

PERLINDUNGAN HUKUM TERHADAP PEMILIK DATA PRIBADI PENGGUNA TEKNOLOGI INFORMASI AKIBAT TINDAK PIDANA PERETASAN¹

Oleh :

Meyse Stevely Sisilia Wuwungan²

Cornelis Dj. Massie³

Josepus Jullie Pinori⁴

ABSTRAK

Penelitian ini bertujuan untuk mengetahui pengaturan data pribadi pengguna teknologi informasi di Indonesia dan untuk mengetahui perlindungan hukum terhadap pemilik data pribadi yang mengalami kebocoran akibat tindakan peretasan. Dengan menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu: 1. Pengaturan perlindungan data pribadi pengguna teknologi informasi di Indonesia, yakni dibentuknya Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi melalui proses yang begitu panjang, dimana pada tahun 2020 telah menjadi Rancangan Undang-undang Perlindungan Data Pribadi yang dikirimkan ke DPR dan disahkan pada tanggal 17 Oktober Tahun 2022. Undang-undang yang berisikan 72 pasal ini membahas mengenai perlindungan terhadap data pribadi warga Indonesia. 2. Perlindungan hukum terhadap pemilik data pribadi yang mengalami kebocoran akibat Tindakan peretasan masih terbilang lemah karena pada kenyataan yang terjadi pada saat ini masih saja terjadi kasus hacking yang disebabkan oleh hacker yang tidak bertanggung jawab, dan juga sebabkan oleh kelalaian pengendali data pribadi dalam memproteksi data warga negara Indonesia sehingga berulang kali situs maupun aplikasi yang dibuat oleh pemerintah diretas, sehingga berakhir dengan tindakan yang tidak bertanggung jawab, yakni dengan dijualnya secara ilegal data pribadi warga negara Indonesia dalam situs-situs dengan sengaja dan menguntungkan pihak-pihak yang tidak bertanggung jawab.

Kata Kunci : *peretasan data pribadi*

PENDAHULUAN

A. Latar Belakang

Perlindungan data pribadi merupakan bagian dari perlindungan konstitusional sebagaimana ditegaskan dalam Undang-Undang Dasar 1945 Pasal 28 G ayat (1) yang berbunyi: "Setiap orang

berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi." dan juga pada Pasal 28H ayat (4) "Setiap orang berhak mempunyai hak milik pribadi dan hak milik tersebut tidak boleh diambil alih secara sewenang-wenang oleh siapapun".

Perlindungan data pribadi juga termasuk dalam tantangan perlindungan hak asasi manusia (HAM) dimana seseorang berhak menentukan dapat atau tidaknya membagi dan bertukar data pribadi mereka, seperti yang tertulis pada Pasal 29 ayat (1) Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia menegaskan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan hak miliknya.

Adanya data pribadi warga Indonesia yang sering di hacking, dengan ini mendorong pemerintah untuk membuat peraturan untuk melindungi data pribadi warga Indonesia. Disahkannya Undang-undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik, kemudian mengalami revisi karena mengalami beberapa kekurangan, kemudian diganti dengan Undang-undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik atau yang sering kita sebut UU ITE. UU ITE dibentuk untuk mengantisipasi semua bentuk *cyber crime*, dalam hal ini kejahatan *hacking*, meski telah mengalami beberapa revisi akan tetapi masih saja ada kekurangan dan dampak yang kurang baik yang ditimbulkan harus diperbaiki terutama pasal karet atau ketidakjelasan arti agar Undang-undang ITE ini tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.⁵ Dengan ini dibentuklah Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), dengan adanya Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, menjadi harapan agar dapat melindungi data pribadi warga Indonesia dengan maksimal.

Dalam pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik menyatakan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. Dan juga pada Pasal 65 ayat

¹ Artikel Skripsi

² Mahasiswa Fakultas Hukum Unsrat, NIM 19071101063

³ Fakultas Hukum Unsrat, Doktor Ilmu Hukum

⁴ Fakultas Hukum Unsrat, Doktor Ilmu Hukum

⁵ Tomi Wicaksono Putra, Hamidah Abdurrachman, Achmad Irwan Hamzani *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*, (Jawa Tengah: Penerbit PT Nasya Expanding Management, 2023), hlm. 96

(1) dan (2) Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi menegaskan bahwa, setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi, serta dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.⁶

Perkembangan teknologi dan internet pada khususnya telekomunikasi, multimedia dan teknologi informasi di era globalisasi saat ini sangatlah pesat sehingga pada akhirnya merubah struktur organisasi dan hubungan sosial masyarakat, dan juga telah mengubah gaya hidup masyarakat secara global sehingga menimbulkan perubahan dalam kerangka budaya, sosial, ekonomi, dan hukum yang berlangsung secara cepat dan signifikan.⁷

Pesatnya perkembangan teknologi informasi dan komunikasi digital di Indonesia diiringi dengan meningkatnya produktivitas dan efisiensi masyarakat untuk memenuhi keinginan dan kebutuhan hidup, baik dalam komunikasi, berbelanja, melakukan *video conference*, melakukan transaksi elektronik, melakukan peradilan secara *online* yang saat ini dapat dilakukan dengan lebih muda dan cepat tanpa dibatasi oleh jarak, ruang dan waktu, seperti pada layanan *e-commerce*, *e-banking*, *e-education*, *e-government*, *e-court* serta *e-litigation* yang dapat memudahkan masyarakat dalam melakukan berbagai aktivitas. Namun dibalik kemudahan-kemudahan tersebut masih ada ancaman bagi para pengguna teknologi digital, salah satunya ialah keamanan data pribadi yang dimiliki oleh setiap pengguna.⁸ Dimana pengguna diwajibkan untuk memasukan data pribadi kedalam sistem elektronik yang dibuat oleh penyelenggara sistem elektronik. Ada beberapa oknum yang menyalahgunakan kepintarannya tentang teknologi untuk melakukan perbuatan ilegal dengan mencuri data dan menjualnya di situs berbahaya atau yang sering dikenal dengan nama *darkweb*. Hal tersebut dapat dilihat dari banyaknya kasus kebocoran data pribadi yang terjadi, seperti kasus kebocoran data Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan yang terjadi pada tahun 2021 dimana

sekitar 279 juta data warga Indonesia termasuk mereka yang sudah meninggal dunia diduga diretas dan dijual di forum daring oleh pengguna forum berbagi database RaidForums dengan akun bernama Kotz. Data yang diduga berasal dari BPJS Kesehatan tersebut dikonfirmasi oleh Kementerian Kominfo yang menemukan bahwa sampel data yang bocor diduga kuat identik dengan data BPJS Kesehatan. Hal tersebut didasarkan pada data Nomor Kartu, Kode Kantor, Data Keluarga/Data Tanggungan, dan status pembayaran yang identik dengan data BPJS Kesehatan.⁹

