

Volume 12 Nomor 2 September 2025

Jurnal Jendela Hukum

<https://www.ejournalwiraraja.com/index.php/FH>

P-ISSN : 2355-5831, E-ISSN : 2355-9934

PERLINDUNGAN HUKUM BAGI KORBAN ATAS KEBOCORAN PUSAT DATA NASIONAL SEMENTARA (PDNs) PERSPEKTIF PERLINDUNGAN DATA PRIBADI

Slamet Mahfud Chushairi.¹ Abshoril Fithry.² Rusfandi.³

^{1,2,3} Universitas Wiraraja Madura

amoxkenari@gmail.com,¹ abshorilfithry@wiraraja.ac.id,² rusfandi@wiraraja.ac.id,³

Abstract

The advancement of information technology has accelerated the digitalization of data across various sectors, including government institutions. However, this digital transformation also increases the risk of violations against citizens' privacy rights, particularly through personal data breaches. The data breach incident involving the Temporary National Data Center (PDNs) in 2023 serves as a real example of the state's weak data governance, which directly impacts the legal protection of affected individuals. This research aims to analyze the urgency of legal regulation for victims of data breaches from the perspective of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), as well as to elaborate on the legal consequences of such violations. This study employs a normative juridical method with a statutory and case approach. The findings reveal that although the PDP Law regulates the rights of data subjects—including the right to information, breach notification, and compensation—the implementation in the PDNs case remains inadequate. The government, as a data controller, failed to transparently notify victims and has not provided sufficient legal remedies. Furthermore, the absence of the Personal Data Protection Authority (PDPA) has resulted in a lack of supervision and enforcement. The legal consequences for violations by state institutions are ineffective, despite the PDP Law providing for administrative, civil, and even criminal sanctions.

Keywords: Personal Data Protection. PDNs. PDP Law.

Abstrak

Perkembangan teknologi informasi telah mendorong digitalisasi data secara masif di berbagai sektor, termasuk sektor pemerintahan. Namun, digitalisasi tersebut juga meningkatkan risiko pelanggaran terhadap hak privasi warga negara, salah satunya melalui kebocoran data pribadi. Insiden kebocoran yang menimpa Pusat Data Nasional Sementara (PDNs) pada tahun 2024 menjadi contoh nyata lemahnya tata kelola data oleh negara, yang berdampak langsung terhadap perlindungan hukum bagi para korban. Penelitian ini bertujuan untuk menganalisis urgensi pengaturan hukum bagi korban kebocoran data dalam perspektif Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), serta menggambarkan konsekuensi yuridis atas pelanggaran tersebut. Penelitian ini menggunakan metode yuridis normatif, dengan pendekatan perundang-undangan dan studi kasus. Hasil penelitian menunjukkan bahwa meskipun UU PDP telah mengatur hak-hak subjek data, termasuk hak atas informasi, hak atas pemberitahuan kebocoran, dan hak atas ganti rugi, implementasinya dalam kasus PDNs masih sangat minim. Pemerintah sebagai pengendali data tidak transparan dalam memberi pemberitahuan kepada korban dan belum memberikan pemulihan hukum

yang memadai. Selain itu, belum terbentuknya Otoritas Pelindungan Data Pribadi (OPDP) menyebabkan absennya pengawasan dan penegakan hukum. Konsekuensi yuridis terhadap pelanggaran oleh instansi negara pun tidak berjalan efektif, meskipun UU PDP telah membuka ruang sanksi administratif, perdata, hingga pidana.

Kata Kunci: Perlindungan Data Pribadi. PDNs. UU PDP.

1. PENDAHULUAN

Kehadiran teknologi yang berkembang sangat signifikan melahirkan suatu perubahan yang juga signifikan dalam hal kebutuhan serta gaya hidup umat manusia yang semakin hari tidak bisa lepas dan cenderung bergantung pada teknologi, salah satu contohnya adalah manusia modern tidak lagi harus antri di pos atau di wartel untuk memberikan kabar kepada keluarga, teman, atau koleganya cukup hanya dengan duduk santai dengan smartphone-nya sudah bisa dan bahkan tidak hanya berupa pesan, melainkan juga bisa berupa pesan suara atau bahkan video call. Kemajuan teknologi telah mampu mengubah sistem komunikasi konvensional menjadi serba digital tanpa ada sekat ruang dan waktu, itulah yang disebut internet. Internet merupakan dunia baru yang segala bentuk aktivitasnya dilakukan secara online. Internet terus meningkatkan kapasitas dan kualitasnya untuk semakin mempermudah aktivitas manusia modern, dan terbukti bahwa hampir seluruh manusia di bumi ini menggunakannya. Bentuk dari adanya peningkatan kapasitas serta kualitas internet adalah dengan banyaknya fitur layanan online yang semakin mempermudah para penggunanya yaitu dengan lahirnya fitur integrasi antar platform.

