tersebut, serta Mempertegas pengaturan hukum terkait penyalagunaan

kerahasiaan data pribadi. Secara cepat menangani berbagai kasus penyalagunaan terhadap kerahasiaan data pribadi pengguna jaringan internet sehingga menimbulkan efek jera.

**Kata Kunci: Perlindungan Hukum; Data Pribadi; Pengguna Internet.**

*Dikirim: 2024-10-25*

*Direvisi: 2024-12-26*

*Dipublikasi: 2024-12-31*

## 1. PENDAHULUAN

Perkembangan modern di Indonesia saat ini telah berkembang pesat, kehidupan sosial dan budaya masyarakat saling berhubungan dan hampir tidak terdapat batas antara ruang dan waktu. Perkembangan teknologi informasi utamanya *interconnection-networking* (internet), membawa pengaruh besar di kehidupan manusia. Informasi telah melahirkan suatu etika baru bahwa setiap pihak yang mempunyai informasi memiliki naluri yang senantiasa mendistribusikan kepada pihak lain. Perkembangan ekonomi modern saat ini, informasi, termasuk data pribadi, sangatlah berharga karena memiliki nilai ekonomi yang tinggi sehingga banyak digunakan oleh perusahaan. Keadaan ini dikenal dengan istilah digital dossier, yaitu pengumpulan informasi tentang seseorang dalam jumlah yang banyak dengan menggunakan teknologi digital yang diawali sejak awal tahun 1970 dengan menggunakan komputer hingga sekarang dengan menggunakan internet.

Salah satu perkembangan teknologi informasi adalah revolusi di bidang teknologi komputer yang dapat menyimpan data dalam jumlah yang besar yang dinamakan *cloud computing* atau komputasi awan, yang merupakan gabungan pemanfaatan teknologi komputer ('komputasi') dan pengembangan berbasis internet (awan), *Cloud computing* adalah teknologi yang menggunakan internet dan server pusat yang jauh untuk menjaga atau mengelola data pelanggan. *Cloud computing* membantu konsumen dan pebisnis untuk menggunakan aplikasi tanpa melakukan instalasi, mengakses file pribadi mereka di manapun dengan menggunakan akses internet. Teknologi ini memungkinkan efisiensi dengan memusatkan penyimpanan, pemrosesan dan memori data.

Jaringan internet yang mudah diakses dan dijangkau oleh setiap masyarakat membuat ketersediaan informasi, baik lokal maupun global hingga budaya masyarakat yang tidak memandang batas usia mudah didapatkan. Akses internet yang sangat mudah didapatkan dijadikan sebagai kesempatan baru di masa depan, menggeser pandangan atau tradisi yang ada. David Held mengemukakan bahwa, teknologi dan informasi terdapat beberapa unsur diantaranya keluasan (*extencity*), kekuatan (*intencity*), kecepatan (*velocity*), dan dampak (*impact*) luar biasa yang tidak terbayangkan sebelumnya. Hal-hal tersebut yang kemudian menghasilkan kesempatan namun juga ancaman dalam proses memajukan kualitas kehidupan manusia melalui pemanfaatan jaringan internet.<sup>1</sup>

Pengguna jasa internet sangatlah luas bukan hanya sebatas jual beli online, bahkan pengguna jasa internet melalui sosialmedia pun sangatlah banyak. Hal tersebut berdampak positif bagi masyarakat karena memudahkan masyarakat atau pengguna bertemu secara online dalam jaringan internet untuk melakukan transaksi maupun hubungan tanpa harus

---

<sup>1</sup> Fayakhun Andriadi, "Pemanfaatan Akses Internet Dalam Mendukung Kemajuan Bangsa," [www.kompasiana.com](https://www.kompasiana.com/fayakhun/55002c84a33311e57250ff78/pemanfaatan-akses-internet-dalam-mendukung-kemajuan-bangsa?page=3&page_images=1), 2010, [https://www.kompasiana.com/fayakhun/55002c84a33311e57250ff78/pemanfaatan-akses-internet-dalam-mendukung-kemajuan-bangsa?page=3&page\\_images=1](https://www.kompasiana.com/fayakhun/55002c84a33311e57250ff78/pemanfaatan-akses-internet-dalam-mendukung-kemajuan-bangsa?page=3&page_images=1).

bertemu secara langsung. Namun dibalik dampak positif tersebut, terdapat pula dampak negatifnya yaitu bocornya kerahasiaan data pribadi, hal ini dikarenakan berbagai sosial media dan aplikasi pada jaringan internet memerlukan data pribadi pengguna untuk menghubungkan pengguna yang satu dan pengguna lainnya, yang mengharuskan adanya pemberian data pribadi pada jaringan internet agar memudahkan pengenalan terhadap individu tersebut yang ingin melakukan transaksi pada jaringan internet. Demikian di era perkembangan internet yang sangat pesat ini diperlukan adanya perlindungan hukum bagi pengguna jasa internet terhadap kerahasiaan data pribadi sesuai dengan prinsip negara Indonesia sebagai negara hukum sebagaimana terkandung dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (selanjutnya disebut UUD) Pasal 1 Ayat (3) yang menyatakan bahwa negara Indonesia adalah negara hukum.

Penjelasan terkait data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi (selanjutnya disebut UU Data Pribadi), dalam Pasal 1 Ayat 1, mengatur bahwa: "Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik". Selanjutnya dalam Pasal 1 Ayat 2 mengatur bahwa: "Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi". Penggunaan jaringan internet sebagaimana di atur dalam Pasal 4 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE), sangat mempunyai banyak manfaat dalam berbagai bidang kehidupan, yaitu<sup>2</sup>: a) untuk sarana konektivitas dan komunikasi; b) akses informasi, pengetahuan, dan edukasi; c) alamat dan pemetaan; d) kemudahan bisnis; e) serta hiburan. Dilihat dari berbagai manfaat yang diberikan jaringan internet diatas namun juga mempunyai dampak negatif terhadap penggunanya, salah satunya yaitu hilangnya kerahasiaan data pribadi pengguna jasa internet. Peningkatan penggunaan jaringan internet serta ketergantungan masyarakat terhadap penggunaan jaringan internet karena memudahkan masyarakat dalam melakukan berbagai hubungan melalui jaringan internet misalnya penggunaan jasa internet dalam hal jual beli online.