Kasus yang terjadi pada tahun 2022 dimana seorang peretas bernama Bjorka membocorkan 3,2 miliar data aplikasi PeduliLindungi ke publik. Adapun data yang diunggah, yaitu nama, email, nomor induk kependudukan (NIK), nomor kartu tanda penduduk (KTP), nomor telepon, tanggal lahir, identitas perangkat, status Covid-19, riwayat *check-in*, riwayat pelacakan kontak, vaksinasi, dan masih banyak data lainnya. Data tersebut benar valid terdata di data kependudukan saat dilakukan pengecekan menggunakan aplikasi pengecek nomor KTP.¹⁰

Pada bulan juli tahun 2023, Bjorka membocorkan sebanyak 34 juta data yang diklaim sebagai data paspor. Dalam kasus ini Bjorka membagikan sampel sebanyak satu juta data nama pengguna paspor, data ini meliputi , NIKIM (National Identiti Kartu Identitas Masyarakat), nomor paspor, tanggal pembuatan, tanggal kadaluarsa, tanggal lahir, dan jenis kelamin.¹¹

Kasus-kasus kebocoran data yang terjadi di atas berpotensi besar disalahgunakan, dimana data tersebut dapat digunakan untuk membuat identitas palsu maupun penipuan dengan mengatasnamakan data pribadi orang lain yang bocor.

Peredaran data pribadi dalam teknologi digital yang tidak mengenal batas menjadikan semakin mudahnya data pribadi seseorang terekspos atau dipindah tangankan secara semena-mena tanpa izin dari pemilik data.

⁶ Pasal 65 ayat (1) dan (2) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

⁷ Dikdik M. Arief Mansur, Elisatris Gultom, *Cyber Law Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2005), hlm 2.

⁸ Himakom, *Perlindungan Data Pribadi di Era Digital*, <http://himakom.student.unv.ac.id/perlindungan-data-pribadi-di-era-digital/>, diakses pada tanggal 10 Agustus 2023.

⁹ *BPJS Kesehatan: Data ratusan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat'*, kata pakar, <https://www.bbc.com/indonesia/indonesia-57196905>, diakses pada tanggal 02 September 2023.

¹⁰ Andri Saubani, *CISSReC: 3,2 Miliar Data PeduliLindungi Bocor*, <https://news.republika.co.id/berita/rle9di409/cissrec-32-miliar-data-pedulilindungi-bocor>, diakses pada tanggal 10 Agustus 2023.

¹¹ *Sebanyak 34 juta data pemegang paspor Indonesia diduga 'bocor'*, <https://www.bbc.com/indonesia/articles/c9e7e9grjmko>, diakses pada tanggal 02 September 2023.

Lemahnya perlindungan data di Indonesia membuat para *hacker* (peretas) dengan mudah meretas maupun melakukan pembajakan terhadap data yang mengakibatkan bocornya data pribadi, pemerasan dan penipuan online. Banyaknya kasus kebocoran data yang terjadi telah menunjukkan kegagalan dalam melindungi data pribadi oleh penyelenggara atau pengendali data pribadi baik dari pemerintah maupun dari swasta.

B. Rumusan Masalah

1. Bagaimana pengaturan perlindungan data pribadi pengguna teknologi informasi di Indonesia?
2. Bagaimana perlindungan hukum terhadap pemilik data pribadi yang mengalami kebocoran akibat tindakan peretasan ?

C. Metode Penelitian

Penelitian ini menggunakan metode penelitian hukum normatif.

PEMBAHASAN

A. Pengaturan Data Pribadi Pengguna Teknologi Informasi Di Indonesia

Pengaturan perlindungan data pribadi telah dibahas jauh sebelum adanya kasus-kasus hacking yang sedang marak saat ini yakni pada tahun 2016, dengan pembahasan mengenai 72 pasal dalam Rancangan Undang-Undang (RUU) tersebut pengaturan perlindungan data pribadi menjadi prioritas untuk dibahas berdasarkan putusan DPR RI Nomor 19/DPR RI/I2018-2019 tentang Program Legislasi Nasional RUU Tahun 2015-2019.

Pada tahun 2020, Rancangan Undang-undang Pelindungan Data Pribadi akhirnya dikirimkan kepada DPR dan mengalami dua proses, yaitu pendahuluan dan pembicaraan tingkat I. Proses pendahuluan dilaksanakan pada bulan Januari hingga bulan Februari 2020, yang berisi tahapan penugasan oleh Presiden kepada Menkominfo, Mendagri, dan Menkumham untuk melakukan pembahasan dengan DPR RI. Kemudian pada bulan Februari 2020 sampai bulan Mei 2022, RUU PDP masuk pada tahapan pembicaraan tingkat I, berisi tentang rangkaian rapat panitia kerja pembahasan RUU PDP oleh Komisi I DPR RI dengan tim panitia kerja pemerintah. Pada tanggal 20 September tahun 2020, terjadi tahapan pembahasan tingkat II yang menghasilkan pengesahan RUU menjadi Undang-undang Pelindungan Data Pribadi yang berisikan 16 bab dan 76 pasal.

Rancangan Undang-undang Pelindungan Data Pribadi akhirnya telah disahkan menjadi Undang-Undang Pelindungan Data Pribadi.

Undang-undang ini hadir di tengah masyarakat Indonesia untuk memungkinkan masyarakat memiliki kedaulatan data, pengelolaan penggunaan data oleh industri maupun lembaga negara untuk perlindungan dan keamanan masyarakat. Lahirnya Undang-undang PDP untuk melindungi data pribadi masyarakat yang dikelola oleh penyelenggara system elektronik atau PSE atau mencegah disalahgunakannya data dari pihak yang tidak bertanggung jawab. Presiden Jokowi telah menandatangani Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada tanggal 17 Oktober Tahun 2022.

Undang-undang ini ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi. Undang-undang ini terdiri dari 16 Bab dan 76 pasal.

Pada bagian ini menjelaskan istilah yang dipakai dan siapa saja yang berlaku dalam undang-undang perlindungan data pribadi. Pasal 1 mendefinisikan tentang data pribadi, perlindungan data pribadi, informasi, pengendali data pribadi, prosesor data pribadi, subjek data pribadi, setiap orang, korporasi, badan publik, organisasi internasional, pemerintah pusat yang selanjutnya disebut pemerintah.