Namun perlu juga dipahami bahwa sebelum sampai pada proses yang serba mudah tersebut, biasanya pada tahap pertama membuat akun, pengguna akan diminta beberapa informasi seperti halnya nama, nomor telepon, alamat email, keuangan, Nomor Induk Kependudukan (NIK), dan masih banyak lagi lainnya yang bisa saja di beberapa platform berbeda-beda. Data informasi yang memuat tentang pengguna selanjutnya akan masuk dan disimpan oleh platform tersebut. Tentu si pemilik platform dalam hal ini dapat dengan mudah mengetahui bahkan sampai pada mengendalikan data pribadi seorang pengguna. Disanalah potensi adanya kebocoran data pribadi, dan apalagi ketika pengendali tidak menerapkan sistem keamanan yang baik untuk melindungi data-data tersebut. Oleh karena itu, keamanan data pribadi di era saat ini penting untuk

mendapatkan hak keamanan dan perlindungan yang sangat baik dikarenakan menyangkut data pribadi seseorang yang bisa saja digunakan untuk keperluan yang dapat merugikan pengguna.

Dilansir dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) bahwa jumlah pengguna internet di Indonesia pada tahun 2024 mencapai 221.563.479 jiwa atau setara dengan 79,5% dari total populasi.¹ Dengan posisi berada peringkat 8 kebocoran data terbesar di dunia dalam rentang waktu 2020-2024.² Semakin banyak pengguna internet di suatu negara, maka potensi adanya kebocoran data semakin besar. Hal tersebut dapat dibuktikan dengan banyaknya kasus kebocoran data di Indonesia yang melibatkan banyak sekali data masyarakat yang menjadi korban.

Kebocoran data terjadi ketika data-data sensitif dan pribadi tersebut terekspos secara sengaja atau tidak sengaja atau berhasil diakses oleh pihak lain. Hal ini dapat disebabkan oleh berbagai faktor seperti serangan siber, kesalahan pengguna, atau sistem keamanan yang sangat rentan. Kebocoran data dapat memberikan dampak yang sangat luar biasa, seperti kerugian secara finansial, menciderai nama baik, perbuatan yang melanggar hukum, serta melanggar privasi seseorang. Secara sederhana, ketika suatu data yang terenskripsi bisa dilihat saja oleh pihak yang tidak memiliki hak, maka sudah disebut sebagai kebocoran data.

Pemerintah dalam hal ini memang sudah membuat regulasi untuk mencegah, mengatasi, serta mengatur apabila terjadi kebocoran data. Hal tersebut terbukti dengan di sahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Dimana regulasi tersebut dibuat untuk memberikan perlindungan hukum terhadap data pribadi dan juga didalamnya mengatur kewajiban mengelola data dengan tujuan memberikan keamanan terhadap informasi pribadi. Perlindungan terhadap data pribadi tersebut dilakukan oleh pengendali data pribadi yang dalam pasal 1 ayat (4)

¹ APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," 07 Februari, 2024, <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>.

² Adi Ahdiat, "Indonesia Masuk 10 Negara Dengan Kebocoran Data Terbesar," 02 Juli, 2024, <https://databoks.katadata.co.id/infografik/2024/07/02/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar>.

undang-undang Perlindungan Data Pribadi salah satunya adalah “Pemerintah”. Maka pemerintah memiliki tanggung jawab melindungi data pribadi masyarakat.

Secara sosiologis, perumusan aturan berkaitan dengan Perlindungan Data Pribadi (PDP) juga dapat dipahami bahwa disebabkan oleh kebutuhan dalam melindungi hak-hak individu di tengah kehidupan berbangsa dan bernegara sehubungan dengan pengumpulan, pengolahan, hingga penyebaran data pribadi. Hal tersebut dikarenakan begitu pentingnya menjaga dan melindungi kerahasiaan data pribadi seseorang yang sudah melekat pada setiap individu tersebut. Oleh karenanya, tidak boleh seorangpun apalagi pihak yang tidak berwenang tanpa mendapatkan persetujuan dari pemilik data dapat mengumpulkan, mengolah, memproses, bahkan mengekspos data pribadi.

Justru kenyataan memberikan pelajaran yang sangat berarti, meskipun secara nyata undang-undang Perlindungan Data Pribadi (PDP) sudah disahkan tetapi kebocoran data semakin menjadi-jadi. Artinya bahwa memang efektivitas penerapan undang-undang Perlindungan Data Pribadi (PDP) ini masih banyak hal-hal yang perlu dikaji kembali dan diperbaiki. Hal tersebut dibuktikan Beberapa kasus kebocoran data yang terjadi di Indonesia tidak hanya dialami oleh perorangan ataupun perusahaan, melainkan instansi pemerintah juga kerap mengalami kebocoran data, seperti yang terjadi pada Kementerian Komunikasi dan Informatika (Kemenkominfo), dimana kebocoran data tersebut menyerang Pusat Data Nasional (PDN) yang kemudian mengakibatkan data-data penting seperti data masyarakat yang meliputi Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk (KTP), Nomor Handphone, beserta data-data rahasia lainnya mengalami kebocoran. Hal tersebut juga berakibat pada data yang dimiliki oleh korban tidak dapat diakses. Badan Siber dan Sandi Negara (BSSN) yang dalam kasus kebocoran data Pusat Data Nasional (PDN) tersebut mengungkapkan bahwa memang terdapat pengelolaan sistem keamanan yang buruk oleh Kemenkominfo yang tidak membuat backup (cadangan) terhadap data-data yang tersimpan di dalam server Pusat Data Nasional (PDN). Masyarakat akhirnya menjadi korban atas ketidaksiapan pemerintah dalam mencegah adanya peretasan yang terjadi pada Pusat Data Nasional tersebut. Pusat Data Nasional memuat data rahasia seluruh masyarakat Indonesia, yang ketika data tersebut sudah diretas maka bukan tidak berpotensi melainkan sangat berpotensi adanya