Perkembangan teknologi informasi saat ini telah memungkinkan untuk mengumpulkan, menyimpan, berbagi dan menganalisis data. Konsep perlindungan data pribadi menjelaskan bahwa setiap orang mempunyai hak untuk memutuskan apakah mereka ingin bergabung dengan masyarakat dan berbagi/menukar data pribadi. Undang-Undang Perlindungan Data juga mencakup langkah-langkah perlindungan untuk memastikan keamanan data pribadi dan ketentuan penggunaan data pribadi.<sup>3</sup>

Menurut Pasal 4 UU Pelindungan Data Pribadi, menjelaskan bahwa data individu itu sendiri terbagi menjadi dua jenis. Pertama, data pribadi secara umum seperti nama lengkap,

---

<sup>2</sup> Ashya Ravika Mahar Rhani, "5 Manfaat Internet," [www.kompas.com](https://www.kompas.com), 2020, <https://www.kompas.com/skola/read/2020/10/08/224859069/5-manfaat-internet?page=all#:~:text=KOMPAS.com - Manfaat internet adalah.>

<sup>3</sup> Sinta Dewi Rosadi, "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia," *Yustisia* 5, no. 1 (2016): 22-30, <https://doi.org/10.20961/yustisia.v5i1.8712>.

jenis kelamin, kebangsaan, agama, dan/atau data pribadi disertai tanda pengenal. Kedua, informasi pribadi yang spesifik, termasuk informasi dan data kesehatan, informasi biometrik, informasi genetik, kehidupan/orientasi seks, opini politik, informasi catatan kriminal, informasi tentang anak, informasi keuangan pribadi dan informasi lain yang diwajibkan oleh hukum dengan ketentuan peraturan perundang-undangan. Berdasarkan data dari CNN Indonesia, terdapat setidaknya 10 (sepuluh) kerahasiaan data pribadi pengguna jaringan internet bocor pada tahun 2022. Diantaranya yaitu data pelanggan *indihome* dimana, sebanyak 26 juta data pelanggan bocor dan diperjual belikan di *BreachForms* oleh Bjorka.

Data-data tersebut berupa histori pencarian keyword, user info mencakup email, nama, jenis kelamin, hingga NIK. Hingga Data pengguna jasa internet My Pertamina dan Peduli Lindungi pun bocor dan dijual pada situs gelap.<sup>4</sup> Walaupun data tersebut diretas dan tidak berhasil mendapatkan data yang berkaitan dengan transaksi keuangan pengguna jasa internet tersebut, tetapi hacker/peretas tersebut mengetahui kerahasiaan data pribadi pengguna jasa internet tersebut yang dapat digunakan untuk berbagai penipuan online. Berkaitan hal tersebut, terdapat beberapa contoh kasus dalam penyalahgunaan data pribadi, diantaranya yaitu: 1) Pinjaman online, Dimana mekanisme transaksinya mengisi data secara online akan tetapi dalam hal keterlambatan pembayaran tidak jarang menggunakan kolektor untuk melakukan intimidasi kepada nasabah, keluarga nasabah, pimpinan tempat nasabah bekerja dan bahkan dapat mengakses data dari handphone nasabah; 2) Transportasi online, Dimana konsumen mengalami pelecehan seksual melalui nomor whatsapp. Berdasarkan peristiwa tersebut dapat dikatakan bahwa terdapat metadata berupa data pribadi yang diberikan untuk berbagai kepentingan (perbankan, *e-commerce*, dll), diserahkan secara sukarela dan disimpan sebagai data digital oleh pelaku usaha (atau siapapun yang menerima dan menyimpan data pribadi, metadata rentan untuk disalahgunakan penerima penyimpan data atau dicuri (*hack*) pihak ketiga dan terbuka untuk disalahgunakan, digunakan untuk tujuan-tujuan lain di luar kesepakatan.

Berdasarkan kasus-kasus diatas, maka diperlukan adanya UU ITE Pasal 26 Ayat 1, yang mengatur bahwa: "Penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan," dengan demikian diperlukan regulasi yang jelas terkait keamanan data dan kerahasiaan data pribadi pengguna jasa internet yang terjamin akan keamanan data pribadi tersebut. Undang-Undang terhadap perlindungan mengenai kerahasiaan data pribadi pengguna jasa internet sangat ditunggu oleh masyarakat pengguna jasa internet sebagai bentuk dari perlindungan pemerintah terhadap keamanan data dan kerahasiaan data pribadi warga Negara pengguna jasa internet khususnya untuk menangani kekhawatiran pengguna terkait dengan adanya kebocoran data pribadi pengguna jasa internet ataupun adanya penyalahgunaan data pribadi pengguna jasa internet oleh pihak yang tidak bertanggung jawab, yang dimana dampaknya sangat terasa dan sangat merugikan pengguna jasa internet yang disebabkan oleh lemahnya penegakan hukum khususnya yang berkaitan dengan ITE.<sup>5</sup> Secara universal, instrument

---

<sup>4</sup> CNN Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah," [www.cnnindonesia.com](https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2), 2022, <https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2>.

<sup>5</sup> Sandryones Palinggi and Erich C. Limbongan, "Pengaruh Internet Terhadap Industri ECommerce Dan Regulasi Perlindungan Data

hukum internasional, Deklarasi Universal Hak Asasi Manusia (*Universal Declaration of Human Rights*) telah memberikan landasan hukum bagi negara-negara anggota Perserikatan Bangsa-Bangsa (PBB) dalam melaksanakan kewajibannya untuk melindungi dan menghormati hak privasi setiap warga negaranya.<sup>6</sup>

Secara eksplisit ketentuan perlindungan terhadap data pribadi ini tertuang dalam Pasal 3 dan Pasal 17 Deklarasi Universal Hak Asasi Manusia (DUHAM). Dinyatakan dalam Pasal 3 DUHAM: “*Everyone has the right to life, liberty and security of person* “. Pasal ini memberikan perlindungan terhadap jiwa, kebebasan dan keamanan seseorang, dalam arti lain, setiap orang harus dijamin atas keselamatan atas pribadinya tanpa terkecuali. Selanjutnya, diperjelas oleh Pasal 17 DUHAM melalui Ayat (1) dan Ayat (2) bahwa: “*Everyone has the right to own property alone as well as in association with others; (2) No one shall be arbitrarily deprived of his property.*” Pasal 17 Ayat (1) dan Ayat (2) DUHAM ini menekankan bahwa setiap orang memiliki hak informasi terkait dirinya untuk tetap dijaga dan tidak diketahui oleh umum, tidak hanya secara individu, tetapi juga secara kolektif yaitu ketika berada dalam masyarakat. Pasal 17 Ayat (2) DUHAM ini menegaskan dan menekankan bahwa tidak seorang pun secara sewenang-wenang dapat kehilangan atau dirampas hak atas privasi. Oleh karena itu, hak privasi dapat dihapus diri seseorang melalui kepastian hukum. Pasal 17 Ayat (1) DUHAM diterjemahkan secara bebas sebagai berikut: “Tidak boleh seorang pun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat-menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya.” Kemudian Ayat (2) Pasal 17 DUHAM diartikan secara bebas menjadi: “Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan seperti tersebut di atas”.

