JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.

Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi dalam Insiden Serangan Siber Pusat Data Nasional Sementara

Jonathan Riko Mono[1], Lewiandy[2]
[1]Fakultas Hukum, Universitas Tarumanagara, Indonesia, rikomono88@gmail.com
[2]Fakultas Hukum, Universitas Tarumanagara, Indonesia, lewiandy@fh.untar.ac.id

Corresponding Author: rikomono88@gmail.com

Abstract: *The cyber attack incident against the Temporary National Data Center which included the personal data of the public and various ministries resulted in a violation of the privacy rights of personal data subjects. The right to privacy is part of the Human Rights which have been regulated and recognized by Indonesia as stated in Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution, and therefore needs to be upheld, respected and enforced. This research aims to examine what legal protections are accommodated by Indonesian positive law in relation to the protection of personal data, especially regarding the Temporary National Data Center incident. The research will be carried out using a normative juridical method, namely a research method based on a study of regulations and related legal literature (books and journals). In simple terms, personal data protection, which is an embodiment of the right to privacy regarding information, can be seen and separated into 2 (two) major parts, namely before and after the enactment of Law Number 27 of 2022 concerning Personal Data Protection. In this case, when the Temporary National Data Center incident occurred, the Personal Data Protection Law had not yet come into effect in its entirety. Therefore, this research will explore the regulations during these two periods, determining which regulations apply and can be implemented, as well as how these regulations protect the legal interests of personal data subjects.*

Keyword: *Privacy Rights, Personal Data Protection, Cyber, Temporary National Data Center.*

Abstrak: Insiden serangan siber terhadap Pusat Data Nasional Sementara yang mencakup data pribadi masyarakat dan berbagai kementrian berdampak pada timbulnya pelanggaran terhadap hak privasi subjek data pribadi. Hak privasi merupakan bagian dari Hak Asasi Manusia yang telah diatur dan diakui oleh Indonesia sebagaimana termaktub pada Pasal 28G ayat (1) dan Pasal 28H ayat (4) UUD 1945, dan oleh karenanya perlu untuk dijunjung tinggi, dihormati, dan ditegakkan. Penelitian ini bertujuan untuk menelaah perlindungan hukum apakah yang diakomodir oleh hukum positif Indonesia dalam kaitannya dengan perlindungan data pribadi, terutama terhadap insiden Pusat Data Nasional Sementara. Penelitian akan dilakukan dengan metode yuridis normatif, yaitu metode penelitian yang didasarkan pada kajian terhadap regulasi dan literatur hukum terkait (buku maupun jurnal). Secara sederhana, perlindungan data pribadi yang merupakan pengejawantahan dari hak privasi terhadap informasi dapat dilihat dan dipisahkan dalam 2 (dua) bagian besar, yaitu sebelum dan sesudah berlakunya Undang-Undang

Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Dalam hal ini, ketika insiden Pusat Data Nasional Sementara terjadi, Undang-Undang Perlindungan Data Pribadi belum berlaku secara keseluruhan. Maka dari itu penelitian ini akan menggali regulasi pada kedua masa tersebut, mengerucutkan terkait manakah regulasi yang berlaku dan dapat diimplementasikan, serta bagaimana regulasi tersebut melindungi kepentingan hukum subjek data pribadi.

Kata Kunci: Hak Privasi, Perlindungan Data Pribadi, Siber, Pusat Data Nasional Sementara.

PENDAHULUAN

Indonesia merupakan negara hukum yang menjalankan roda pemerintahannya dengan berdasarkan pada konstitusi. Apabila kita mengacu pada hierarki hukum, maka akan ditemukan bahwa konstitusi negara (dalam hal ini UUD 1945) menempati posisi teratas, yang artinya segala regulasi yang dibuat harus merupakan perpanjangan tangan dan tidak boleh bertentangan dengan konstitusi. Dalam UUD 1945 secara eksplisit dan dalam bab tersendiri, telah diatur mengenai hak asasi manusia, yang mengatur mengenai hak-hak bersifat kodrati yang melekat pada setiap diri manusia (Nurdin, N. & Athahira, A.U., 2022), termasuk pula di dalamnya hak privasi yang diatur dalam Pasal 28G ayat (1) dan 28H ayat (4) UUD 1945.

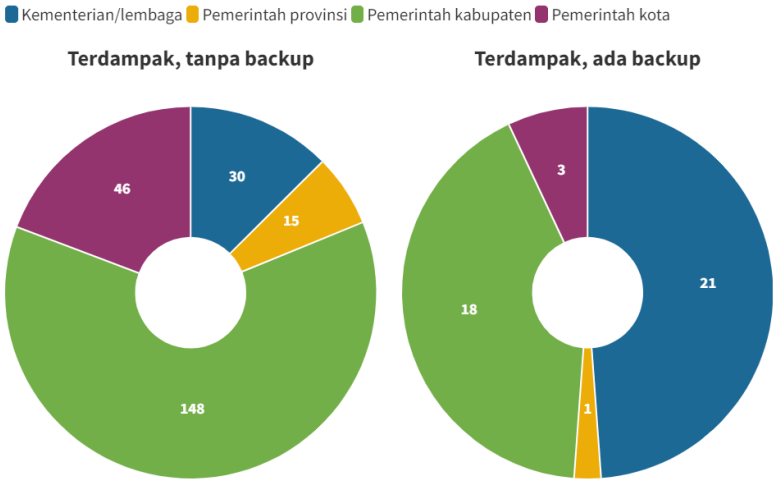
Hak privasi merupakan limitasi terhadap gangguan-gangguan yang tidak diinginkan yang memungkinkan seseorang untuk menentukan batasan tertentu dan kepada pihak mana batasan tersebut diterapkan (Cate, F.H., 2000). Privasi dapat dibagi ke dalam 4 (empat) kategori yaitu privasi terhadap informasi, terhadap anggota badan, terhadap komunikasi, dan terhadap teritori tertentu (Munir, A.B. & Yasin S.H.F., 2002). Di sisi lain, data pribadi mencakup data yang bersifat umum meliputi catatan kependudukan, seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan hingga data-data yang bersifat spesifik seperti data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan lain-lain. Hal ini menunjukkan adanya irisan dan keterkaitan antara hak privasi dengan data pribadi. Dengan diaturnya hak privasi sebagai hak asasi manusia, maka secara tidak langsung untuk mewujudkan pengamanatan dan dapat ditegakkannya hak privasi, perlu dilakukan adanya perlindungan terhadap data pribadi.