penyalahgunaan data yang sudah hacker tersebut peroleh. Tentu saja hal tersebut sangat membahayakan bagi negara secara khusus terhadap masyarakat.

Dampak yang disebabkan oleh adanya kebocoran data sangatlah beragam dan tentu sangat merugikan, baik terhadap pemilik, pengendali, termasuk hacker. Pemilik data yang menjadi korban dari kebocoran data dapat mengalami kerugian berupa pencemaran nama baik, penyalahgunaan data, atau bahkan kerugian secara finansial. Pengendali yang tidak serius atau lali dalam melindungi data sensitif atau pribadi yang merupakan data-data masyarakat, pelanggan, atau yang lainnya akan berhadapan dengan hukum. Selain itu, pengendali akan kehilangan produktivitasnya disebabkan data yang sudah berpindah server, seperti yang terjadi pada kasus kebocoran data Pusat Data Nasional Sementara (PDNs) dimana beberapa layanan publik secara tiba-tiba berhenti beroperasi dan tidak bisa diakses. Hacker sebagai peretas jelas akan berhadapan dengan hukum, disebabkan oleh tindakannya yang merupakan pelanggaran hukum.

Peretasan Pusat Data Nasional (PDN) tentu adalah perbuatan melanggar hukum dan kegagalan melindungi Pusat Data Nasional (PDN) yang secara jelas dan sadar juga merupakan perbuatan melanggar hukum. Sebagaimana telah diatur dalam Undang-Undang Informasi, dan Transaksi Elektronik (UU ITE) pada pasal 30 ayat (3) yang menyatakan bahwa “tindakan yang dilakukan secara sengaja maupun tidak sengaja dengan menerobos hingga menjebol sistem pengaman suatu sistem elektronik merupakan perbuatan yang dilarang. Maka berdasarkan hal itu perbuatan tersebut merupakan tindak pidana yang terancam di hukum 8 tahun ditambah 2/3 sebagaimana yang sudah tercantum dalam pasal 46 ayat (3) dan pasal 52 ayat (3) Undang-Undang Informasi, dan Transaksi Elektronik (UU ITE).

Secara regulasi, pemerintah memang telah mengeluarkan undang-undang untuk melindungi data-data penting terkhusus yang bersifat pribadi sebagai langkah menerapkan keamanan siber. Regulasi tersebut diantaranya seperti Undang-Undang Informasi, dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan Peraturan presiden (PERPRES) Nomor 47 Tahun 2023 yang keseluruhan undang-undang tersebut dibuat untuk memberikan payung hukum terhadap perlindungan data supaya tidak terjadi kekosongan hukum nantinya apabila terjadi suatu

peristiwa yang tidak diinginkan. Terdapat 3 (tiga) tujuan utama dilakukannya keamanan informasi yaitu seperti untuk menjaga kerahasiaan, integritas, serta ketersediaan informasi,³ tetapi regulasi hanya sebatas aturan belaka ketika tidak diimbangi dengan implementasi yang efektif. Hal tersebut terbukti dari adanya kasus kebocoran Pusat Data Nasional Sementara (PDNs) yang kemudian tidak ada suatu bentuk penegakan hukum dan seolah-olah kasus tersebut hilang begitu saja. Hal tersebut disebabkan oleh ketidaksiapan dan tidak seriusnya pemerintah dan aparat penegak hukum dalam menegakkan keadilan. Pemerintah harus segera mengevaluasi serta lebih memperkuat keamanan siber yang ada pada bangsa ini agar tidak memberikan semacam efek ganda (multiplier effect) yang dapat berakibat hilangnya kepercayaan baik dari masyarakat ataupun mitra dari berbagai negara. Serta bukan tidak mungkin bahwa instansi pemerintah akan terus menjadi sasaran empuk oleh para hacker ketika pemerintah gagal untuk mengevaluasi dan memaksimalkan kekuatan keamanan siber negara. Dalam penelitian ini penulis akan mengkaji secara mendalam terhadap Undang-Undang Perlindungan Data Pribadi (UU PDP) dalam memberikan payung hukum terhadap banyaknya kasus kebocoran data khususnya yang terjadi pada server Pusat Data Nasional (PDN).