Indonesia sebagai negara hukum memiliki tanggung jawab untuk mengubah aturan internasional tersebut menjadi aturan positif yang berlaku dan berdampak positif bagi warga negaranya. Sebab, hukum diciptakan dengan tujuan untuk kesejahteraan Masyarakat, dalam dunia usaha, promosi dan peluang peningkatan kesejahteraan masyarakat dilaksanakan secara cepat tanpa batasan lokasi atau regional dan menjangkau seluruh lapisan masyarakat baik nasional maupun internasional. Namun perkembangan teknologi dan informasi tidak hanya bermanfaat, tetapi juga menimbulkan permasalahan yang merugikan masyarakat, seperti penyalahgunaan data, pencurian informasi pribadi, penjualan informasi pribadi, penipuan, dan lain-lain.

Data-data tersebut seperti email, Nomor HP bahkan KTP yang dalamnya berisikan data pribadi (Nama, NIK, Alamat). Pelaku usaha atau penyelenggara sistem elektronik dapat mengumpulkan data pribadi dari pelanggan atau calon pelanggan secara *offline* atau *online*, yang dalam hal ini data digital tersebut dapat diperjualbelikan tanpa sepengetahuan dan izin pemiliknya atau disalahgunakan, dengan adanya penyalahgunaan data pribadi, maka dapat terlihat adanya kelemahan sistem, kurangnya pengawasan, sehingga data pribadi dapat disalahgunakan dan mengakibatkan kerugian bagi pemilik data tersebut. Penyalahgunaan,

---

Pribadi Pelanggan Di Indonesia,” in *Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi)* (Jakarta: Universitas Indraprasta PGRI, 2020), <https://proceeding.unindra.ac.id/index.php/semnasristek/article/view/2543>.

<sup>6</sup> Rudi Natamiharja, “La Liberté d’expression En Indonésie: Évaluation de l’expérience Indonésienne Au Regard Des Standards Internationaux” (Aix-Marseille, 2018), <https://theses.fr/2018AIXM0035>.

pencurian, penjualan data pribadi merupakan suatu pelanggaran hukum dalam bidang teknologi informasi dan juga dapat dikategorikan sebagai pelanggaran atas hak asasi manusia, karena data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi.

## 2. METODE PENELITIAN

Metode penelitian yang digunakan yaitu tipe penelitian yuridis normatif, metode pendekatan masalah yaitu pendekatan perundang-undangan dan pendekatan konseptual, bahan hukum yaitu primer dan sekunder, pengumpulan bahan hukum menggunakan studi kepustakaan, yaitu mengumpulkan bahan-bahan hukum yang relevan untuk mendapatkan data yang valid dan akurat, dari seluruh bahan hukum yang didapat, disusun secara sistematis untuk kemudian diolah dan dianalisis secara yuridis normatif yakni mendeskripsikan masalah yang berkaitan dalam penelitian ini.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Penerapan Hukum Untuk Memberikan Perlindungan Bagi Pengguna Jasa Internet Dan Kerahasiaan Data Pribadi

Penerapan hukum merupakan pemberian atau penetapan sanksi bagi pelanggar atas tindakan penyalagunaan terhadap segala bentuk kebocoran dan penyalagunaan data pribadi pengguna jaringan internet, yang dilakukan demi menjamin terlindunginya kerahasiaan data pribadi pengguna jasa internet. dalam ketentuan hukum perdata, jenis perikatan yang paling penting adalah perikatan yang lahir dari adanya perjanjian<sup>7</sup>, karena perjanjian bersifat mengikat kedua belah pihak yang melakukan kesepakatan. Perjanjian yang dimaksud disini dimana pengguna jasa internet memberikan data pribadinya kepada penyedia jasa internet untuk menggunakan jaringan internet dengan demikian penyedia jasa internet tersebut wajib melindungi data-data pribadi pengguna jaringan internet. Kemudian agar terciptanya suatu kepastian hukum, maka dibutuhkan sanksi dari setiap perbuatan yang dilanggar.

Penerapan hukum tersebut merupakan kebutuhan masyarakat terhadap adanya pelanggaran dalam hal ini pelanggaran terhadap kerahasiaan data pribadi pengguna jasa internet. Hal tersebut harus dilakukan secara tegas agar menimbulkan efek jera bagi setiap orang ataupun kelompok dalam penyalagunaan data pribadi. Risiko yang sering terjadi adalah kebocoran data pribadi pelanggan, penjualan pelanggan data pribadi kepada pihak lain, dan penyalahgunaan data nasabah yang menimbulkan kerugian bagi nasabah.

Berdasarkan data yang dilansir CNBC Indonesia tahun 2021 menyebutkan bahwa PT Bank Pembangunan Database Daerah Jawa Timur telah membocorkan 378 GB data yang berisi 259 database pelanggan, data karyawan, dan data keuangan pribadi. Hal serupa juga pernah dialami oleh bank sentral di Indonesia yaitu Bank Indonesia. Pada tahun 2022, Bank Indonesia mengalami kebocoran data yang modus operandinya adalah mengunci sistem dan mengambil Bank Data Indonesia sebagai bank sentral yang membawahi bank-bank lain dan menjadi pusat uang peredaran di Indonesia. Mengatasi permasalahan tersebut, secara internal bank telah

---

<sup>7</sup> Asyhadie Zaeni, *Hukum Bisnis (Prinsip Dan Pelaksanaannya Di Indonesia)* (Jakarta: Raja Grafindo Persada, 2014), h. 24.

menetapkan sistem keamanan (self-regulation). Seperti yang dilakukan oleh PT. Bank Central Asia, Tbk (BCA).<sup>8</sup>

Berdasarkan data pada CNN Indonesia, terdapat setidaknya 10 (sepuluh) kerahasiaan data pribadi pengguna jaringan internet bocor pada tahun 2022. Diantaranya yaitu data pelanggan indihome dimana, sebanyak 26.000.000 (dua puluh enam juta) data pelanggan bocor dan diperjual belikan di *Breach Forms* oleh Bjorka, Agustus. Data-data tersebut berupa histori penarian keyword, username info mencakup email, nama, jenis kelamin, hingga NIK. Data pengguna jasa internet My Pertamina dan Peduli Lindungi pun bocor dan dijual pada situs gelap<sup>9</sup>. Hal inilah yang melandasi penerapan hukum bagi terciptanya perlindungan terhadap data pribadi pengguna jasa internet yang wajib dilindungi.