Regulasi perlindungan data pribadi di Indonesia dapat disederhanakan dan dibagi ke dalam 2 (dua) masa, yaitu masa sebelum diundangkannya Undang-Undang Perlindungan Data Pribadi dan setelah diundangkannya Undang-Undang Perlindungan Data Pribadi. Sebelum diundangkannya UU PDP, regulasi yang mengatur terkait dengan perlindungan data pribadi cenderung masih terpisah-pisah dalam berbagai regulasi sektoral, dalam artian belum ada wadah yang menghimpun dan mengintegrasikan ketentuan-ketentuan yang ada. Pemerintah sudah menunjukkan perhatian terhadap perlindungan data pribadi dengan membentuk UU PDP, namun regulasi ini belum berlaku secara keseluruhan karena diperlukannya waktu peralihan bagi pihak-pihak terkait untuk menyesuaikan diri dengan ketentuan terkini. Di sisi lain, hak-hak yang melekat pada setiap subjek data pribadi tetap harus dijunjung tinggi dan memperoleh perlindungan hukum dan tidak dapat diabaikan begitu saja.

Fakta inilah yang terjadi pada insiden serangan siber yang menguasai data nasional pada Pusat Data Nasional Sementara yang baru-baru ini menggemparkan tanah air sekaligus menunjukkan begitu rentannya pertahanan siber di Indonesia. Pusat Data Nasional Sementara adalah fasilitas sementara yang dikelola oleh Kementrian Komunikasi dan Informatika dan digunakan untuk penempatan sistem elektronik dan komponen terkait untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data yang akan digunakan untuk mengelola data pemerintah pusat dan daerah untuk digunakan secara bersama-sama dalam rangka mewujudkan program Satu Data Indonesia yang dicanangkan melalui Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, sekaligus mewujudkan Sistem

Pemerintahan Berbasis Elektronik sebagaimana diamanatkan oleh Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik sembari menunggu Pusat Data Nasional permanen siap digunakan. Secara praktis, tujuan dibangunnya Pusat Data Nasional sendiri adalah untuk meningkatkan efisiensi dalam pemanfaatan sumber daya pusat dan daerah.

Insiden penyerangan siber bermula pada 17 Juni 2024 dan dilakukan terhadap PDNS Surabaya. Penyerangan diawali dengan upaya menonaktifkan fitur keamanan yang ada dan baru mulai terasa dampaknya pada 20 Juni 2024 setelah terjadinya gangguan pada layanan imigrasi di beberapa bandara di Indonesia (Anonim, 2024). Setelah ditelaah lebih lanjut, ternyata hal tersebut terjadi karena adanya penginstalan *file* berbahaya yang diikuti dengan penghapusan *file* oleh BrainCipher yang pada akhirnya mengakibatkan sistem keamanan PDNS tidak dapat beroperasi. Serangan tersebut turut mengakibatkan data-data yang ada terenkripsi dan tersandera. Pada tanggal 26 Juni 2024 terkonfirmasi bahwa layanan instansi pemerintah yang terganggu berjumlah 282 layanan dan pihak vendor dan operator (Telkom) menyatakan bahwa data yang terdampak tidak dapat dipulihkan, kecuali apabila terdapat data cadangan (*backup*). Namun faktanya dari keseluruhan instansi yang terdampak, hanya 44 instansi yang memiliki data cadangan tersebut (Makdori, Y, 2024).



Sumber: Kementrian Komunikasi dan Informatika

Gambar 1. Instansi Terdampak Serangan

Dalam penjelasan yang diungkapkan oleh vendor dan operator PDNS pada rapat tertanggal 28 Juni 2024 di DPR RI yang menghadirkan KOMINFO, Telkom (vendor), dan Telkom Sigma (operator). Dalam pembicaraan tersebut, dapat ditarik suatu garis besar yaitu infrastruktur *backup* sudah disediakan, namun inisiatif permintaan harus diajukan oleh instansi terkait. Fakta bahwa hanya segelintir instansi yang mempunyai data cadangan menunjukkan tidak adanya rumusan peraturan yang jelas dalam upaya pengamanan data secara maksimal dan mekanisme antisipasi yang tidak terkoordinasi atau justru menunjukkan adanya ketidakpatuhan oleh instansi tertentu dalam menjalankan kewajiban yang diamanatkan oleh perundang-undangan.