Undang-undang ini juga berlaku untuk setiap orang, badan publik, dan organisasi internasional yang melakukan perbuatan hukum yang berada di wilayah hukum Negara Republik Indonesia dan di luar wilayah hukum Negara Republik Indonesia, yang memiliki akibat hukum di wilayah hukum Negara Republik Indonesia maupun bagi subjek data pribadi warga negara Indonesia di luar wilayah hukum Negara Republik Indonesia. Undang-undang ini tidak berlaku untuk pemrosesan data pribadi oleh orang perseorangan dalam kegiatan pribadi atau rumah tangga. Kemudian Pada BAB II undang-undang ini juga berasaskan perlindungan, kepastian hukum, kepentingan umum, kemanfaatan, kehati-hatian, keseimbangan, pertanggungjawaban, dan kerahasiaan.

Bab III Undang-undang Pelindungan Data Pribadi membagi jenis data pribadi menjadi dua yaitu, data pribadi yang bersifat spesifik dan umum. Data pribadi yang bersifat spesifik sebagaimana yang di atur dalam UU PDP ayat (1) huruf a meliputi:

- a. Data dan informasi kesehatan yaitu catatan atau kekurangan individu yang berkaitan dengan kesehatan fisik, kesehatan mental, dan/atau pelayanan kesehatan;

- b. Data biometrik yaitu data yang berkaitan dengan fisik, fisiologis, atau karakteristik perilaku individu yang memungkinkan identifikasi unik terhadap individu, seperti gambar wajah atau data daktiloskopi. Data biometric juga menjelaskan pada sifat keunikan dan/atau karakteristik seseorang yang harus dijaga dan dirawat, termasuk namun tidak terbatas pada rekam sidik jari, retina mata, dan sampel DNA;
- c. Data genetika yaitu semua data jenis apa pun mengenai karakteristik suatu individu yang diwariskan atau diperoleh selama perkembangan prenatal awal;
- d. Catatan kejahatan yaitu merupakan catatan tertulis tentang seseorang yang pernah melakukan perbuatan melawan hukum atau melanggar hukum atau sedang dalam proses peradilan atas perbuatan yang dilakukan, antaran lain catatan kepolisian dan pencatuman dalam daftar pencelakan atau penangkalan;
- e. Data anak;
- f. Data keuangan pribadi yaitu termasuk namun tidak terbatas kepada data jumlah simpanan pada bank, termasuk Tabungan, deposito, dan data kartu kredit; dan/atau
- g. Data lainnya sesuai dengan ketentuan peraturan perundang-undangan

Data pribadi yang bersifat umum sebagaimana yang diatur dalam UU PDP ayat (1) huruf b meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan; dan/atau data pribadi yang dikombinasikan untuk mengidentifikasi seseorang, yaitu data pribadi yang dikombinasikan untuk mengidentifikasi seseorang antara lain nomor telepon seluler dan IP Address.

Hak-hak terhadap subjek data pribadi diatur dalam BAB IV Undang-undang Pelindungan Data Pribadi Pasal 5, Pasal 6, Pasal 7, Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, Pasal 12, dan Pasal 13 ayat (1) dan (2). Subjek data pribadi berhak mendapatkan informasi tentang kejelasan informasi, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, dan akuntabilitas pihak yang meminta data pribadi,¹² subjek data pribadi berhak melengkapi, memperbaharui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi tentang dirinya sesuai dengan tujuan pemrosesan data pribadi,¹³ subjek data pribadi berhak mendapatkan akses dan memperoleh salinan data pribadi

tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan,¹⁴ subjek data pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan,¹⁵ subjek data pribadi berhak menarik kembali persetujuan pemrosesan data pribadi tentang dirinya yang telah diberikan kepada pengendali data pribadi,¹⁶ subjek data pribadi berhak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang hanya didasarkan pada pemrosesan secara otomatis, termasuk pemprofilan, yang menimbulkan akibat hukum atau berdampak pada subjek data pribadi,¹⁷ subjek data pribadi berhak menunda atau membatasi pemrosesan data pribadi secara proposional sesuai dengan tujuan pemrosesan data pribadi,¹⁸ subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan,¹⁹ subjek data pribadi berhak mendapatkan dan/atau menggunakan data pribadi tentang dirinya dari pengendali data pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik,²⁰ subjek data pribadi berhak menggunakan dan mengirimkan data pribadi tentang dirinya ke pengendali data lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip perlindungan data pribadi berdasarkan Undang-Undang ini.²¹

Kewajiban pengendali data pribadi dan prosesor data pribadi dalam pemrosesan data pribadi, pada Undang-Undang Pelindungan Data Pribadi pasal 19 mengatur bahwa pengendali data pribadi dan prosesor data pribadi meliputi setiap orang, badan publik, dan organisasi internasional,²² kemudian pasal 20 ayat (1) mengatur kewajiban pengendali data pribadi bahwa pengendali data pribadi wajib memiliki dasar pemrosesan data pribadi, dasar pemrosesan data pribadi sendiri meliputi:

- a. Persetujuan yang sah secara eksplisit dari subjek data pribadi untuk 1 (satu) atau beberapa tujuan tertentu yang telah

¹² Pasal 5 Undang-undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi

¹³ Pasal 6 Undang-undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi

¹⁴ *Ibid.* Pasal 7

¹⁵ *Ibid.* Pasal 8

¹⁶ *Ibid.* Pasal 9

¹⁷ *Ibid.* Pasal 10

¹⁸ *Ibid.* Pasal 11

¹⁹ *Ibid.* Pasal 12

²⁰ Pasal 13 ayat 1 Undang-undang No.27 Tahun 2022 tentang Pelindungan Data Pribadi

²¹ *Ibid.* Pasal 13 ayat 2

²² *Ibid.* Pasal 19

disampaikan oleh pengendali data pribadi kepada subjek data pribadi;

- b. Pemenuhan kewajiban perjanjian dalam hal subjek data pribadi merupakan salah satu pihak atau untuk memenuhi permintaan subjek data pribadi pada saat akan melakukan perjanjian;
- c. Pemenuhan kewajiban hukum dari pengendali data pribadi sesuai dengan ketentuan peraturan perundang-undangan
- d. Pemenuhan perlindungan kepentingan vital subjek data pribadi
- e. Pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan pengendali data pribadi berdasarkan peraturan perundang-undangan dan
- f. Pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan pengendali data pribadi dan hak subjek data pribadi.²³