Berdasarkan Pasal 27 Ayat (3) UU ITE, mengatur bahwa: "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Maka sanksi atau penerapan hukum yang diterima dan dijatuhkan padanya diatur dalam UUKITE tersebut yaitu pada Pasal 45 yang menegaskan bahwa: "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 Ayat (1), Ayat (2), Ayat (3), atau Ayat (4) yaitu: a) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan; b) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian; c) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik; d) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Pasal 1365 KUHP mengatur terkait perbuatan melawan hukum, mengatur bahwa: "Tiap perbuatan yang melanggar hukum dan membawa kerugian kepada orang lain, mewajibkan orang yang menimbulkan kerugian itu karena kesalahannya untuk menggantikan kerugian tersebut," dengan demikian, setiap orang yang melakukan perbuatan melanggar hukum diwajibkan untuk mengganti kerugian yang timbul dari kesalahannya tersebut. OJK berwenang mengenakan sanksi administratif terhadap penyelenggara berupa: a) Peringatan tertulis: Peringatan tertulis diberikan OJK bagi penyedia jasa melalui jaringan internet yang diduga menyebarkan data pribadi pengguna jaringan internet sebagai langkah awal sebelum dikenakan sanksi administratif jika terbukti menyebarkan data pribadi pengguna jaringan internet; b) Denda: Denda yaitu kewajiban untuk membayar sejumlah uang tertentu yang dikenakan pada penyedia jasa internet jika terbukti menyebarkan data

---

<sup>8</sup> Nancy Silvana Haliwela, "The Essence of Legal Protection of Personal Data of Customers In Banking Transactions," *SASI* 29, no. 3 (2023): 548-56, <https://doi.org/10.47268/sasi.v29i3.1528>.

<sup>9</sup> CNN Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah." *Op. Cit.*

pribadi pengguna jasa internet; c) Pembatasan kegiatan usaha: Pembatasan kegiatan usaha adalah salah satu sanksi administratif yang diterima jika penyedia jasa melalui jaringan internet terbukti melakukan penyebaran data pribadi pengguna jasa internet; d) Pencabutan izin: Sanksi administratif akhir yang didapatkan atau diterima penyedia jasa internet yaitu pencabutan izin usaha pada jaringan internet jika menyalagunakan serta menyebarkan data pribadi pengguna jaringan internet.

Tindakan-tindakan diatas dilakukan dengan tujuan agar memberikan efek jera bagi setiap penyedia jasa internet agar tidak mengulangi kesalahan yang sama dan pengguna jaringan internet tersebut mendapatkan perlindungan terhadap kerahasiaan data pribadi tersebut. Kemajuan teknologi informasi dan komunikasi yang semakin meningkat ini menjadikan banyaknya penggunaan jaringan internet oleh pengguna jasa internet. Namun dibalik penggunaannya yang sangat luas dan banyak terdapat berbagai ancaman salah satunya berkaitan dengan penyalagunaan data pribadi pengguna jasa internet, dengan demikian diperlukan peran dari berbagai pihak dalam penerapan perlindungan hukum terhadap data pribadi pengguna jasa internet, untuk menjamin adanya keamanan dan perlindungan terhadap kerahasiaan data pribadi pengguna jasa internet.

Pihak-pihak yang bertanggungjawab dalam penerapan perlindungan hukum terhadap kerahasiaan data pribadi pengguna jasa internet yaitu antara lain:<sup>10</sup>

#### 1) Pemerintah

Pemerintah yang berperan sebagai legislator mempunyai dua tanggung jawab pokok yang harus dipenuhi dalam melindungi informasi dan kerahasiaan data pribadi pengguna jasa internet milik warga negaranya. Tanggung jawab yang pertama yaitu pemerintah harus membuat kerangka hukum atau peraturan hukum yang kuat yang mengatur terkait perlindungan hukum terhadap kerahasiaan data pribadi pengguna jasa internet sebagai hak privasi. Tanggung jawab yang kedua yang harus dilakukan, yaitu pemerintah harus melakukan pengawasan serta penegakkan hukum terhadap regulasi yang dibuat tersebut.

#### 2) Pihak penyedia jasa internet pemroses data pengguna jasa internet

Upaya melindungi data setiap pengguna jasa internet dalam penggunaan internet maka, salah satu pihak yang harus berperan aktif dalam mengontrol pemrosesan data pengguna jasa internet yaitu pihak penyedia jasa internet tersebut dalam pemroses data pengguna jasa internet. Segala sesuatu hambatan yang terjadi dalam penggunaan internet, tentunya pihak tersebut harus dapat mengatasi serta harus dapat pula memilih langkah-langkah mitigasi terhadap resiko yang mungkin terjadi yang menjadi benteng jika terjadi suatu kebocoran data pengguna jasa internet pada system tersebut, karena hal ini adalah merupakan tugas dan tanggung jawab mereka sebagai pihak yang memegang kendali terhadap data pribadi pengguna jasa internet tersebut. Merujuk pada Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 8 tahun 2020 Tentang Sistem Pengaman dan Penyelenggaraan Sistem

---

<sup>10</sup> Ananthia Ayu D, Titis Anindyajati, and Abdul Ghoffar, "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital" (Jakarta, 2019), [https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian\\_123\\_Penelitian\\_Hak\\_Privasi\\_dan\\_Studi\\_Komparasi.pdf](https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian_123_Penelitian_Hak_Privasi_dan_Studi_Komparasi.pdf).

Elektronik, mengharuskan untuk mensertifikasi data pribadi pengguna jasa internet berdasarkan resiko, baik itu level tertinggi maupun terendah.

Kewajiban penyedia jasa internet sebagaimana diatur dalam Peraturan Kemenkoinfo Nomor 4 Tahun 2016 yaitu sebagai berikut: a) Melakukan pengujian keautentikan identitas dan memeriksa otorisasi Pengguna Sistem Elektronik yang melakukan Transaksi Elektronik; Hal ini dimaksudkan penyedia jasa internet wajib melakukan verifikasi bahwa pengguna jasa internet yang memberikan data pribadi dalam penggunaan jasa internet merupakan benar dirinya dan bukan data pribadi orang lain; b) Memiliki dan melaksanakan kebijakan dan prosedur untuk mengambil tindakan jika terdapat indikasi terjadi pencurian data; Penyedia jasa internet wajib memiliki sistem dan kebijakan dalam pengawasan dan perlindungan data pribadi pengguna jasa internet agar terhindar dari pencurian data pribadi pengguna jasa internet tersebut; c) Memastikan pengendalian terhadap otorisasi dan hak akses terhadap sistem, database, dan aplikasi Transaksi Elektronik; Penyedia jasa internet wajib mengendalikan setiap data pribadi pengguna jasa internet dan akses terhadap data pribadi pengguna jasa internet tersebut; d) Menyusun dan melaksanakan metode dan prosedur untuk melindungi dan/atau merahasiakan integritas data, catatan, dan informasi terkait Transaksi Elektronik; Penyedia jasa internet wajib melakukan berbagai metode dan prosedur dalam usaha merahasiakan dan melindungi data pribadi pengguna jasa internet; e) Memiliki dan melaksanakan standar dan pengendalian atas penggunaan dan perlindungan data jika pihak penyedia jasa memiliki akses terhadap data tersebut; Setiap penyedia jasa internet wajib melaksanakan pengendalian terhadap data-data pribadi pengguna jasa internet yang diberikan dalam penggunaan jaringan internet agar terhindar dari berbagai hal yang mengancam pencurian data pribadi pengguna jasa internet; f) Memiliki rencana keberlangsungan bisnis termasuk rencana kontingensi yang efektif untuk memastikan tersedianya sistem dan jasa Transaksi Elektronik secara berkesinambungan; Penyedia jasa internet wajib melakukan rencana kontingensi yang efektif terhadap sistem jaringan internet tersebut; g) Memiliki prosedur penanganan kejadian tak terduga yang cepat dan tepat untuk mengurangi dampak suatu insiden, penipuan, dan kegagalan Sistem Elektronik. Penyedia jasa internet wajib memiliki prosedur dalam penanganan berbagai hal yang dapat mengancam keselamatan data pribadi pengguna jasa internet.