Berdasarkan fakta dan latar belakang yang telah dikemukakan, meskipun peretas yang bersangkutan dalam peristiwa ini telah memberikan kode akses secara cuma-cuma kepada pemerintah, tidak berarti bahwa permasalahan yang terjadi menjadi tuntas, karena perlu ada tanggung jawab pemerintah untuk memastikan kejadian serupa tidak terulang dan bertanggung jawab untuk memulihkan data. Maka dari itu, penulis hendak melakukan penelitian ini untuk memberikan edukasi kepada masyarakat sekaligus gambaran yang komprehensif terhadap kejadian ini ditinjau dari hukum positif yang berlaku, sehingga menjadi jelas bagaimana

perlindungan hukum terhadap hak privasi subjek data pribadi menurut hukum positif Indonesia.

METODE

Jenis penelitian yang akan digunakan adalah penelitian normatif yang didasarkan pada kajian terhadap teori-teori hukum dan peraturan perundang-undangan yang berkaitan dengan topik yang dibahas (ND, M.F & Achmad, Y., 2017). Penelitian akan dilakukan dengan mendalami kejadian faktual yang terjadi dari sudut pandang hukum guna menemukan jawaban terhadap pokok permasalahan dan mendapatkan pengertian dan gambaran yang menyeluruh.

Pengumpulan data akan dilakukan melalui studi kepustakaan dengan memanfaatkan sumber hukum yang bertalian dengan topik yang dikaji, yakni bahan hukum primer berupa peraturan perundang-undangan dari tingkat tertinggi hingga tingkat terendah dan bahan hukum sekunder seperti buku, jurnal hukum, surat kabar, internet, dll.

Penelitian ini menggunakan pendekatan undang-undang (*statute approach*), yaitu pendekatan yang dilakukan dengan menelaah dan menganalisis seluruh regulasi yang berkaitan dengan permasalahan yang ditarik sebagai rumusan masalah (Marzuki, P.M., 2022).

Analisis data akan dilakukan dengan menyelaraskannya pada pendapat ahli, teori hukum, maupun kajian-kajian hukum terdahulu (bahan hukum sekunder), sehingga akan diperoleh suatu argumentasi yang tepat dalam menyikapi persoalan yang terjadi.

HASIL DAN PEMBAHASAN

Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi Menurut Hukum Positif di Indonesia

Sebagai bentuk pengamanatan hak privasi subjek data pribadi, telah dirumuskan sejumlah ketentuan untuk melindungi data pribadi. Pengaturan sebelum adanya Undang-Undang Perlindungan Data Pribadi masih cenderung terpisah-pisah dalam berbagai peraturan tingkat sektoral. Berikut merupakan substansi yang diatur dalam regulasi tersebut.

a) Undang-Undang tentang Administrasi Kependudukan

Undang-Undang Administrasi Kependudukan mengatur mengenai data kependudukan sebagai hasil dari pendaftaran penduduk dan catatan sipil. Pengelolaan data kependudukan ini berada di bawah Kementrian Dalam Negeri, yang mencakup data perseorangan dan data agregat.

Data perseorangan meliputi Nomor Kartu Keluarga, Nomor Induk Kependudukan, Nama lengkap, Jenis Kelamin, Tempat dan Tanggal Lahir, Golongan Darah, Agama, Status Perkawinan, status dalam keluarga, cacat yang dialami (fisik maupun mental), jenjang pendidikan terakhir, data orang tua dari perorangan tersebut (data diri maupun bukti perkawinan dan/atau perceraian), hingga data biometrik (sidik jari dan iris mata), dan hal-hal lain yang merupakan rahasia seseorang.

Di sisi lain, data agregat dapat diartikan sebagai kumpulan dari data-data perseorangan yang merupakan himpunan data yang berkaitan dengan peristiwa-peristiwa kependudukan (seperti pergantian alamat), peristiwa penting (seperti kelahiran, kematian, perkawinan, perceraian, perubahan status kewarganegaraan, dll.), data kelompok yang digolongkan berdasarkan cakupan jenis kelamin, usia, agama, pendidikan, maupun pekerjaan baik yang sifatnya kualitatif maupun kuantitatif.

Lebih lanjut, diatur pula mengenai data pribadi yang termasuk dalam bagian data perseorangan yang harus disimpan, dirawat, dijaga kerahasiaannya, serta dilindungi oleh negara. Di antara banyaknya data kependudukan, diatur data pribadi yang wajib untuk dilindungi, meliputi keterangan tentang cacat fisik dan/atau mental;

sidik jari; iris mata; tanda tangan; dan elemen data lainnya yang merupakan aib seseorang.

Secara garis besar, Undang-Undang Administrasi Kependudukan hanya mengatur kewajiban pemerintah untuk melindungi data pribadi dan menjaga kerahasiaannya, tanpa mengatur lebih lanjut terkait bagaimana perlindungan tersebut diimplementasikan dan pertanggungjawaban pemerintah dalam hal data yang dikelolanya terekspos ke pihak yang tidak seharusnya.

b) Undang-Undang tentang Informasi dan Transaksi Elektronik

Data Pribadi yang diatur dalam UU ITE adalah data elektronik. Diatur bahwa untuk menggunakan informasi melalui media elektronik yang melibatkan data pribadi, pihak tersebut harus mendapatkan persetujuan dari pemilik data pribadi yang bersangkutan terlebih dahulu. Hal ini merupakan wujud untuk menjamin hak privasi subjek data pribadi untuk hidup bebas dari gangguan, berkomunikasi tanpa dimata-matai, dan hak untuk mengawasi akses terhadap informasi mengenai dirinya. Terhadap pelanggaran hak privasinya, pihak yang bersangkutan dapat mengajukan gugatan atas kerugian yang mereka alami.