Pengendali data pribadi juga wajib untuk menyampaikan informasi mengenai legalitas dari pemrosesan data pribadi, tujuan pemrosesan data pribadi, jenis dan relevansi data yang akan diproses, jangka waktu retensi dokumen yang memuat data pribadi, rincian mengenai informasi yang dikumpulkan, jangka waktu pemrosesan data pribadi, dan hak subjek data pribadi sebagaimana yang telah diatur dalam Undang-undang perlindungan data pribadi pasal 21 ayat (1). Apabila terdapat perubahan informasi sebagaimana dimaksud dalam pasal 21 ayat (1), pengendali data wajib memberitahukan kepada subjek data pribadi sebelum terjadi perubahan informasi.²⁴ Dalam melakukan pemrosesan data pribadi, pengendali data pribadi juga wajib untuk menjaga kerahasiaan data pribadi, sebagaimana diatur dalam UU PDP pasal 36,²⁵ dan wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi dibawah kendali pengendali data pribadi.²⁶

Berbicara tentang pengawasan terhadap data pribadi, tentu saja ada pejabat atau petugas yang bertanggung jawab atas hal tersebut. Pada Undang-undang PDP pasal 53 mengatur tentang pejabat atau petugas yang melaksanakan fungsi perlindungan data pribadi. Pejabat atau petugas juga mempunyai pengertian sebagai petugas yang bertanggung jawab untuk memastikan kepatuhan atas prinsip perlindungan data pribadi dan

mitigasi resiko pelanggaran perlindungan data pribadi.²⁷

Pemerintah berperan dalam penyelenggaraan perlindungan data pribadi dan dilaksanakan oleh lembaga yang ditetapkan oleh presiden dan bertanggung jawab langsung kepada presiden. Lembaga penyelenggara perlindungan data pribadi melaksanakan:

- a. Perumusan dan penetapan kebijakan dan strategi perlindungan data pribadi yang menjadi panduan bagi subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi,
- b. Pengawasan terhadap penyelenggaraan perlindungan data pribadi
- c. Penegakan hukum administratif terhadap pelanggaran UU PDP, dan
- d. Fasilitasi penyelesaian di luar pengadilan.²⁸

Lembaga penyelenggara perlindungan data pribadi juga berwenang untuk:

- a. Merumuskan dan menetapkan kebijakan di bidang perlindungan data pribadi,
- b. Melakukan pengawasan terhadap kepatuhan pengendali data pribadi,
- c. Menjatuhkan sanksi administratif atas pelanggaran perlindungan data pribadi yang dilakukan pengendali data pribadi dan/atau prosesor data pribadi,
- d. Membantu aparat penegak hukum dalam penanganan dugaan tindak pidana data pribadi sebagaimana dimaksud dalam undang-undang ini,
- e. Bekerja sama dengan lembaga perlindungan data pribadi negara lain dalam rangka penyelesaian dugaan pelanggaran perlindungan data pribadi lintas negara,
- f. Melakukan penilaian terhadap pemenuhan persyaratan transfer data pribadi ke luar wilayah hukum negara republik Indonesia,
- g. Memberikan perintah dalam rangka tindak lanjut hasil pengawasan kepada pengendali data pribadi dan/atau prosesor data pribadi,
- h. Melakukan publikasi hasil pelaksanaan pengawasan perlindungan data pribadi sesuai dengan ketentuan peraturan perundang-undangan,
- i. Menerima aduan dan/atau laporan tentang dugaan terjadinya pelanggaran perlindungan data pribadi,
- j. Melakukan pemeriksaan dan penelusuran atas pengaduan, laporan dan/atau hasil pengawasan terhadap dugaan terjadinya pelanggaran perlindungan data pribadi,

²³ Pasal 20 ayat (1) Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

²⁴ Pasal 21 ayat (1) Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

²⁵ *Ibid.* Pasal 36

²⁶ *Ibid.* Pasal 37

²⁷ *Ibid.* Pasal 53

²⁸ Pasal 59 Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

- k. Memanggil dan menghadirkan setiap orang dan/atau badan publik yang terkait dengan dugaan pelanggaran perlindungan data pribadi,
- l. Meminta keterangan, data, informasi dan dokumen dari setiap orang dan/atau badan publik terkait dugaan pelanggaran perlindungan data pribadi,
- m. Memanggil dan menghadirkan ahli yang diperlukan dalam pemeriksaan dan penelusuran terkait dugaan pelanggaran perlindungan data pribadi,
- n. Melakukan pemeriksaan dan penelusuran terhadap sistem elektronik, sarana, ruang, dan/atau tempat yang digunakan pengendali data pribadi dan/atau prosesor data pribadi, termasuk memperoleh akses terhadap data dan/atau menunjuk pihak ketiga, dan
- o. Meminta bantuan hukum kepada kejaksaan dalam penyelesaian sengketa perlindungan data pribadi.²⁹

Ada beberapa contoh organisasi dan lembaga penyelenggara perlindungan data pribadi yang ditetapkan oleh Presiden dan bertanggung jawab langsung kepada Presiden, contohnya yaitu lembaga Badan Siber dan Sandi Negara (BSSN), BSSN sendiri diresmikan oleh Presiden Joko Widodo pada 13 April 2021 ke dalam Peraturan Presiden nomor 28 tahun 2021, BSSN merupakan lembaga transformasi peleburan lembaga keamanan informasi pemerintah yang telah ada sebelumnya, yaitu Lembaga Sandi Negara (Lemsaneg) dan Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementerian Komunikasi dan Informatika (KemKominfo) sebagaimana diatur dalam Perpes nomor 53 tahun 2017 tentang BSSN yang selanjutnya disempurnakan dengan Perpres nomor 133 tahun 2017. Dengan dibentuknya BSSN, maka pelaksanaan seluruh tugas dan fungsi di bidang Persandian di Lemsaneg serta pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, dan keamanan jaringan dan infrastruktur telekomunikasi yang ada di KemKominfo dilaksanakan oleh BSSN. Terdapat juga tugas dari BSSN yaitu, melaksanakan tugas pemerintahan di bidang keamanan siber dan sandi untuk membantu Presiden dalam menyelenggarakan pemerintahan.

Terdapat juga struktur kelembagaan keamanan siber indonesia yang di bagi menjadi empat bagian³⁰, yaitu:

- a. Regulator, dalam bagian ini terdapat Direktorat Keamanan Informasi-Kominfo, IDSIRTI (Indonesia Security Incident Response Team on Internet Infrastructure)-Kominfo, Lembaga Sandi Negara.
- b. Pertahanan/militer, dalam pertahanan dan militer terdapat kementerian Pertahanan dan TNI.
- c. Penegak Hukum, yakni Polisi, Kementerian Hukum dan HAM, kejaksaan, dan pengadilan.
- d. Intelejen, terdapat BIN (Badan Intelejen Negara), dan BAIS (Badan Intelejen Strategis).

Terdapat juga larangan dan pidana perihal penggunaan data pribadi tertuang dalam pasal-pasal yaitu Pasal 65 yang berbunyi:

- a. Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.
- b. Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya.
- c. Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya.