Pihak Penyedia Sistem Elektronik jaringan internet yang strategis dan tinggi wajib dan harus memiliki Sertifikat Sistem Manajemen Pengamanan Informasi terkait data pribadi pengguna jasa internet. Penyedia jasa internet rendah juga dapat memiliki Sertifikat Sistem Manajemen Pengamanan Informasi data pribadi pengguna jasa internet. Sertifikasi Sistem Manajemen Pengamanan Informasi terkait data pribadi pengguna jasa internet dilakukan oleh Lembaga Sertifikasi yang diakui oleh Menteri. Lembaga Sertifikasi harus memenuhi syarat sebagai berikut:<sup>11</sup> a) Berbentuk badan hukum Indonesia; b) Berdomisili di Indonesia; c) Terakreditasi oleh Komite Akreditasi Nasional; d) Memiliki Tim Auditor yang beranggotakan paling sedikit 1 (satu) Auditor Permanen; e) Memiliki Tim pengambil keputusan sertifikasi.

### 3) Aparat Penegak hukum

---

<sup>11</sup> *Ibid*

Aparat penegak hukum merupakan pihak yang berperan penting dalam penegakan hukum, para aparat penegak hukum tersebut, meliputi:<sup>12</sup> a) Polisi; b) Hakim; c) Jaksa, maupun; d) BSSN. Ranah dan tanggung jawab mereka sebagai penegak hukum. Korelasi atau hubungan antar pihak ini menjadi salah satu kunci untuk menegakkan hukum yang ada sebagai upaya perlindungan terhadap data pribadi pengguna jasa internet.

Kemampuan dan kemauan para aparat penegak hukum (hakim, jaksa dan polisi) diperlukan agar memahami apa itu pelanggaran privasi khususnya dalam kaitan dengan *e-commerce*. Hakim dan penegak hukum lainnya harus mampu menyelesaikan kasus-kasus yang muncul sebagai akibat terjadinya perubahan kondisi sosial masyarakat tersebut. Pada akhirnya, dengan adanya struktur yang memadai, diharapkan dapat memberikan kontribusi terhadap pembentukan hukum yang responsif. Hukum responsif adalah hukum yang dapat mengakomodasi dan mengikuti perubahan zaman terutama dalam hal ini berkaitan dengan hukum teknologi informasi yang selalu cepat berubah.

#### 4) Pengguna Jasa internet

Pihak ini juga berperan penting dalam menjaga privasi terhadap data pribadi yaitu pengguna jasa internet itu sendiri. Ketika melakukan aktivitas bermedia sosial dalam penggunaan jasa internet, baiknya pengguna jasa internet paham dan mengerti betul terkait kode etik dan tata cara dalam menggunakan jasa internet tersebut. Pengguna jasa internet juga harus tahu terkait apa yang boleh dilakukan dan tidak boleh dilakukan dalam penggunaan internet agar hal-hal yang tidak diinginkan tidak terjadi kedepannya. Karena dikhawatirkan regulasi dan pihak lain sudah menjalankan perannya dengan baik, namun pengguna jasa internetlah yang malah tidak mematuhi peraturan atau malah menggambar sendiri data pribadi yang menjadi privasinya.

Berikut ini berbagai cara yang harus dilakukan oleh pengguna jasa itu sendiri demi menjamin kerahasiaan data pribadinya antara lain:<sup>13</sup> a) Menjaga kerahasiaan dan kekuatan sandi akun serta melakukan penggantian sandi akun secara berkala. Hal ini dilakukan demi menjaga keamanan data pribadi yang dapat dilakukan oleh pengguna itu sendiri agar meminimalisir terjadinya pencurian data pribadi dan penyalagunaan data pribadi oleh pihak lain; b) Menghindari penggunaan koneksi internet wireless (Wi-Fi) di sembarang tempat. Menggunakan koneksi internet wireless dapat mengancam terjadinya pencurian data pribadi oleh pihak pemberi wifi tersebut; c) Gunakanlah perangkat lunak (*software*) yang legal dan lakukan pembaharuan secara berkala untuk memperkecil adanya celah keamanan yang mungkin saja muncul. Pengguna jasa internet wajib menggunakan aplikasi-aplikasi yang aman agar terhindar dari adanya pencurian data pribadi; d) Berhati-hati terhadap tautan mencurigakan yang disebar melalui pesan singkat dan surel ataupun kanal lainnya. Karena, tautan tersebut bisa saja berupa tautan palsu yang nantinya akan mengarah pada praktik kejahatan, seperti phishing. *Phising* yaitu upaya yang dilakukan oleh pihak tertentu untuk mendapatkan informasi data pribadi seseorang dengan teknik pengelabuan. Pengelabuan dalam istilah komputer adakalanya penipuan yang dicirikan dengan percobaan untuk

---

<sup>12</sup> *Ibid*

<sup>13</sup> Iteba.ac.id, "Perlindungan Data Pribadi Di Era Digital," <https://iteba.ac.id/>, 2023, <https://iteba.ac.id/berita/perlindungan-data-pribadi-di-era-digital/>.

mendapatkan informasi yang sensitif, seperti kata sandi dan kartu kredit, dengan menyamar sebagai seseorang atau pebisnis tepercaya melalui komunikasi elektronik resmi, seperti surat elektronik atau pesan instan.

Perlindungan data konsumen yang berkaitan dengan data pribadi di atur dalam POJK No. 77 /POJK.01/ 2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dalam Pasal 26. Pasal tersebut mewajibkan penyelenggara untuk menjaga kerahasiaan data pribadi pengguna jasa. Pasal 29 kemudian menyatakan bahwa penyelenggara wajib memperhatikan prinsip-prinsip dasar perlindungan pengguna, yaitu transparansi, perlakuan adil, keandalan, kerahasiaan, dan keamanan data, serta penyelesaian perselisihan pengguna dengan mudah, cepat, dan terjangkau. Selain kewajiban, penyelenggara tidak boleh mengungkapkan data Pengguna dengan cara apa pun kepada pihak ketiga, kecuali Pengguna menyetujui hal ini secara elektronik dan/atau karena undang-undang mewajibkannya. Apabila penyelenggara melanggar kewajiban dan larangan dalam POJK ini, maka akan dikenakan sanksi administratif. Sanksi tersebut berupa peringatan tertulis, kewajiban membayar denda dalam bentuk uang, pembatasan kegiatan usaha dan pencabutan izin.