UU ITE juga mengatur mengenai kewajiban pemerintah untuk menetapkan instansi atau institusi yang menguasai data elektronik strategis dan harus dilindungi. Bagi instansi atau institusi yang ditetapkan, mereka diwajibkan untuk membuat rekam cadang (*backup*) terhadap data-data yang dikelolanya serta mengaitkannya ke pusat data untuk memastikan keamanan data. Sedangkan bagi intansi atau institusi lain yang tidak ditetapkan oleh pemerintah, cukup melakukan pengamanan data sesuai dengan keperluannya masing-masing.

c) Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik

Peraturan Pemerintah ini mengatur mengenai ruang lingkup Penyelenggara Sistem Elektronik berikut dengan kewajibannya, pengawasan penyelenggaraan Sistem Elektronik, peran pemerintah dalam penyelenggaraan Sistem dan Transaksi Elektronik, sanksi administratif, dan lain sebagainya.

Penyelenggaraan Sistem Elektronik dilaksanakan oleh Penyelenggara Sistem Elektronik baik dalam lingkup publik maupun pada lingkup privat. Adapun yang termasuk ke dalam kategori Penyelenggara Sistem Elektronik Lingkup Publik meliputi instansi penyelenggara negara dan/atau institusi lain yang ditunjuk untuk menyelenggarakan sistem elektronik untuk dan atas nama penyelenggara negara. PP ini mewajibkan Penyelenggara Sistem Elektronik tersebut untuk menerapkan manajemen resiko untuk mengantisipasi kerusakan atau kerugian yang berpotensi terjadi.

Untuk memproses data pribadi, Penyelenggara tidak wajib meminta persetujuan terlebih dahulu dari subjek data terkait sepanjang apa yang dilakukannya didasari oleh ketentuan peraturan perundang-undangan dan/atau sebagai wujud pengimplementasian kewajibannya dalam rangka pelayanan publik bagi kepentingan umum.

Dalam hal penyelenggara gagal melindungi data pribadi yang mereka kelola, mereka diwajibkan untuk melakukan pemberitahuan tertulis kepada pemilik data yang bersangkutan. Untuk mencegah kegagalan tersebut berdampak semakin luas, penyelenggara lingkup publik wajib mempunyai rencana untuk menanggulangi gangguan atau ancaman yang akan datang. Dalam hal Penyelenggara Lingkup Publik menggunakan layanan pihak ketiga, harus dilakukan suatu pengelompokkan data berdasarkan tingkat risiko yang ditimbulkan.

Penyelenggara harus mempunyai standarisasi, prosedur, dan sistem keamanan dalam menjalankan kegiatannya untuk meminimalisir kemungkinan gangguan, kegagalan, dan kerugian. Dalam hal kegagalan atau gangguan terjadi dan mengakibatkan dampak yang serius karena adanya tindakan pihak lain, penyelenggara diwajibkan untuk mengamankan informasi dan dokumen elektronik yang dikelolanya dan segera melapor pada penegak hukum, kementrian, atau lembaga terkait.

Untuk menjamin keandal sistem elektroniknya, penyelenggara turut diwajibkan untuk melakukan uji kelayakan terhadap seluruh maupun sebagian komponen dalam sistem elektroniknya.

PP ini mengatur lebih lanjut terkait dengan peran pemerintah, yang salah satunya mencakup penetapan instansi atau institusi yang memiliki data elektronik strategis dan wajib diproteksi sebagaimana diatur pada UU ITE, antara lain sektor administrasi pemerintahan, energi, sumber daya mineral, transportasi, keuangan, kesehatan, teknologi informasi dan komunikasi, pangan, pertahanan, dll.

Lain dari itu, pemerintah juga berperan untuk melindungi kepentingan umum dari gangguan yang mungkin terjadi, yaitu dengan menetapkan strategi keamanan siber nasional, mengatur perlindungan terhadap infrastruktur vital berikut dengan manajemen risikonya, menyelenggarakan pengamanan dan penanganan insiden, dll.

Untuk menjamin ditegakkannya regulasi tersebut, diatur pula ketentuan mengenai sanksi administratif berupa teguran tertulis, denda administratif, penghentian sementara, pemutusan akses, dan/atau dikeluarkan dari daftar.

d) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik

Perlindungan Data Pribadi dalam Sistem Elektronik yang diatur pada Permenkominfo ini mencakup bagaimana data pribadi diperoleh, dikumpulkan, diolah, dianalisis, disimpan, ditampilkan, diumumkan, disebarluaskan, dan dimusnahkan.

Peraturan Menteri ini mewajibkan setiap Penyelenggara Sistem Elektronik untuk mempunyai aturan internal perlindungan data pribadi sebagai bentuk antisipasi terhadap ketidakberhasilan melindungi data pribadi yang dikelolanya. Selain itu, sebagai bentuk pencegahan, penyelenggara diwajibkan untuk mengadakan pelatihan pencegahan perlindungan data pribadi dan melakukan edukasi yang bersifat meningkatkan kesadaran sumber daya manusia.