Perlindungan hukum adalah suatu upaya hukum yang harus dilakukan oleh pihak yang berwenang untuk memberikan rasa aman secara lahir maupun batin kepada masyarakat agar dapat merasakan hak-hak yang dijamin dan dilindungi oleh hukum.⁴ Perlindungan hukum tidak hanya meliputi perlindungan atas harkat dan martabat semata melainkan adanya pemajuan hak asasi manusia secara konstitusional disesuaikan dengan

³ Rakhmadi Rahman et al., *BUKU AJAR PENGANTAR SISTEM INFORMASI*, ed. Efitra, pertama (PT. Sonpedia Publishing Indonesia, 2023), [https://books.google.co.id/books?hl=en&lr=&id=4JjMEAAQBAJ&oi=fnd&pg=PA54&dq=\)+keamanan+informasi+merupakan+suatu+bentuk+perlindungan+terhadap+informasi+dan+unsur-unsur+penting+yang+ada+di+dalamnya+seperti+kerahasiaan,+integritas,+dan+ketersediaan+tidak+t](https://books.google.co.id/books?hl=en&lr=&id=4JjMEAAQBAJ&oi=fnd&pg=PA54&dq=)+keamanan+informasi+merupakan+suatu+bentuk+perlindungan+terhadap+informasi+dan+unsur-unsur+penting+yang+ada+di+dalamnya+seperti+kerahasiaan,+integritas,+dan+ketersediaan+tidak+t).

⁴ Armeylia Muliati, "PERLINDUNGAN HUKUM TERHADAP ANAK JALANAN DITINJAU DARI PERATURAN DAERAH KOTA MALANG No. 9 TAHUN 2013 TENTANG PENANGANAN ANAK JALANAN, GELANDANGAN DAN PENGEMIS (STUDI DINAS SOSIAL P3AP2KB KOTA MALANG)," 2024, 18–50, <https://eprints.umm.ac.id/id/eprint/10209>.

peraturan perundang-undangan atau seperangkat undang-undang yang bisa saling melindungi.⁵

Kebocoran data yang terjadi di Indonesia disebabkan oleh 3 faktor utama yang menjadi penyebab dari kebocoran data,⁶ yaitu, tidak jelasnya SOP yang ada di dalam organisasi tersebut. Dengan adanya SOP yang baik dapat membantu sebuah organisasi memberikan informasi yang sangat cukup untuk penyusunan standart pelayanan sehingga dapat memberikan informasi sebuah kinerja pelayanan yang akan dilakukan. Sumber daya manusia yang berkualitas akan memiliki tingkat akurasi yang baik, dimana hal tersebut merupakan kemampuan sumber daya manusia yang memiliki ketepatan terhadap tujuan suatu sistem yang ingin dicapai. Selain itu, performa dari sumber daya manusia juga menjadi salah satu ukuran dalam melihat kualitas sumber daya manusia yang ada. Performa dapat meliputi segala fenomena fisik. Kemampuan organisasi dalam mencapai tujuan ditentukan oleh sejauh mana sumber daya manusia yang dimilikinya (efektivitas). Efektivitas merupakan perpaduan utuh antara kualitas sumber daya manusia, sistem, design dan pengembangan sebuah organisasi untuk mencapai tujuan dan misi yang telah ditetapkan.⁷ Secara umum, masyarakat memahami bahwa teknologi merupakan sebuah alat elektronik yang canggih, tetapi hal tersebut berbeda dengan beberapa pemaknaan yang dilakukan oleh para ahli terhadap teknologi, seperti halnya yang didefinisikan oleh Paul Saetiles yang memaknai teknologi bukanlah hanya sebatas alat atau permesinan saja, melainkan meliputi sebuah proses, sistem, manajemen, dan mekanisme kendali manusia bukan manusia.⁸

Dari permasalahan yang sudah dijabarkan di atas, tidak adanya kejelasan penegakan hukum atas kasus kebocoran data yang secara jelas terdapat kelalaian dari pihak instansi

⁵ P M Hadjon, *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara* (Bina Ilmu, 1987), <https://books.google.co.id/books?id=zzjaGwAACAAJ>.

⁶ T. Rahmat Kautsar, "Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi Dan Regulasi Perlindungan Data Pribadi," 2022, 1–101, [https://repository.ar-raniry.ac.id/id/eprint/25647/1/T. Rahmat Kausar%2C 180802084%2C FISIP%2C IAN.pdf](https://repository.ar-raniry.ac.id/id/eprint/25647/1/T.%20Rahmat%20Kausar%20180802084%20FISIP%20IAN.pdf).

⁷ Kirana Putri Estiningtyas, "Pengaruh Kapabilitas Teknologi Informasi Dan Kualitas Sumber Daya Manusia Terhadap Keamanan Sistem Informasi Akuntansi (Studi Pada Bank Bjb Pusat Kota Bandung)" (STIE Ekuitas, 2022).