### **3.2 Bentuk Perlindungan Hukum Bagi Pengguna Jasa Internet Terhadap Kerahasiaan Data Pribadi**

Menurut Philipus M. Hadjon Bentuk Perlindungan Hukum dilaksanakan sebagai kumpulan aturan atau kaidah hukum yang dilakukan untuk melindungi suatu hal dari hal lainnya. Berkaitan dengan kerahasiaan data pribadi pengguna jasa internet, berarti hukum memberikan perlindungan terhadap hak-hak pengguna jasa internet dari sesuatu yang mengakibatkan tidak terpenuhinya hak-hak tersebut dalam hal ini kerahasiaan data pribadi pengguna jaringan internet tersebut<sup>14</sup>. Data pribadi pengguna jasa internet merupakan data yang sifatnya privasi dan tidak boleh ada intervensi dari pihak lainnya. Berdasarkan kajian antropologis, biologis, dan sosiologis menunjukkan bahwa dalam masyarakat primitif sekalipun, setiap individu selalu memiliki keinginan untuk semacam privasi, dalam menjamin terpenuhinya perlindungan hukum bagi pengguna jasa internet terhadap kerahasiaan data pribadi maka terdapat beberapa bentuk perlindungan hukum diantaranya:<sup>15</sup>

- 1) Adanya Pengawasan Pemerintah baik secara langsung maupun tidak langsung kepada pengguna jasa internet terhadap kerahasiaan data pribadi dalam penggunaan jaringan internet.

Bentuk perlindungan hukum bagi pengguna jasa internet terhadap kerahasiaan data pribadi dalam bentuk pengawasan tersebut dilakukan agar mengawasi data-data pribadi pengguna jasa internet dari segala bentuk tindakan penyalagunaan data pribadi pengguna jasa internet tersebut. Berdasarkan Permen Kominfo Nomor 20 Tahun 2016 tentang perlindungan data pribadi dalam sistem elektronik Pasal 35 menegaskan bahwa: (1) Pengawasan terhadap pelaksanaan Peraturan Menteri ini dilaksanakan oleh Menteri dan/atau pimpinan Intansi Pengawas dan Pengatur Sektor, dengan demikian pemerintah dalam hal ini menteri kominfo

---

<sup>14</sup> Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi* (Surabaya: Peradaban, 2007), h. 1-2.

<sup>15</sup> D, Anindyajati, and Ghoffar, "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital." *Op.Cit.*

atau pimpinan sektor memberikan pengawasan terhadap terlindunginya kerahasiaan data pribadi pengguna jaringan internet; (2) Pengawasan yang dilaksanakan Menteri sebagaimana dimaksud pada Ayat meliputi pengawasan secara langsung maupun tidak langsung. Pengawasan tersebut dapat dilakukan secara langsung maupun tidak langsung; (3) Menteri berwenang meminta data dan informasi dari Penyelenggara Sistem Elektronik dalam rangka perlindungan Data Pribadi. Penyelenggara atau penyedia jasa internet wajib memberikan data dan informasi kepada kementerian kominfo agar dapat melakukan perlindungan terhadap kerahasiaan data pribadi pengguna jaringan internet; (4) Permintaan data dan informasi sebagaimana dimaksud pada Ayat (3) dapat dilakukan secara berkala atau sewaktu-waktu apabila diperlukan; (5) Menteri mendelegasikan kewenangan pengawasan kepada Direktur Jenderal. Menteri dapat memberikan perwakilan dalam rangka pengawasan perlindungan hukum terhadap kerahasiaan data pribadi pengguna jaringan internet.

## 2) Adanya Prinsip Perlindungan Keamanan Data Pribadi

Perlindungan keamanan data pribadi ini mewajibkan segala bentuk perlindungan terhadap kerahasiaan data pribadi pengguna jasa internet yang baik yang terhindar dari resiko kehilangan atau akses tidak sah, perusakan, penggunaan, perubahan, atau pengungkapan data pribadi pengguna jaringan internet.

Penyedia jasa internet berkewajiban untuk menjaga keamanan data pengguna jasa internet atau penggunanya yang tercantum dalam Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Prinsip Tanggung Jawab Mutlak atau disebut Prinsip Tanggung Jawab Absolute / mutlak (*Absolute Liability*) adalah prinsip yang wajib menjadi tanggung jawab penyedia jasa internet terhadap data pribadi pengguna jaringan internet tersebut. Terdapat Implementasi Nasional atas Prinsip-prinsip Dasar Perlindungan terhadap data pribadi pengguna jasa internet, yang dimana beberapa prinsipnya adalah:<sup>16</sup> a) *Use Limitation Principle* (Prinsip Pembatasan Penggunaan Data): Prinsip pembatasan penggunaan data ini menjelaskan bahwa data pribadi tidak boleh diungkapkan dan disediakan serta digunakan untuk tujuan lain selain yang ditentukan oleh penyedia jasa internet kecuali dengan persetujuan dari pemilik data atau pengguna jasa internet tersebut atau oleh otoritas hukum, dengan demikian prinsip ini secara tegas membatasi penyedia jasa internet dalam mengelola data pribadi pengguna jaringan internet hanya digunakan untuk memvalidasi penggunaan internet oleh pengguna jasa internet dan hal tersebut dilindungi oleh peraturan perundang-undangan; b) *Security Safeguards Principle* (Prinsip Perlindungan Keamanan Data): Prinsip perlindungan keamanan data ini menjelaskan bahwa kewajiban dan keharusan dalam melindungi data pribadi dengan melakukan penjagaan keamanan yang baik dan wajar terhadap risiko seperti kehilangan akses, perusakan, penggunaan, dan modifikasi maupun pengungkapan data yang tidak sah.