Peraturan Menteri ini juga mengatur terkait dengan hak pemilik data pribadi seperti kerahasiaan terhadap data pribadinya dan hak untuk mengajukan pengaduan terhadap kegagalan penyelenggara dalam melindungi kerahasiaan datanya itu. Pengaduan tersebut dapat diajukan kepada Menteri Komunikasi dan Informatika apabila kegagalan perlindungan data pribadi tidak diberitahukan secara tertulis atau mengakibatkan kerugian bagi pemilik data pribadi.

Pemberitahuan wajib dilakukan kepada pemilik data pribadi dalam hal terjadi suatu kegagalan perlindungan paling lambat 14 hari sejak diketahuinya kegagalan tersebut berikut dengan alasan mengapa hal tersebut bisa terjadi. Pemberitahuan sebagaimana tersebut di atas harus dilakukan secara tertulis kecuali dalam kondisi dimana pemilik data pribadi yang bersangkutan telah menyetujui untuk diberitahu melalui sistem elektronik apabila terjadi kegagalan perlindungan pada saat mereka menyerahkan data pribadinya. Penyelenggara Sistem Elektronik juga harus memastikan bahwa pemberitahuan tersebut telah diterima oleh Pemilik Data Pribadi yang datanya terekspos, apabila kegagalan perlindungan data tersebut berpotensi menimbulkan kerugian bagi yang bersangkutan.

Sejatinya regulasi yang mengatur terkait dengan perlindungan hukum bagi subjek/pemilik data pribadi sudah cukup kompleks bahkan sebelum adanya UU PDP. Namun, perlu dilihat kembali apakah terdapat ketentuan yang bertentangan atau berbeda dengan pengaturan yang ada pada UU PDP.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi merupakan bentuk perhatian serius pemerintah dalam menegakkan perlindungan hak privasi dan data pribadi di Indonesia. Dengan regulasi ini, pengaturan mengenai Perlindungan Data Pribadi yang sebelumnya terpisah-pisah menjadi terintegrasi pada 1 (satu) sumber, sehingga pelaksanaan perlindungan data pribadi pun diharapkan dapat semakin meningkat dan efektif.

UU PDP mengklasifikasikan Data Pribadi ke dalam 2 (dua) bagian, yaitu data pribadi yang bersifat spesifik (seperti data dan informasi kesehatan, biometrik, genetika, catatan kejahatan, data anak, dan data keuangan pribadi) dan data pribadi yang bersifat umum (seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan status perkawinan). Undang-Undang ini mengatur mengenai hak subjek data pribadi untuk mengetahui apa tujuan pemrosesan data pribadinya dilakukan, hak untuk memperbaiki kesalahan data pribadi tentang dirinya, dan lain sebagainya. Dalam Pasal 12 disebutkan bahwa subjek data pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya.

Pihak yang mengelola data pribadi, terbagi ke dalam 2 kategori, yaitu pengendali data pribadi (pihak yang menentukan tujuan kendali data dan mengelola data tersebut) dan prosesor data pribadi (pihak yang memproses data pribadi bagi pengendali yang menunjuknya) yang terbagi mencakup orang, badan publik, dan organisasi internasional. Pemrosesan data pribadi tidak hanya dapat dilakukan jika ada persetujuan eksplisit dari subjek data pribadi, tetapi dapat dilakukan dengan berlandaskan pada wewenang yang ditentukan oleh perundang-undangan sebagai rangka pelayanan publik. Hal ini mengartikan bahwa suatu badan publik (lembaga yang tugas pokoknya berkaitan dengan penyelenggaraan negara) dapat melakukan pemrosesan data dengan didasari oleh kewenangannya sebagai lembaga sebagaimana diamanatkan oleh perundang-undangan tanpa perlu meminta persetujuan langsung dari subjek data pribadi yang bersangkutan.

Dalam memproses data pribadi, Pengendali wajib memperhitungkan resiko, salah satunya apabila pengendalian data dilakukan dalam skala besar. Sebagai langkah pengamanan, Pengendali diwajibkan untuk memproteksi dan menjamin data yang berada di bawah kendalinya aman dengan merumuskan dan mengimplementasikan langkah teknis yang dilakukan sebagai wujud perlindungan terhadap potensi gangguan.

Pengendali wajib melindungi data pribadi yang dikelolanya dari pemrosesan yang tidak sah serta mencegah data tersebut diakses oleh pihak yang tidak seharusnya dengan cara yang ilegal. Pencegahan tersebut dilakukan dengan menerapkan sistem keamanan yang andal, aman, dan bertanggung jawab. Ketentuan yang berkaitan dengan kurun waktu harus dilakukannya pemberitahuan dipersingkat menjadi paling lama 72 jam (3 hari). Selain melakukan pemberitahuan kepada subjek data pribadi, pengendali data pribadi juga harus memberitahu lembaga yang bergerak dalam bidang perlindungan data pribadi. Adapun cakupan substansi yang harus dimuat dalam notifikasi tersebut berupa apa, kapan, dan bagaimana data pribadi yang bersangkutan dapat terekspos, berikut dengan upaya penanganan dan pemulihannya. Dalam Pasal 47 disebutkan secara eksplisit bahwa “Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Pelindungan Data Pribadi”.