Pengaturan pada pasal 66 ini dimaksudkan agar seseorang tidak menggunakan data diri yang bukan miliknya yang sampai dapat merugikan pemilik data orang tersebut. Terdapat juga ketentuan pidana dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi antara lain sebagai berikut yang termaktub dalam Pasal 67 yang berbunyi:

- a. Setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud menguntungkan diri sendiri atau orang lain yang mengakibatkan kerugian subjek data pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (Lima Miliar Rupiah).
- b. 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)

²⁹ Pasal 60 Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

³⁰ Indah dkk, *Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)*, Jurnal Bidang Penelitian Informatika, Vol.1, No. 1, Oktober 2022, hlm 4.

tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah).

- c. Setiap orang dengan sengaja 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 Rp. 5.000.000.000,00 (lima miliar rupiah).

Pada pasal 68 menjelaskan terkait pemalsuan data pribadi yang menimbulkan kerugian terhadap korban dan keuntungan bagi pelaku, yakni “setiap orang yang dengan sengaja membuat data pribadi palsu atau memalsukan data pribadi dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian terhadap orang lain sebagaimana dimaksud dalam Pasal 66 dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau pidana denda paling banyak Rp. 6.000.000.000,00 (enam miliar rupiah)”. Selain dipidana dengan pidana sebagaimana dimaksud pada Pasal 67, dan Pasal 68, hal ini juga dapat dipidana dengan pidana tambahan sesuai dengan pasal 69 berupa perampasan keuntungan dan/atau harta benda yang diperoleh atau hasil tindak pidana dan pembayaran ganti rugi. Hal ini selain dijatuhi pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68, jika korporasi terbukti melakukan tindak pidana, maka sanksi lebih lanjut dapat dijatuhkan kepada koperasi sesuai dengan pasal 70, yang menjelaskan keadaan dimana hukuman tambahan dapat dijatuhkan yaitu:

- a. Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 67 dan Pasal 68 dilakukan oleh korporasi, pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, dan/atau Korporasi.
- b. Pidana yang dapat dijatuhkan kepada Korporasi hanya pidana denda.
- c. Pidana denda yang dijatuhkan kepada Korporasi paling banyak 10 (sepuluh) kali dari maksimal pidana denda yang diancamkan.
- d. Selain dijatuhi pidana denda sebagaimana dimaksud pada ayat (2). Korporasi dapat dijatuhi pidana tambahan berupa:
 - 1) Perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil tindak pidana;
 - 2) Pembekuan seluruh atau sebagian usaha korporasi;
 - 3) Pelarangan permanen melakukan perbuatan tertentu;
 - 4) Penutupan seluruh atau sebagian tempat usaha dan/atau kegiatan korporasi;

- 5) Melaksanakan kewajiban yang telah dilalaikan;
- 6) Pembayaran ganti kerugian;
- 7) Pencabutan izin;
- 8) Pembubaran korporasi.

Pada proses penerapan hukum materil, hukum formil atau hukum acara juga turut andil dalam proses peradilan. Hukum acara yang baik akan berdampak baik juga pada sebuah keadilan. Mengenai kasus peretasan data pribadi atau kejahatan *hacking* data pribadi diatur dalam Pasal 71 dan Pasal 72 Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yaitu pada pasal 71 berbunyi:

- a. Dalam hal pengadilan menjatuhkan Keputusan pidana denda, terpidana diberikan waktu jangka waktu 1 (satu) bulan sejak putusan telah memperoleh kekuatan hukum yang tetap untuk membayar denda tersebut.
- b. Dalam hal terdapat alasan kuat, jangka waktu sebagaimana dimaksud dalam ayat (1) dapat diperpanjang untuk waktu paling lama 1 (satu) bulan.
- c. Dalam hal terpidana tidak membayar pidana denda dalam jangka waktu sebagaimana dimaksud pada ayat (1) atau ayat (2) maka harta kekayaan atau pendapatan terpidana dapat disita dan dilelang oleh jaksa untuk melunasi pidana denda yang tidak dibayar.
- d. Dalam hal penyitaan dan pelelangan harta kekayaan atau pendapatan sebagaimana dimaksud pada ayat (3) tidak cukup atau tidak memungkinkan untuk dilaksanakan, pidana denda yang tidak dibayar diganti dengan pidana penjara paling lama sebagaimana diancamkan untuk tindak pidana yang bersangkutan.
- e. Lamanya pidana penjara sebagaimana dimaksud pada ayat (4) yang ditentukan oleh hakim, dicantumkan dalam putusan pengadilan.

Peraturan serta lembaga penyelenggara pelindungan data pribadi yang termaktub di atas menunjukkan keseriusan dari pemerintah untuk melindungi setiap informasi data pribadi warga negara Indonesia dari ancaman-ancaman yang timbulkan oleh pihak-pihak yang tidak bertanggung jawab.

B. Perlindungan Hukum terhadap pemilik data pribadi yang mengalami kebocoran akibat tindakan peretasan

Perlindungan hukum terhadap pemilik data pribadi pada kenyataannya masih mengalami kebocoran akibat tindakan peretasan yang di sebabkan oleh pihak-pihak yang tidak bertanggungjawab atau *hacker*, seperti pada tahun

2021 terdapat kasus kebocoran data badan penyelenggara jaminan sosial (BPJS) kesehatan, dimana sekitar 279 juta data warga Indonesia termasuk mereka yang sudah meninggal dunia yang diretas dan dijual ke forum daring oleh pengguna forum berbagai data base RaidForums dengan akun bernama Kotz. Data yang diduga berasal dari BPJS Kesehatan tersebut dikonfirmasi oleh Kementerian Kominfo yang menemukan bahwa sampel data yang bocor diduga kuat identik dengan data BPJS Kesehatan. Hal tersebut didasarkan pada data nomor kartu, kode kantor, data keluarga/data tanggungan, dan status pembayaran yang identik dengan data BPJS Kesehatan. Dalam kasus ini Kementerian Kominfo melakukan pemanggilan terhadap direksi BPJS Kesehatan sebagai pengelola data pribadi yang diduga bocor untuk melakukan proses investigasi secara mendalam,³¹

Tahun 2022 terjadi juga kasus di mana seorang peretas bernama Bjorka membocorkan 3,2 Milliar data aplikasi PeduliLindungi ke publik. Adapun data yang diunggah, yaitu nama, email, nomor induk kependudukan (NIK), nomor kartu tanda penduduk (KTP), nomor telepon, tanggal lahir, identitas perangkat, status Covid-19, riwayat chek-in, riwayat pelacakan kontak, vaksinasi, dan masih banyak data lainnya. Data tersebut valid terdapat di data kependudukan saat dilakukan pengecekan menggunakan aplikasi pengecekan nomor KTP.³² Terdapat juga kebocoran data pelanggan IndiHome, Bjorka mengklaim sudah mengantongi 26 juta history browsing pelanggan IndiHome. Informasinya mencakup keyword, email, nama, jenis kelamin, dan nomor induk kependudukan atau NIK.³³