## 3) Adanya Pengamanan Data Pribadi Pengguna Jasa Internet

Menjaga kerahasiaan data pribadi pengguna jasa internet maka diperlukan pengamanan data dalam jaringan internet. Hal ini dilakukan dengan tujuan agar data tidak dapat dibaca

---

<sup>16</sup> Rizka Nurdinisari et al., "Perlindungan Hukum Terhadap Privasi Dan Data Pribadi Pengguna Telekomunikasi Dalam Penyelenggaraan Telekomunikasi Khususnya Dalam Menerima Informasi Promosi Yang Merugikan" (Universitas Indonesia, 2013).

dan dimengerti oleh pihak lain kecuali penyedia dan pengguna jasa internet yang memiliki data tersebut. Pengamanan data tersebut selain bertujuan untuk meningkatkan keamanan data, juga mempunyai fungsi lain yaitu untuk: a) Melindungi data pribadi pengguna jaringan internet agar tidak dapat dibaca oleh orang/pihak lain yang tidak berhak terhadap data tersebut. Pengamanan ini wajib dilakukan oleh Penyedia jasa internet melalui lembaga-lembaga tersertifikasi dalam proses pengamanan data pribadi pengguna jasa internet untuk melindungi kerahasiaan data pribadi; b) Mencegah agar orang/pihak lain yang tidak berhak tidak menyisipkan, menghapus, dan merubah data pribadi pengguna jasa internet tersebut. Pencegahan pengamanan data dilakukan agar mencegah pihak lain mencuri data pribadi pengguna jaringan internet untuk menyalagunakan data pribadi tersebut.

Hal-hal diatas harus dan wajib dilaksanakan demi menjaga keamanan data pribadi pengguna jaringan internet.

4) Adanya sanksi administratif terhadap penyalagunaan data pribadi pengguna jaringan internet.

Sanksi administratif yang dijatuhkan kepada pelanggaran penyalagunaan data pribadi pengguna jaringan internet yaitu berupa<sup>17</sup>: a) Peringatan tertulis: Peringatan tertulis ini diberikan kepada setiap penyedia jasa internet yang menyalagunakan data pribadi pengguna jaringan internet sebagai bahan peringatan. Sehingga penyedia jasa internet wajib memperbaiki masalah yang terjadi akibat penyalagunaan terhadap kerahasiaan data pribadi pengguna jaringan internet; b) Denda: Kewajiban untuk membayar sejumlah uang tertentu; Denda diberikan kepada penyedia jasa internet ataupun orang yang melakukan penyalagunaan data pribadi pengguna jaringan internet sebagai sanksi administratif yang didapatkan akibat melakukan pelanggaran hukum tersebut; c) Pembatasan kegiatan usaha: Jika penyedia jasa internet tidak mampu memperbaiki sistem elektronik dalam jaringan internet yang dimilikinya dalam hal kerahasiaan data pribadi pengguna jaringan internet, maka pemerintah dapat membatasi kegiatan usaha dari penyedia jasa internet tersebut; d) Pencabutan izin: Pencabutan izin dilakukan kepada penyedia jasa internet jika melakukan pelanggaran terhadap kerahasiaan data pribadi pengguna jaringan internet tersebut.

Adanya sanksi administratif berupa, peringatan tertulis, denda, pembatasan kegiatan usaha bahkan pencabutan izin merupakan sanksi yang diberikan sebagai upaya perlindungan dan penerapan hukum bagi setiap penyalagunaan penggunaan data pribadi pengguna jasa internet dan memberikan efek jera bagi setiap penyalagunaan penggunaan data pribadi pengguna jasa internet dan melindungi pengguna jasa internet dari berbagai upaya pencurian data pribadi oleh penyedia jasa internet dan berbagai pihak yang ingin melakukan pencurian data pribadi pengguna jasa internet tersebut.

Sebagai bagian dari perlindungan privasi, penghormatan terhadap hak privasi harus dimulai untuk menjamin kepastian hukum. Oleh karena itu perlindungan terhadap perlindungan data harus ditempatkan pada peraturan perundang-undangan yang mempunyai kekuasaan tertinggi yaitu konstitusi, karena konstitusi atau konstitusi merupakan perbuatan hukum tertinggi suatu negara. Kepastian hukum (asas legalitas) diperlukan dan

---

<sup>17</sup> D, Anindyajati, and Ghoffar, "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital." *Op. Cit.*

tidak dapat dikesampingkan dalam rangka perlindungan hukum di semua negara. Langkah negara untuk menjamin kepastian hukum adalah dengan ditegaskan dan dijaminnya hak-hak tersebut dalam konstitusi, dan melalui instrumen itulah karakter negara terlihat, sistem hukum apa yang dipakai dan bagaimana pengaturan pemerintahannya,<sup>18</sup> dengan demikian, sudah waktunya negara Indonesia memiliki regulasi yang jelas terhadap perlindungan data pribadi.

Upaya pengaturan terkait hak privasi atas data pribadi merupakan perwujudan atas pengakuan dan perlindungan hak-hak dasar manusia. Oleh karenanya, penyusunan Rancangan Undang-Undang tentang Perlindungan Data pribadi mempunyai landasan filosofis yang kuat serta dapat dipertanggungjawabkan. Landasan filosofis yang dimaksud adalah Pancasila yang merupakan *rechtsidee* (cita hukum) serta gagasan untuk mewujudkan hukum kepada yang dicita-citakan. Perlindungan Data Pribadi adalah bentuk perwujudan amanat konstitusi yang harus diatur dalam bentuk Undang-Undang. Pasal 28 UUD 1945 Amandemen Keempat, mengatur bahwa: “Setiap orang memiliki atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang berada dalam kekuasaannya, serta memiliki hak atas rasa aman dan perlindungan dari ancaman ketakutan berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

Pasal ini memberikan pesan pentingnya dibentuk peraturan perundang-undangan yang melindungi data pribadi. Putusan Mahkamah Konstitusi Nomor 006/PUU-I/2003 menguatkan bahwa pengaturan Perlindungan Data Pribadi harus dalam bentuk Undang-Undang. Sebagaimana dikuatkan oleh Putusan Mahkamah Konstitusi bahwa terkait ketentuan yang menyangkut hak asasi manusia, harus diatur dalam bentuk Undang-Undang. Pasal 14 UU Perlindungan data pribadi disebutkan terkait prinsip-prinsip dan hak-hak pemilik data pribadi dalam hal: a) Keamanan nasional; b) Kepentingan proses penegakan hukum; c) Kepentingan pers sepanjang data pribadi diperoleh dari informasi yang sudah dipublikasikan dan disepakati oleh pemilik; d) Kepentingan penelitian ilmiah dan statistik sepanjang data pribadi diperoleh dari informasi yang sudah dipublikasikan (konfirmasi kembali untuk kepentingan penelitian).

Perlindungan data pribadi menekankan bahwa setiap orang berhak menentukan nasibnya sendiri seperti apakah dirinya akan melakukan sharing data atau tidak dan apabila sharing data dilakukan maka ia berhak juga menentukan syarat yang hendak dipenuhi dalam suatu komunitas masyarakat Perlindungan data pada dasarnya dapat berhubungan secara khusus dengan privasi seperti yang dikemukakan oleh Allan Westin yang untuk pertama kali mendefinisikan privasi sebagai hak individu, grup atau lembaga untuk menentukan apakah informasi tentang mereka akan dikomunikasikan atau tidak kepada pihak lain sehingga definisi yang dikemukakan oleh Westin disebut dengan *information privacy* karena menyangkut informasi pribadi.<sup>19</sup> Pendapat Westin ini apabila kita bawa dalam konteks bisnis *Fintech* yang berkembang pesat di tengah lajunya perkembangan teknologi informasi, bisa dipahami bahwa data pribadi perlu dilindungi karena data pribadi merupakan bagian dari privasi individu,

---

<sup>18</sup> Rudi Natamiharja and Stefany Mindoria, “Perlindungan Data Privasi Dalam Konstitusi Negara Anggota ASEAN” (Lampung, 2019), h. 3.