Pentransferan data pribadi baik yang berada dalam wilayah hukum Negara Republik Indonesia (dalam negeri) maupun pentransferan ke luar negeri juga menjadi materi yang diatur dalam undang-undang ini. Pada bagian lainnya, diatur pula sanksi administratif yang akan dijatuhkan oleh lembaga baru yang bergerak khusus di bidang perlindungan data pribadi sebagaimana diamanatkan pembentukannya oleh UU ini. Lembaga tersebut bertanggung jawab

kepada presiden dan akan melaksanakan perumusan dan penetapan strategi perlindungan data pribadi, melakukan fungsi pengawasan terhadap perlindungan data pribadi, menegakkan hukum administratif, dan menyelesaikan sengeketa di luar pengadilan.

Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi dalam Insiden Serangan Siber Pusat Data Nasional Sementara

Dalam rangka mewujudkan Sistem Pemerintahan Berbasis Elektronik, dibentuklah infrastruktur penunjang, yaitu Pusat Data Nasional, Jaringan Intra Pemerintah, dan Sistem Penghubung Layanan Pemerintah. Dalam penelitian ini, kita akan secara spesifik membatasi pembicaraan pada Pusat Data Nasional. Pada dasarnya Pusat Data Nasional adalah pusat data yang digunakan secara bagi pakai oleh pemerintah pusat dan daerah yang saling terhubung. Pusat Data Nasional ini diselenggarakan oleh Kementrian Komunikasi dan Informatika. Sembari menunggu Pusat Data Nasional yang ada di Cikarang, Batam, dan Ibukota Nusantara siap untuk digunakan, dibentuklah fasilitas sementara untuk mengelola data nasional yaitu Pusat Data Nasional Sementara.

Serangan siber terhadap Pusat Data Nasional Sementara perlu mendapatkan perhatian serius dari pemerintah. Di sisi lain masyarakat pun harus mengetahui betul apa saja hak-haknya dan bagaimana hukum positif melindungi data pribadinya. Ketidakpastian mengenai regulasi manakah yang berlaku pada saat insiden ini-lah yang menjadi hal yang menarik untuk dikaji dan perlu diluruskan. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi diundangkan dan dinyatakan berlaku pada 17 Oktober 2022. Tetapi jika kita cermati rumusan pasal yang terkandung dalam undang-undang tersebut, kita akan menemukan bahwa sejumlah ketentuan tidak dapat digunakan seketika itu juga, karena diperlukannya waktu penyesuaian bagi lembaga-lembaga terkait (paling lama 2 tahun), terlebih lagi karena syarat-syarat yang mengatur ketentuan lebih lanjut pada UU PDP, perlu mengacu pada Peraturan Pelaksananya (Peraturan Pemerintah dan Peraturan Presiden) yang mana belum tersedia ketika insiden PDNS terjadi (Juni 2024). Dalam ketentuan peralihan UU PDP, dapat digarisbawahi bahwa regulasi yang ada sebelum UU PDP dinyatakan tetap berlaku selama tidak bertentangan dengan UU PDP.

Oleh karenanya, penulis akan mengklasifikasikan manakah ketentuan pada UU PDP yang sudah berlaku pada saat insiden PDNS terjadi dan mencantumkan bagaimana hukum positif melindungi hak privasi subjek data pribadi yang terdampak oleh serangan siber pada PDNS.

UU ITE menyatakan bahwa subjek data pribadi dapat mengajukan gugatan atas kerugian yang timbul karena adanya penggunaan informasi yang berkaitan dengan data pribadi elektroniknya. Pada ketentuan tersebut, dicantumkan bahwa penggunaan data pribadi seseorang harus mendapatkan persetujuan dari yang bersangkutan. Pada PP 71/2019 dan UU PDP, persetujuan subjek data pribadi bukanlah satu-satunya dasar untuk menggunakan dan/atau memproses data pribadi seseorang. Pemrosesan dapat dilakukan tanpa persetujuan subjek data pribadi selama tindakan pengendali data pribadi didasari oleh ketentuan perundang-undangan dan dalam rangka kepentingan umum dan pelayanan publik. Dalam hal ini, pemrosesan data yang dilakukan oleh KOMINFO selaku pengendali data pribadi dari PDNS berdasar karena merupakan perpanjangan tangan untuk mewujudkan program Satu Data Indonesia dan Sistem Pemerintahan Berbasis Elektronik.

PP 71/2019 mewajibkan Penyelenggara Sistem Elektronik untuk menyelenggarakan Sistem Elektronik secara andal, aman, serta bertanggung jawab dengan menerapkan manajemen risiko terhadap kerusakan atau kerugian yang mungkin timbul. Hal ini serupa dengan pengaturan pada UU PDP yang mewajibkan Pengendali Data Pribadi untuk melindungi data pribadi dari pemrosesan yang tidak sah dan mencegah data pribadi diakses secara tidak sah. Pencegahan tersebut dilakukan dengan menggunakan sistem keamanan yang andal, aman,

dan bertanggung jawab. PP 71/2019 telah mewajibkan adanya suatu sistem pengamanan berupa tata cara, sistem pencegahan, dan penanggulangan gangguan.

PP 71/2019 sudah mengatur kewajiban notifikasi kepada pemilik Data Pribadi yang datanya gagal untuk dilindungi dan memiliki rencana penanggulangan gangguan atau bencana. Terhadap kegagalan atau gangguan yang diakibatkan oleh pihak lain (termasuk di dalamnya hacker), Penyelenggara Sistem Elektronik diwajibkan untuk mengamankan Informasi Elektronik dan/atau Dokumen Elektroniknya.