Pada bulan juli tahun 2023, Bjorka membocorkan sebanyak 34 juta data paspor. Dalam kasus ini Bjorka membagikan sampel sebanyak 1 juta data nama pengguna paspor. Data ini meliputi NIKIM (National Identiti Kartu Identitas Masyarakat), nomor paspor, tanggal pembuatan, tanggal kadaluwarsa, tanggal lahir,

dan jenis kelamin.³⁴ Bjorka juga membocorkan 1.3 miliar informasi pendaftaran SIM card yang dipunyai oleh kominfo, informasi tersebut dijual dengan harga US\$50 ribu atau sama dengan Rp743,5 Juta.³⁵ Kemudian bjorka membocorkan 105 juta informasi warga Indonesia yang akan mengikuti pemilihan umum berasal dari Komisi Pemilihan Umum (KPU), data ini di unggah oleh Bjorka pada 6 september 2022 pada forum breached. To. Informasi yang dibocorkan yaitu NIK, Kartu Keluarga, nama lengkap, tempat tanggal lahir, gender, hingga usia, dalam informasi yang dibocorkan tersebut berasal dari daerah Sulawesi Selatan serta Sulawesi Tenggara. Terbaru ini terdapat kasus data bocor sebesar 204 juta data pemilihan umum 2024 yang dicuri dari situs Komisi Pemilihan Umum dan dijual ke situ BreachForums. Data ini berisikan nama lengkap, nomor induk kependudukan, nomor kartu keluarga, nomor KTP (berisi paspor untuk pemilih di luar negeri), jenis kelamin, tanggal lahir, status pernikahan, Alamat lengkap. Serta kodefikasi tempat pemungutan suara (TPS).³⁶

Kasus kebocoran data BPJS Kesehatan dan kasus kebocoran data lainnya yang disebabkan oleh *hacker* yang bernama Bjorka, secara hukum telah melanggar Undang-undang Pelindungan Data Pribadi pasal 65, pasal 67, yang berbunyi, Pasal 65 ayat (1) "Setiap orang dilarang secara melawan hukum memperoleh atau mengumpulkan yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi."³⁷, kemudian ayat (2) "Setiap orang dilarang secara melawan hukum mengungkapkan data pribadi yang bukan miliknya."³⁸, dan ayat (3) Setiap orang dilarang secara melawan hukum menggunakan data pribadi yang bukan miliknya"³⁹. Pada pasal 67 juga menjelaskan tentang sanksi pidana dan sanksi administrasi, pada pasal 67 ayat (1) berbunyi

³¹ *BPJS Kesehatan: Data ratusan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar*, <https://www.bbc.com/indonesia/indonesia-57196905>, diakses pada tanggal 02 September 2023.

³² Andri Saubani, *CISSReC: 3,2 Miliar Data PeduliLindungi Bocor*, <https://news.republika.co.id/berita/rle9di409/cissrec-32-miliar-data-pedulilindungi-bocor>, diakses pada tanggal 10 Agustus 2023.

³³ Retia Kartika Dewi, *Penjelasan Telkom soal 26 Juta Data Pelanggan Indihome Diduga Bocor*, <https://www.kompas.com/tren/read/2022/08/22/060500065/penjelasan-telkom-soal-26-juta-data-pelanggan-indihome-diduga-bocor?page=all>, diakses pada tanggal 11 Maret 2024.

³⁴ *Sebanyak 34 juta data pemegang paspor Indonesia diduga 'bocor'*, <https://www.bbc.com/indonesia/articles/c9e7e9grjmko>, diakses pada tanggal 02 September 2023.

³⁵ CNN Indonesia, *1,3 Miliar Data Sim Card Diduga Bocor di Forum Gelap, Kominfo Bantah*, <https://www.cnnindonesia.com/teknologi/20220901122745-192-841874/13-miliar-data-sim-card-diduga-bocor-di-forum-gelap-kominfo-bantah>, di akses pada tanggal 04 Maret 2024.

³⁶ BBC News, *Ratusan Juta Data Pemilih dari Situs KPU diduga diretas, apa akibatnya?*, <https://www.bbc.com/indonesia/articles/cgxpk9k3ve5o>, diakses pada tanggal 04 Maret 2024.

³⁷ Pasal 65 ayat (1) Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

³⁸ *Ibid.* Pasal 65 ayat (2)

³⁹ *Ibid.* Pasal 65 ayat (3)

“setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain yang dapat kerugian subjek data pribadi sebagaimana dimaksud dalam pasal 65 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp. 5.000.000.000,00 (lima miliar rupiah).⁴⁰ Pada pasal 67 ayat (2) juga berbunyi “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 Rp. 4.000.000.000,00 (empat miliar rupiah).⁴¹

Hacker bukanlah salah satu pihak yang dapat disalahkan atas terjadinya *hacking* terhadap data pribadi. Pengendali data pribadi juga merupakan pihak yang bertanggungjawab atas terjadinya kasus terhadap data pribadi yang bocor karena kelalaian pengendali data pribadi dalam menjalankan kewajibannya. Pada kasus kejahatan *hacking*, berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi telah mengatur bentuk sistem pertanggungjawaban pidana kejahatan *hacking* data pribadi dan siapa saja yang dapat diminta pertanggungjawaban pidana. Menurut Undang-Undang Pelindungan Data Pribadi ada beberapa subjek yang dapat diminta pertanggungjawaban pidana, antarlain yaitu:

- a. Pengumpul, pembocor, pengguna, dan pemalsu data pribadi (*Hacking*)
- b. Pertanggungjawaban Pidana bagi pelaku Kporasi
- c. Badan publik pengendali data pribadi baik pemerintah maupun swasta