⁸ Kautsar, "Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi Dan Regulasi Perlindungan Data Pribadi."

pemerintah sebagai pengendali data menjamin keamanan data subjek data, maka dalam penelitian ini akan menganalisis lebih dalam tentang bagaimana Urgensi Pengaturan Hukum Bagi Korban Atas Kebocoran Data Pusat Data Nasional Sementara (PDNs) Perspektif Perlindungan Data Pribadi? Serta bagaimana Konsekuensi Yuridis Terhadap Perlindungan Hukum Bagi Korban Atas Kebocoran Data Pusat Data Nasional Sementara (PDNs) Perspektif Perlindungan Data Pribadi?

Tujuan dari penyusunan skripsi ini adalah untuk menganalisis urgensi pengaturan hukum dalam memberikan perlindungan kepada korban kebocoran data pada Pusat Data Nasional Sementara (PDNS) dalam perspektif perlindungan data pribadi serta mengidentifikasi dan mengkaji konsekuensi yuridis terhadap perlindungan hukum bagi korban kebocoran data PDNS berdasarkan ketentuan dalam Undang-Undang Perlindungan Data Pribadi. Dengan disusunnya skripsi ini diharapkan dapat menambah wawasan dan referensi akademik mengenai perlindungan hukum bagi korban kebocoran data Pusat Data Nasional Sementara (PDNs) dalam perspektif Undang-Undang Perlindungan Data Pribadi, dapat memberikan kontribusi terhadap perkembangan kajian hukum di bidang Perlindungan Data Pribadi (PDP) dan sistem keamanan siber (Cyber Security System), dan Memberikan rekomendasi bagi pengelola sistem elektronik terkhusus Pusat Data Nasional Sementara (PDNs) dalam meningkatkan sistem keamanan data agar kejadian serupa tidak terulang kembali.

Beberapa penelitian terdahulu berkaitan dengan kebocoran data diantaranya dilakukan oleh Diyu Sulaeman dan Anyelir Puspa Kemala dengan judul Analisis Hukum terhadap Tindak Pidana Pencurian Identitas di Indonesia,⁹ Anita Dian Eka Kusuma dengan judul Regulasi Kejahatan Siber Menurut Hukum Internasional (Studi Kasus: Peretasan Pusat Data Nasional),¹⁰ dan Miftahussurur dengan judul Peretasan Data Website Perusahaan Dalam Perspektif Hukum Pidana.¹¹ Dari penelitian terdahulu di atas memiliki kesamaan topik dengan penelitian ini yaitu tentang kebocoran data tetapi

⁹ Diyu Sulaeman and Anyelir Puspa Kemala, "Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia," *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 133–48.

¹⁰ Anita Dian Eka Kusuma, "Regulasi Kejahatan Siber Menurut Hukum Internasional (Studi Kasus: Peretasan Pusat Data Nasional)" (Universitas Jambi, 2025).

¹¹ Miftahussurur Miftahussurur, "Peretasan Data Website Perusahaan Dalam Perspektif Hukum Pidana" (Universitas Wiraraja, 2024).

memiliki perbedaan yang signifikan dan fundamental yaitu dari segi perspektif yuridisnya, dimana dalam penelitian ini menggunakan perspektif perlindungan data pribadi.

2. METODE PENELITIAN

Dalam penelitian ini, penulis akan menggunakan jenis penelitian yuridis normatif yang dalam hal ini menggunakan konsepsi hukum sebagaimana yang sudah tertulis dalam peraturan perundang-undangan (law in book) atau menjadikan kaidah norma sebagai dasar serta patokan dalam setiap perilaku manusia yang dianggap pantas. Pendekatan yang akan digunakan dalam penelitian ini adalah pendekatan peraturan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan studi kasus berupa isu hukum (case approach).

Dalam penelitian ini, penulis akan menggunakan dua sumber hukum, yaitu sumber hukum primer seperti Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi, dan Transaksi Elektronik, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Peraturan Pemerintah Nomor 71 Tahun 2022 Tentang Penyelenggaraan Sistem Elektronik dan Transaksi Elektronik, Peraturan Presiden Nomor 47 Tahun 2023 Tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, Kitab Undang-Undang Hukum Pidana (KUHP), dan Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Sumber hukum sekunder yaitu sumber bahan hukum yang dapat memberikan penjelasan terhadap bahan hukum primer. Bahan hukum sekunder terdiri dari buku, literatur, jurnal, skripsi, tesis, artikel yang memiliki hubungan dengan permasalahan yang akan penulis teliti. Selain dua sumber hukum utama tersebut, penulis juga akan menggunakan sumber hukum tersier untuk mempermudah penulis memberikan penjelasan terhadap bahan hukum primer maupun sekunder yang terdiri dari kamus hukum, Kamus Besar Bahasa Indonesia (KBBI) dan ensiklopedia. Penulis menggunakan studi kepustakaan (library research) dalam mengumpulkan data. Studi kepustakaan terdiri dari buku, jurnal, skripsi, tesis, artikel, dan lain sebagainya yang memiliki relevansi dengan pokok permasalahan pada proposal skripsi ini.