PP ini menetapkan sektor mana saja yang mengelola data elektronik strategis. Apabila kita menyelaraskan hal ini dengan pengaturan yang ada pada Peraturan Presiden 95/2018 tentang Sistem Pemerintahan Berbasis Elektronik, hanya diatur bahwa setiap instansi pusat dan daerah harus menggunakan Pusat Data Nasional. Namun tidak ada ketentuan yang mewajibkan instansi pemerintah ini untuk melakukan rekam cadang elektronik. Hal ini tentunya tidak sejalan dengan ketentuan baru UU PDP yang menyatakan bahwa Pengendali Data Pribadi harus melakukan penilaian risiko dalam melakukan pemrosesan data pribadi. Dalam hal ini, Pusat Data Nasional menghimpun data dengan skala yang sangat besar dan untuk itu pemerintah seharusnya tahu bahwa risiko yang ada pun sangat tinggi. Seharusnya, pengendali data pribadi PDNS melakukan upaya pengamanan secara maksimal sebelum membentuk fasilitas yang ada dengan mewajibkan seluruh instansi pemerintah yang memasukkan datanya pada PDNS untuk memiliki rekam cadang.

Di sisi lain Permenkominfo mengatur kewajiban Penyelenggara Sistem Elektronik untuk mempunyai aturan internal perlindungan data pribadi dan peningkatan kesadaran sumber daya manusia dengan pengadaan pelatihan untuk menjamin perlindungan data pribadi berhasil dilakukan. Selain itu, diatur pula mekanisme pengaduan yang dapat disampaikan kepada Menteri Komunikasi dan Informatika. Namun, dalam kasus ini pihak yang berkepentingan atau pihak yang seharusnya bertanggungjawab atas insiden siber ini adalah KOMINFO, sehingga upaya pengaduan kepada menteri ini tidak akan berjalan efisien.

UU PDP menyatakan bahwa Pengendali Data Pribadi wajib bertanggung jawab atas pemrosesan Data Pribadi dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban pelaksanaan prinsip Pelindungan Data Pribadi. Untuk itu, ketika terjadi suatu kebocoran data, maka Pengendali Data Pribadi harus menanggung segala akibat yang ditimbulkan. Terhadap pelanggaran apabila pengendali data pribadi tidak menunjukkan adanya tanggung jawab, dapat dijatuhkan sanksi administratif oleh lembaga perlindungan data pribadi. Namun, sebagaimana telah dijelaskan pada bagian sebelumnya, ketentuan ini belum dapat diimplementasikan karena belum dibentuknya lembaga terkait. Selain daripada kelembagaan dan sanksi administratif, ketentuan dalam UU PDP dapat dinyatakan sudah berlaku, namun tidak memiliki konsekuensi hukum yang dapat dikenakan sanksi karena banyak ketentuan harus menunggu pengaturan lebih lanjut dari peraturan pelaksana untuk dapat diimplementasikan secara efektif dan jelas. Sebagai contoh, Pasal 12 UU PDP menyatakan bahwa subjek data pribadi dapat menggugat dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi tentang dirinya. Tetapi ketentuan mengenai kriteria suatu tindakan dapat dikategorikan pelanggaran harus menilik pada ketentuan yang akan diatur pada Peraturan Pemerintah (belum tersedia pada saat insiden PDNS terjadi), sehingga gugatan yang diajukan oleh subjek data pribadi nantinya akan sia-sia karena tidak berlandaskan oleh suatu ketentuan yang terang-benderang. UU PDP dapat dinyatakan efektif berlaku secara menyeluruh hanya untuk ketentuan pidananya saja karena pengaturannya yang sudah jelas (tidak perlu menunggu aturan pelaksana).

Lain dari pada itu, apabila kita membicarakan terkait dengan sanksi administratif, ini tidak akan berdampak signifikan dan merubah banyak hal apabila diterapkan terhadap pengendali data pribadi yang menyangkut kepentingan masyarakat luas (dalam hal ini Kementrian Komunikasi dan Informatika). Peneliti tidak memandang bahwa sanksi administratif merupakan solusi yang optimal. Hal ini dikarenakan sejumlah sanksi

administratif tidak akan mungkin dapat diterapkan dalam konteks KOMINFO dan pengelolaan data publik. Sekalipun KOMINFO melakukan pelanggaran dengan tidak mematuhi regulasi yang ada, tidak mungkin dilakukan penghentian sementara pemrosesan data pribadi dan/atau penghapusan dan pemusnahan data pribadi, karena menimbang aktivitas pelayanan publik yang harus tetap dijalankan.