<sup>19</sup> Alan F Westin, “Privacy And Freedom,” *Washington and Lee Law Review* 25, no. 1 (1968): 166-70, <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>.

sehingga pemilik data pribadi itu sendirilah yang menentukan apakah data pribadinya boleh diakses dan diketahui oleh orang lain atau tidak. Artinya segala data pribadi tersebut apabila pihak lain ingin mengetahuinya harus dengan persetujuan pemilik data pribadi.

Sebagai bagian dari perlindungan privasi, penghormatan terhadap hak privasi harus dimulai untuk menjamin kepastian hukum. Oleh karena itu perlindungan terhadap perlindungan data harus ditempatkan pada perbuatan hukum yang mempunyai kewenangan tertinggi yaitu konstitusi, karena konstitusi atau konstitusi merupakan perbuatan hukum tertinggi suatu negara. Kepastian hukum (asas legalitas) diperlukan dan tidak dapat dikesampingkan dalam rangka perlindungan hukum di semua negara. Langkah negara untuk menjamin kepastian hukum merupakan penegasan dan jaminan hak-hak tersebut dalam konstitusi, yang dalam hal ini karakter negara dapat dilihat dari apa yang disajikan dengan bantuan instrumen tersebut, sistem hukum apa yang dipakai dan bagaimana pengaturan pemerintahannya,<sup>20</sup> dengan demikian, sudah waktunya negara Indonesia memiliki regulasi yang jelas terhadap perlindungan data pribadi.

#### 4. KESIMPULAN

Bentuk pengawasan terhadap data pribadi pengguna jasa internet sesuai dengan Pasal 35 Permen Kominfo Nomor 20 Tahun 2016 tentang perlindungan data pribadi dalam sistem elektronik. Adanya Prinsip Perlindungan keamanan data pribadi sesuai Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dimana Penyedia jasa internet berkewajiban untuk menjaga keamanan data pengguna jasa internet atau penggunanya. Adanya Pengamanan data pribadi pengguna jasa internet Untuk mengamankan data pribadi pengguna jasa internet dari pihak yang tidak berhak.

#### REFERENSI

##### Jurnal

Haliwela, Nancy Silvana. "The Essence of Legal Protection of Personal Data of Customers In Banking Transactions." *SASI* 29, no. 3 (2023): 548-56. <https://doi.org/10.47268/sasi.v29i3.1528>.

Palinggi, Sandryones, and Erich C. Limbongan. "Pengaruh Internet Terhadap Industri ECommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan Di Indonesia." In *Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi)*. Jakarta: Universitas Indraprasta PGRI, 2020. <https://proceeding.unindra.ac.id/index.php/semnasristek/article/view/2543>.

Rosadi, Sinta Dewi. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia." *Yustisia* 5, no. 1 (2016): 22-30. <https://doi.org/10.20961/yustisia.v5i1.8712>.

Westin, Alan F. "Privacy And Freedom." *Washington and Lee Law Review* 25, no. 1 (1968): 166-70.

---

<sup>20</sup> Natamiharja and Mindoria, "Perlindungan Data Privasi Dalam Konstitusi Negara Anggota ASEAN." *Op. Cit*, h. 3.

<https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlu>.

## Buku

Hadjon, Philipus M. *Perlindungan Hukum Bagi Rakyat Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi*. Surabaya: Peradaban, 2007.

Zaeni, Asyhadie. *Hukum Bisnis (Prinsip Dan Pelaksanaannya Di Indonesia)*. Jakarta: Raja Grafindo Persada, 2014.

## Online/World Wide Web, Disertasi/Tesis/Skripsi, Dan Lain-Lain

Andriadi, Fayakhun. "Pemanfaatan Akses Internet Dalam Mendukung Kemajuan Bangsa." [www.kompasiana.com](http://www.kompasiana.com), 2010.  
[https://www.kompasiana.com/fayakhun/55002c84a33311e57250ff78/pemanfaatan-akses-internet-dalam-mendukung-kemajuan-bangsa?page=3&page\\_images=1](https://www.kompasiana.com/fayakhun/55002c84a33311e57250ff78/pemanfaatan-akses-internet-dalam-mendukung-kemajuan-bangsa?page=3&page_images=1).

CNN Indonesia. "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah." [www.cnnindonesia.com](http://www.cnnindonesia.com), 2022.  
<https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2>.

D, Ananthia Ayu, Titis Anindyajati, and Abdul Ghoffar. "Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital." Jakarta, 2019.  
[https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian\\_123\\_Penelitian\\_Hak\\_Privasi\\_dan\\_Studi\\_Komparasi.pdf](https://www.mkri.id/public/content/infoumum/penelitian/pdf/hasilpenelitian_123_Penelitian_Hak_Privasi_dan_Studi_Komparasi.pdf).

Iteba.ac.id. "Perlindungan Data Pribadi Di Era Digital." <https://iteba.ac.id/>, 2023.  
<https://iteba.ac.id/berita/perlindungan-data-pribadi-di-era-digital/>.

Natamiharja, Rudi. "La Liberté d'expression En Indonésie: Évaluation de l'expérience Indonésienne Au Regard Des Standards Internationaux." Aix-Marseille, 2018.  
<https://theses.fr/2018AIXM0035>.

Natamiharja, Rudi, and Stefany Mindoria. "Perlindungan Data Privasi Dalam Konstitusi Negara Anggota ASEAN." Lampung, 2019.

Nurdinisari, Rizka, Edmon Makarim, Agus Sardjono, and Brian Amy Prastyo. "Perlindungan Hukum Terhadap Privasi Dan Data Pribadi Pengguna Telekomunikasi Dalam Penyelenggaraan Telekomunikasi Khususnya Dalam Menerima Informasi Promosi Yang Merugikan." Universitas Indonesia, 2013.

Rhani, Ashya Ravika Mahar. "5 Manfaat Internet." [www.kompas.com](http://www.kompas.com), 2020.  
[https://www.kompas.com/skola/read/2020/10/08/224859069/5-manfaat-internet?page=all#:~:text=KOMPAS.com - Manfaat internet adalah ,](https://www.kompas.com/skola/read/2020/10/08/224859069/5-manfaat-internet?page=all#:~:text=KOMPAS.com - Manfaat internet adalah,)