3. HASIL DAN PEMBAHASAN

Pusat Data Nasional Sementara (PDNs) merupakan bagian dari proyek strategis pemerintah Indonesia dalam mewujudkan Sistem Pemerintahan Berbasis Elektronik (SPBE). Fungsinya adalah menyimpan dan mengintegrasikan data seluruh instansi pemerintah, termasuk kementerian, lembaga, dan pemerintah daerah.¹² Namun pada 20 Juni 2024, terjadi insiden siber serius berupa serangan ransomware terhadap PDNs. Menurut pernyataan resmi dari Badan Siber dan Sandi Negara (BSSN), insiden tersebut menyebabkan enkripsi dan penyanderaan data penting, serta disrupti terhadap layanan publik digital di berbagai instansi, termasuk Kementerian Kesehatan dan Imigrasi. Pelaku meminta tebusan dalam bentuk cryptocurrency, dan diduga menggunakan varian ransomware LockBit 3.0. Serangan siber tersebut berdampak pada data pribadi milik jutaan warga negara Indonesia berpotensi terekspos, seperti NIK, Nama Lengkap, Alamat, Riwayat Kesehatan, dan Data Kepegawaian.¹³ Hingga saat ini, tidak ada laporan resmi dari pemerintah mengenai jumlah pasti korban, jenis data yang bocor, serta bentung pertanggung jawaban terhadap korban kebocoran data. Kebocoran PDNs tentu tidak hanya menimbulkan kekhawatiran atau hilangnya trust dari masyarakat ke pemerintah, tetapi juga menimbulkan kerugian material dan imaterial bagi para pemilik data.

Di Indonesia sendiri sudah memiliki regulasi berkaitan dengan perlindungan data pribadi, yaitu Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.¹⁴ Namun masih banyak sekali kekurangan dalam proses implementasinya seperti tidak adanya regulasi turunan serta mekanisme yang jelas dalam proses pemulihan, kompensasi, dan pengaduan korban atas kebocoran data. Selain itu, di Indonesia juga masih belum dibentuk lembaga pengawas yang fokus mengakomodir

¹² Eka Hero Ramadhani, I Ketut Agung Enriko, and Erika Lety Istikhomah Puspita Sari, "Kajian Strategik Manajemen Keamanan Siber Terhadap Proyek Telematika Di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional," *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi* 6, no. 1 (2025): 570–80.

¹³ DISKOMINFO, "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware," 04 Juli, 2024, <https://kominfo.lhokseumawekota.go.id/berita/read/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware-202407051720150165>.

¹⁴ Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," no. 016999 (2022).

seluruh kepentingan dalam perlindungan data pribadi, seperti halnya Otoritas Perlindungan Data Pribadi (OPDP).¹⁵ Dalam konteks kebocoran data Pusat Data Nasional Sementara (PDNs) masih belum menemukan titik terang dan seolah-olah hilang begitu saja, hal itu disebabkan dengan tidak adanya tindak lanjut misalnya seperti pemberlakuan sanksi baik administratif atau pidana terhadap pihak yang sudah lalai dalam melindungi data pribadi. Oleh karena itu, urgensi pengaturan hukum bagi korban atas kebocoran data semakin penting mengingat tidak adanya kesiapan dalam infrastruktur hukum dan agar perlindungan tidak hanya bersifat normatif tetapi juga implementatif.¹⁶

Selain proses implementasi UU Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang masih belum optimal serta ketidaksiapan infrastruktur hukum terkait perlindungan data pribadi, urgensi pengaturan hukum perlindungan data pribadi juga berlandaskan atas kerentanan terhadap penyalahgunaan atau kebocoran data seperti yang sudah terjadi. Setiap warga negara yang telah dengan sukarela memberikan data terhadap negara sebagaimana amanah undang-undang sangat berpotensi mengalami kejahatan siber, dan tanpa adanya perlindungan hukum yang konkret dapat dipastikan bahwa korban tidak memiliki kekuatan hukum untuk menuntut ganti rugi atau perlindungan hukum yang memadai, sedangkan sudah jelas bahwa perlindungan data pribadi juga merupakan amanah UUD 1945 dalam pasal 28G ayat (1) yang berbunyi "Negara berkewajiban untuk menjamin keamanan dan kerahasiaan data pribadi warga negara, apalagi jika data tersebut berada dalam pengelolaan instansi pemerintah".¹⁷ Maraknya kasus kebocoran data di Indonesia apalagi insiden tersebut terjadi di tubuh instansi pemerintah adalah bukti konkret bahwa tidak hanya sistem dalam pemerintahan yang

¹⁵ Bella Christine and Christine S T Kansil, "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Syntax Literate; Jurnal Ilmiah Indonesia* 7, no. 9 (2022): 16331–39.

¹⁶ Willy Medi Christian Nababan, "Korupsi PDNS Perburuk Kondisi Keamanan Data Nasional," 25 Mei, 2025, <https://www.kompas.id/artikel/picu-serangan-siber-korupsi-pdns-kian-perburuk-kondisi-keamanan-data-nasional>.