Semangat perlindungan hak privasi subjek data pribadi patut diapresiasi, tetapi tidak dengan pengimplementasiannya. Banyak hal yang dapat diperbaiki ke depannya, sehingga subjek data pribadi dapat menegakkan haknya secara efektif dan maksimal, di antaranya dengan perumusan sanksi pendisiplinan bagi pegawai yang bekerja pada instansi pemerintahan (seperti mutasi jabatan, pemberhentian tidak dengan hormat, dll.) Selain itu, penulis memandang terlalu sulit bagi subjek data pribadi untuk membuktikan bahwa dirinya telah dirugikan oleh suatu tindakan pengendali data pribadi karena adanya kesenjangan kedudukan. Oleh karena itu, selain dari pada perumusan ketentuan yang memberikan subjek data pribadi hak untuk menggugat, perlu kiranya diatur secara eksplisit dalam undang-undang bahwa beban pembuktian berada pada sisi pengendali data pribadi dan/atau adanya tanggung jawab mutlak, sehingga dengan terjadinya suatu insiden siber, pengendali data pribadi yang bersangkutan dapat dinyatakan bertanggung jawab penuh, tidak hanya terhadap pemulihan data tetapi berikut dengan pemberian kompensasi kepada subjek data pribadi yang terdampak. Karena dengan tanggung jawab mutlak inilah, pengendali data pribadi dapat secara otomatis memperketat celah dan melakukan pengamanan yang maksimal terhadap data yang diprosesnya.

KESIMPULAN

Pembentukan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menunjukkan semangat pemerintah dalam memperjelas regulasi yang berkaitan dengan Perlindungan Data di Indonesia. Ketentuan dan gebrakan baru terkait dengan pembentukan lembaga yang akan melakukan fungsi pengawasan, menerima aduan dari masyarakat, menjadi fasilitas penyelesaian sengketa di luar pengadilan patut untuk diapreasiasi. Selain itu, dirumuskannya kewajiban pengendali data pribadi dan/atau prosesor data pribadi untuk menunjuk pejabat atau petugas yang melaksanakan fungsi perlindungan data pribadi sebagaimana diamanatkan oleh UU PDP juga patut dihargai.

Namun sayangnya, peraturan ini tidak dapat dijadikan dasar pijakan yang kokoh bagi subjek data pribadi dalam masa peralihan (dalam hal ini oleh subjek data pribadi yang datanya terdampak oleh insiden siber pada Pusat Data Nasional Sementara) dikarenakan belum siapnya peraturan pelaksana dan belum dibentuknya kelembagaan yang bergerak di bidang perlindungan data pribadi, sehingga sanksi administratif pun belum dapat dikenakan kepada pelanggar hak subjek data pribadi dengan menggunakan regulasi terkini (UU PDP). Satu-satunya bentuk perlindungan yang berkonsekuensi hukum untuk menegakkan hak subjek data pribadi adalah dengan pengajuan gugatan atas kerugian. Namun dengan regulasi yang ada saat ini, posisi subjek data pribadi cenderung sangat lemah dalam upaya menegakkan hak-haknya, hal ini terjadi karena adanya perbedaan kedudukan antar pihak. Kecil kemungkinan subjek data pribadi dapat mengetahui secara detail operasional dan kejadian yang terjadi pada sistem internal pengendali data pribadi karena adanya kerahasiaan. Hal ini berimbas pada kemungkinan ditolaknya gugatan subjek data pribadi dikarenakan minimnya bukti. Maka dari itu, sudah seharusnya dirumuskan secara tertulis bahwa beban pembuktian terhadap terjadinya kerugian berada pada diri pengendali data pribadi atau bahkan perlu diterapkan tanggung jawab mutlak.

REFERENSI

Buku

Marzuki, P.M. (2022). *Penelitian Hukum Edisi Revisi*, Cetakan ke-17. Jakarta. Kencana Prenadamedia Group, 2022.

Munir, A.B. & Yasin S.H.F. (2002). *Privacy and Data Protection*. Malaysia. Sweet & Mawell Asia.

ND, M.F & Achmad, Y. (2017). *Dualisme Penelitian Hukum Normatif & Empiris*, Cetakan ke-4. Yogyakarta. Pustaka Pelajar.

Nurdin, N. & Athahira, A.U. (2022). *HAM, Gender Dan Demokrasi (Sebuah Tinjauan Teoritis Dan Praktis)*. Jatinangor. CV Sketsa Media.

Jurnal

Cate, F. H. (2000). Principles of Internet Privacy. *Connecticut Law Review*, 32 (3), 877-896.

Internet

Anonim. (2024, Juni 27). Pusat Data Nasional Sementara Lumpuh Akibat Ransomware, Mengapa Instansi Pemerintah Masih Rentan terhadap Serangan Siber? *BBC.com*. https://www.bbc.com/indonesia/articles/cxee2985jrvo, diakses pada tanggal 8 Oktober 2024, pukul 19:25 WIB.

Hardiansyah, Z. (2024, Juli 10). Kronologi Serangan Ransomware Ke PDN Dan Penanganannya Yang Tak Kunjung Usai. *Kompas.com*. https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai, diakses pada tanggal 8 Oktober 2024, pukul 19:51 WIB.

Makdori, Y. (2024, Juni 27). Dari 282 Instansi yang Terdampak Peretasan PDNS, Hanya 44 yang Punya Backup. *Asumsi*. https://asumsi.co/post/93028/dari-282-instansi-yang-terdampak-peretasan-pdns-hanya-44-yang-punya-back-up/, diakses pada tanggal 8 Oktober 2024, pukul 19:55 WIB.

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Indonesia.

Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Indonesia.

Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan. Indonesia.

Undang-Undang Republik Indonesia Nomor 8 Tahun 2011 tentang Informasi dan Transaksi Elektronik. Indonesia.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Indonesia.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Indonesia.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Indonesia.

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Indonesia.

Peraturan Presiden Republik Indonesia Nomor 39 Tahun 2019 tentang Satu Data Indonesia

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

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