Pada pasal 35 Undang-undang pelindungan data pribadi mengatakan “pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diprosesnya dengan melakukan penyusunan dan penerapan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan, dan penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan resiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi”.⁴² Pengendali data pribadi juga wajib menjaga

kerahasiaan data pribadi dan wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi. Dalam setiap kasus yang termaktub di atas juga meupakan kelalaian pengendali data pribadi yang tidak dapat memaksimalkan proteksi terhadap data pribadi warga Indonesia, seperti pada kasus bjorka yang berulang kali meretas situs pemerintahan yang mengakibatkan kebocoran data pribadi dan data daftar pemilu rakyat Indonesia yang di perjual belikan secara ilegal didalam sebuah forum, terbaru dalam kasus yang serupa yang dilakukan oleh *hacker* yang bernama Jimbo yang telah meretas situs KPU kemudian membocorkan data pemilih dan membagikan sampel di situs BreachForums. Dalam hal ini, subjek data pribadi sesuai pasal 12 ayat (1) Undang-Undang Pelindungan Data Pibadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.⁴³ Pada kasus kebocoran DPT Pemilu 2024 telah mencapai tahap persidangan, sidang gugatan dugaan kebocoran data Daftar Pemilih Tetap (DPT) digelar dengan awalan pembacaan tuntutan penggugat yang bernama Rico Nurfriansyah Ali dengan nomor perkara 4-PKE-DKPP/I/2024. Dalam sidang tersebut terdapat tiga tuntutan yang diminta untuk dikabulkan Majelis Dewan Kehormatan Penyelenggara Pemilu (DKPP) pada sidang tersebut, yang pertama, menerima dan mengabulkan pengaduan pengadu untuk seluruhnya, yang kedua meminta DKPP unutkan menetapkan para tergugat Komisioner KPU RI sebagai pelanggar etik, dan yang ketiga merupakan pemberhentian tetap kepada tergugat.⁴⁴ Dalam kasus ini KPU telah melanggar Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi Pasal 39 ayat 1 yang berbunyi “pengendali data pribadi wajib mencegah data pribadi di akses secara tidak sah”, dan Pasal 46 ayat 1 “dalam hal terjadi kegagalan pelindungan data pribadi, pengendali data wajib menyampaikan pemberitahuan secara tertulis paling 3 x 24 jam kepada subjek data pribadi dan lembaga”.⁴⁵ Pengendali data pribadi dapat dijatuhkan sanksi administratif yang melakukan

⁴⁰ Pasal 67 ayat (1) Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

⁴¹ *Ibid.* Pasal 67 ayat (2)

⁴² Pasal 35 Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

⁴³ Pasal 12 ayat (1) Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

⁴⁴ Singgih Wiryo, *Sidang Dugaan Kebocoran DPT Pemilu 2024, DKPP Diminta Pecat Semua Komisioner KPU*, <https://nasional.kompas.com/read/2024/02/28/14581061/sidang-dugaan-kebocoran-dpt-pemilu-2024-dkpp-diminta-pecat-semua-komisioner> , diakses pada tanggal 04 Maret 2024.

⁴⁵ Pasal 46 ayat (1) Undang-undang No.27 Tahun 2022 tentang Perlindungan Data Pribadi

pelanggaran terhadap Undang-Undang Perlindungan Data Pribadi pasal 20 ayat (1), pasal 21, pasal 24, pasal 25 ayat (2), pasal 26 ayat (3), pasal 27, pasal 28, pasal 29, pasal 30, pasal 31, pasal 32 ayat (1), pasal 34 ayat (1), pasal 35, pasal 36, pasal 37, pasal 38, pasal 39 ayat (1), pasal 40 ayat (1), pasal 41 ayat (1) dan (3), pasal 42 ayat (1), pasal 43 ayat (1), pasal 44 ayat (1), pasal 45, pasal 46 ayat (1) dan ayat (3), pasal 47, pasal 48 ayat (1), pasal 49, pasal 51 ayat (1) dan ayat (5), pasal 52, pasal 53 ayat (1), pasal 55 ayat (2), dan pasal 56 ayat (2) sampai dengan ayat (4) dikenai sanksi administratif.

Sanksi administratif sebagaimana dimaksud diatas adalah berupa peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi dan/atau denda administratif. Sanksi administratif berupa denda administratif dikenakan paling tinggi 2 (dua) persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.

Undang-undang perlindungan data pribadi harus dapat di implementasikan dalam kasus-kasus yang terjadi diatas, selain pengimplementasian Undang-undang perlindungan data pribadi, pemerintah juga harus dapat meningkatkan keamanan terhadap setiap situs-situs maupun setiap aplikasi yang menyimpan semua data pribadi warga Indonesia, salah satu cara yaitu, meningkatkan kemampuan dari sang pengendali data pribadi dan prosesor data pribadi, karena pada setiap kasus yang termaktub di atas, salah satu pihak yang bertanggung jawab yaitu pengendali data pribadi dan prosesor data pribadi. Maka dari itu pemerintah Indonesia harus dapat mengimplementasikan Undang-undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi terhadap data pribadi warga Indonesia agar terhindar dari hacking yang dapat di pergunakan dengan tidak baik oleh para hacker yang tidak bertanggung jawab.

PENUTUP

A. Kesimpulan

1. Pengaturan perlindungan data pribadi pengguna teknologi informasi di Indonesia, yakni dibentuknya Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi melalui proses yang begitu panjang, dimana pada tahun 2020 telah menjadi Rancangan Undang-undang Perlindungan Data Pribadi yang dikirmkan ke DPR dan disahkan pada tanggal 17 Oktober Tahun 2022. Undang-undang yang berisikan 72 pasal ini membahas mengenai perlindungan terhadap data pribadi warga Indonesia.

2. Perlindungan hukum terhadap pemilik data pribadi yang mengalami kebocoran akibat Tindakan peretasan masih terbilang lemah karena pada kenyataan yang terjadi pada saat ini masih saja terjadi kasus hacking yang disebabkan oleh hacker yang tidak bertanggung jawab, dan juga sebabkan oleh kelalaian pengendali data pribadi dalam memproteksi data warga negara Indonesia sehingga berulang kali situs maupun aplikasi yang dibuat oleh pemerintah diretas, sehinggah berakhir dengan tindakan yang tidak bertanggung jawab, yakni dengan dijualnya secara ilegal data pribadi warga negara Indonesia dalam situs-situs dengan sengaja dan menguntungkan pihak-pihak yang tidak bertanggung jawab.

B. Saran

1. Mengsosialisasikan Undang-undang Perlindungan Data Pribadi kepada warga Indonesia agar warga Indonesia dapat mengetahui hak-hak apa saja yang dipunya dalam Undang-undang Perlindungan Data Pribadi.
2. Pengendali data pribadi dan prosesor data pribadi harus meningkatkan proteksi keamanan data pribadi dalam bidang teknologi agar tidak terjadi lagi hacking terhadap data pribadi warga Indonesia.

DAFTAR PUSTAKA

A. Buku

- Asikin, Zainal dkk. (2003). *Dasar-Dasar Hukum Perburuhan*. Jakarta: PT. RajaGrafindo Persada.
- Chazawi, Adami. (2011). *Pelajaran Hukum Pidana Bagian I*. Jakarta: Rajawali Pers.
- Gunandi, Ismu dan Jonaedi Efendi. (2014). *Cepat dan Mudah Memahami Hukum Pidana*. Jakarta: Kencana.
- Hadjon, Phlipus M. (2011). *Pengantar Hukum Administrasi Indonesia*. Yogyakarta: Gajah Mada University Press.
- Hakim, Lukman. (2020). *Asas-Asas Hukum Pidana*. Yogyakarta: Deepublish.
- Kansil, C.S.T. (1989). *Pengantar Ilmu Hukum Dan Tata Hukum Indonesia*. Jakarta: Penerbit Balai Pustaka.
- Karo Karo, Rizky .P.P. dan Teguh Prasetyo. (2020). *Pengaturan Perlindungan Data Pribadi Di Indonesia*. Bandung: Nusamedia.
- Lamintang, P.A.F dan Fransiscus Theojunior Lamintang. (2014). *Dasar-Dasar Hukum Pidana Di Indonesia* Jakarta: Sinar Grafika.

Maiyestati. (2022). *Metode Penelitian Hukum*. Padang: LPPM Universitas Bung Hatta.

Mansur, Dikdik M Arief dan Elisatris Gultom. (2005), *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditma.

Marthalia, Debby dkk. (2022). *Perlindungan Hukum Terhadap HKI*. Batam: Yayasan Cendikia Mulia Mandiri.

Maskun. (2013). *Kejahatan Siber (cyber crime)*. Jakarta: Prenada Media Group.

Mesran dkk. (2023). *Pengantar Teknologi Informasi*. Deli Serdang: Graha Mitra Edukasi.

Putra, Tomi Wicaksono dkk. (2023). *Pertanggungjawaban Pidana Terhadap Kejahatan Hacking*. Bojong Pekalongan: NEM.

Saufik, Iman. (2021). *Pengantar Teknologi Informasi*. Semarang: Yayasan Prima Agus Teknik.

Situmeang, Sahat Maruli T. (2020). *Cyber Law*. Bandung: Cakra.

Sofyan, Andi dan Nur Azizah. (2016). *Hukum Pidana*. Makassar: Pustaka Pena Press.

Wahyuni, Fitri. (2017). *Dasar-Dasar Hukum Pidana*. Tangerang: PT. Nusantara Persada Utama.

Wibowo, Sastya Hendri dkk. (2022). *Cyber Crime Di Era Digital*. Padang: PT. Global Eksekutif Teknologi.

B. Konvensi

Konvensi 108 tentang Perlindungan Individu sehubungan dengan Pemrosesan Data Pribadi secara Otomatis

C. Peraturan Perundang-Undangan

Undang-Undang Dasar 1945 Negara Republik Indonesia

Undang-Undang Nomor 39 Tahun 1999 Tentang Hak Asasi Manusia

Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan

Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

D. Jurnal

Hartono. (2014). *Hacker Dalam Perspektif Hukum Indonesia*. Jurnal Masalah-Masalah Hukum. Vol. 43 No. 1.

Hertianto, M R. (2021). *Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia*. Jurnal Kretha Partika. Vol. 43 No. 1.

I Gusti Ayu Suanti Karnadi Singgi dkk. (2020). Jurnal Konstruksi Hukum. Vol. 1 No. 2.

Indah dkk. (2022). *Peran Cyber Security Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)*. Jurnal Bidang Penelitian Informatika, Vol.1, No. 1.

Murti, H. (2005). *Cybercrime*. Jurnal Teknologi Informasi Dinamik. Vol. 10 No. 1.

Tampubulon, W S. (2016). *Upaya Perlindungan Hukum Bagi Konsumen Ditinjau Dari Undang-Undang Perlindungan Konsumen*. Jurnal Ilmiah. Vol. 04 No. 01.

E. Internet

Andri Saubani. CISSReC: 3,2 Miliar Data PeduliLindungi Bocor. <https://news.republika.co.id/berita/rle9di409/cissrec-32-miliar-data-pedulilindungi-bocor>, (diakses pada tanggal 10 Agustus 2023).

Badan Siber dan Sandi Negara, *Tentang BSSN*, <https://www.bssn.go.id/tentang-bssn/>, (diakses pada tanggal 04 maret 2024.)

BBC News, *Ratusan Juta Data Pemilih dari Situs KPU diduga diretas, apa akibatnya?*, <https://www.bbc.com/indonesia/articles/cgxp-k9k3ye5o>, (diakses pada tanggal 04 Maret 2024.)

BPJS Kesehatan: Data ratusan juta peserta diduga bocor - 'Otomatis yang dirugikan masyarakat', kata pakar, <https://www.bbc.com/indonesia/indonesia-57196905>, (diakses pada tanggal 02 September 2023.)

CNN Indonesia, 1,3 Miliar Data Sim Card Diduga Bocor di Forum Gelap, Kominfo Bantah, <https://www.cnnindonesia.com/teknologi/20220901122745-192-841874/13-miliar-data-sim-card-diduga-bocor-di-forum-gelap-kominfo-bantah>, (di akses pada tanggal 04 Maret 2024.)

Himakom, Perlindungan Data Pribadi di Era Digital, <http://himakom.student.uny.ac.id/perlindungan-data-pribadi-di-era-digital/>, (diakses pada tanggal 10 Agustus 2023).

Liputan Media, "Jual Beli Data Pribadi, BRTI; Itu melanggar Hukum, <https://aptika.kominfo.go.id/2019/05/jual-beli-data-pribadi-brti-itu-melanggar-hukum/>, (diakses pada 01 April 2024).

Novina Putri Bestari, *Data Pribadi Orang Lain Dipakai Buat Pinjam diPinjol*,

<https://www.cnbcindonesia.com/tech/20221103143919-37-384908/horor-data-pribadi-orang-lain-dipakai-buat-pinjam-di-pinjol>,
(diakses pada tanggal 01 April 2024).

Retia Kartika Dewi, Penjelasan Telkom soal 26 Juta Data Pelanggan Indihome Diduga Bocor,

<https://www.kompas.com/tren/read/2022/08/22/060500065/penjelasan-telkom-soal-26-juta-data-pelanggan-indihome-diduga-bocor?page=all>, (diakses pada tanggal 11 Maret 2024.)

Sebanyak 34 juta data pemegang paspor Indonesia diduga 'bocor',
<https://www.bbc.com/indonesia/articles/c9e7e9grjmko>, (diakses pada tanggal 02 September 2023.)

Singgih Wiryono, Sidang Dugaan Kebocoran DPT Pemilu 2024, DKKP Diminta Pecat Semua Komisioner KPU,
<https://nasional.kompas.com/read/2024/02/28/14581061/sidang-dugaan-kebocoran-dpt-pemilu-2024-dkpp-diminta-pecat-semua-komisioner>, (diakses pada tanggal 04 Maret 2024.)