¹⁷ UNDANG-UNDANG DASAR NEGARA, REPUBLIK INDONESIA, and 1945, "UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA 1945" 1, no. 1 (1945).

lemah, tetapi juga pemerintah tidak dengan sungguh-sungguh melaksanakan amanah UUD 1945.

Dalam konteks kebocoran data Pusat Data Nasional Sementara (PDNS) untuk mendapatkan gambaran dan pemahaman secara komprehensif selain mengkaji dari berbagai aspek seperti filosofis, historis, dan sosiologis yang sudah peneliti jabarkan di atas, dalam hal ini peneliti juga akan mengkaji secara yuridis terkait Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Menimbang:

- a. bahwa perlindungan data pribadi merupakan salah satu hak asasi manusia yang merupakan bagian dari perlindungan diri pribadi maka perlu diberikan landasan hukum untuk memberikan keamanan atas data pribadi, berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
- b. bahwa perlindungan data pribadi ditujukan untuk menjamin hak warga negara atas perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan diri pribadi dan menumbuhkan kesadaran masyarakat serta menjamin pengakuan dan penghormatan atas pentingnya perlindungan data pribadi.¹⁸

Sebagaimana tercantum dalam huruf a di atas bahwa melindungi data pribadi seseorang merupakan salah satu implementasi dari pengakuan dan penghormatan terhadap Hak Asasi Manusia (HAM). Hal tersebut sesuai dengan prinsip data protection as a human right yang menyatakan bahwa data pribadi adalah bagian dari hak atas privasi, sesuai dengan pasal 12 Deklarasi Universal Hak Asasi Manusia (HAM) yang berbunyi "tidak seorangpun dapat diganggu sewenang-wenang atas urusan pribadinya, keluarganya, rumah tangganya, atau hubungan surat-menyuratnya, juga tidak diperkenankan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapatkan perlindungan hukum terhadap gangguan atau pelanggaran".¹⁹ Dari Hal tersebut sangat jelas bahwa Negara berkewajiban menjamin keamanan dan perlindungan

¹⁸ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

¹⁹ DEKLARASI UNIVERSAL and HAK-HAK ASASI MANUSIA, "DEKLARASI UNIVERSAL HAK-HAK ASASI MANUSIA," no. Iii (1948): 1–6.

hukum atas hak privasi seseorang dan menjamin hak tersebut ketika ada pelanggaran sekalipun pelanggaran tersebut dilakukan oleh tubuh instansi pemerintah itu sendiri. Kemudian hal tersebut diperkuat dengan apa yang sudah tersirat pada UU No.27 Tahun 2022 tentang Perlindungan Data Pribadi di huruf b bahwa perlindungan data pribadi ditujukan untuk menjamin hak warga negara untuk menumbuhkan kesadaran masyarakat dan menjamin pengakuan dan penghormatan tentang pentingnya perlindungan data pribadi.²⁰ Pada huruf b tersebut merupakan afirmasi tentang betapa pentingnya perlindungan data pribadi dan pentingnya menjamin hak seorang warga negara, maka dalam hal ini Negara sebagai pengelola data warga Negara memiliki kewajiban tersebut.

Dalam konteks insiden kebocoran data Pusat Data Nasional Sementara (PDNs), pemerintah telah gagal menjamin perlindungan dan keamanan data pribadi atau hak privasi seseorang dengan bocornya data warga negara. Selain itu, pemerintah juga gagal menjamin hak tersebut ketika terdapat pelanggaran sekalipun disebabkan oleh pemerintah itu sendiri. Dalam hal ini masih belum ada kejelasan terkait dengan penegakan hukum terhadap KEMENKOMINFO yang telah lalai dalam menjamin keamanan dan perlindungan data warga negara, padahal Badan Siber dan Sandi Negara (BSSN) telah menyatakan bahwa sistem keamanan yang diterapkan sangatlah lemah dan rentan mengalami serangan siber.²¹ Berdasarkan hal tersebut artinya pemerintah sebagai pengendali data sebagaimana pasal 1 ayat (4) UU PDP telah melakukan pelanggaran terhadap Hak Asasi Manusia disebabkan dengan tidak adanya keseriusan dalam menjamin perlindungan dan keamanan data pribadi warga negara dan gagal dalam menjamin hak korban atas pelanggaran HAM yang dilakukan oleh instansi pemerintah itu sendiri. Kegagalan pemerintah dalam menjamin perlindungan, keamanan, serta pelanggaran terhadap Hak Asasi Manusia dapat dianggap sebagai perbuatan melawan hukum oleh penguasa, pelanggaran terhadap kewajiban konstitusional, dan pelanggaran prinsip kehati-hatian sebagaimana pasal 3 UU PDP.²²

²⁰ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

²¹ Nikita Dewi Kurnia Salwa, "Tantangan & Hambatan Besar Yang Dihadapi CSIRT-BSSN Indonesia," 18 Nov, 2024, <https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn>.

²² Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

Kegagalan KEMENKOMINFO memberikan perlindungan dan keamanan terhadap data pribadi warga negara disebabkan dengan lemahnya sistem perlindungan dan keamanan Pusat Data Nasional Sementara (PDNs), hal itu dibuktikan dengan penggunaan sandi yang sangat lemah, tidak adanya Standart Operasional Perusahaan (SOP) sebagai standart tekhnis perlindungan data yang jelas dan lemahnya infrastruktur dalam melindungi dan mengamankan data pribadi warga negara. Dalam hal tersebut pemerintah tidak mengindahkan aturan penyelenggaraan perlindungan data pribadi yang sudah diatur dalam UU PDP sebagaimana berikut:

- a. Pasal 35 menyatakan bahwa pengendali data pribadi wajib melindungi dan memastikan keamanan data pribadi yang diproses dengan melakukan penyusunan SOP untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan undang-undang, dan menentukan standarisasi keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data.
- b. Pasal 36 yang berbunyi bahwa pengendali data wajib menjaga kerahasiaan data pribadi yang dikelolanya.
- c. Pasal 37 yang menyatakan bahwa pengendali data pribadi wajib melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data pribadi di bawah kendali pengendali data pribadi.
- d. Pasal 38 yang menyatakan bahwa pengendali data pribadi wajib melindungi data pribadi dari pemrosesan yang tidak sah.
- e. Pasal 39 ayat (1) yang menyatakan bahwa pengendali data pribadi wajib mencegah data pribadi diakses secara tidak sah. Ayat (2) pencegahan sebagaimana dimaksud pada ayat (1) dilakukan dengan menggunakan sistem keamanan terhadap data pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab. dan Ayat (3) pencegahan sebagaimana dimaksud ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang-undangan.²³

²³ Pribadi.

Berdasarkan hal tersebut maka dapat dinyatakan bahwa pemerintah memang tidak serius dalam menjamin perlindungan data pribadi warga negara dengan tidak membuat SOP yang jelas, tidak ada standart keamanan yang kuat, serta pengawasan yang lemah dan gagal dalam menjaga kerahasiaan serta melindungi data pribadi dari pemrosesan yang tidak sah. Sampai saat ini tidak ada keterbukaan informasi atau pemberitahuan dari pemerintah berkaitan dengan informasi kebocoran Pusat Data Nasional Sementara (PDNs) kepada masyarakat, sedangkan hal tersebut juga diatur dalam UU PDP Pasal 5 dan diperkuat dengan pasal 46 ayat (1) yang berbunyi "Dalam hal kegagalan perlindungan data pribadi, pengendali data wajib menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada subjek data pribadi dan lembaga. Diperjelas kemudian di ayat (2) "pemberitahuan tertulis yang dimaksud ayat (1) minimal memuat data pribadi yang terungkap, kapan dan bagaimana data pribadi terungkap, dan upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data pribadi.

Tidak adanya transparansi berkaitan dengan kebocoran data yang terjadi sebagaimana telah diatur dalam perundang-undangan jelas adalah perbuatan melawan hukum oleh pemerintah. Dan sampai saat ini pun masih belum ada kejelasan penegakan hukum dan bentuk tanggung jawab dari pemerintah atas insiden kebocoran data yang terjadi. Padahal sebagaimana pasal 47 dijelaskan bahwa pengendali data dalam hal ini wajib bertanggung jawab dan menunjukkan pertanggungjawaban dalam pemenuhan kewajiban melaksanakan prinsip perlindungan data pribadi, sebab faktanya tidak cukup hanya dengan mengundurkan diri hal itu bukanlah pertanggung jawaban melainkan lari dari tanggung jawab. KEMENKOMINFO sebagai pengendali data warga negara harus ditindak tegas sebagaimana peraturan yang sudah berlaku sesuai dengan pasal 49 bahwa pengendali data pribadi wajib melaksanakan perintah lembaga dalam rangka penyelenggaraan perlindungan data pribadi sesuai dengan UU PDP.²⁴

Tidak adanya lembaga khusus yang mengakomodir segala bentuk kepentingan Pusat Data Pribadi juga menjadi problem tersendiri dalam menjalankan dan menegakkan UU PDP itu sendiri. Sedangkan di dalam UU PDP sudah diatur terkait pembentukan

²⁴ Pribadi.

lembaga yang berfungsi untuk memberikan perlindungan terhadap data pribadi sebagaimana pasal 53, 54, 58, 59, 60 dan 61 UU PDP.²⁵ Namun faktanya pemerintah di Indonesia masih belum membentuk lembaga tersebut sehingga berbagai insiden kebocoran data yang terjadi di Indonesia yang disebabkan oleh kelalaian instansi pemerintah pada akhirnya seolah-olah terabaikan begitu saja tanpa adanya penindakan hukum yang jelas dan tegas.²⁶ Padahal jika dianalisis dalam hal regulasi sudah lengkap tinggal membuat regulasi turunan dan membentuk lembaga yang khusus bergerak dalam ruang perlindungan data pribadi, tetapi hal itu tidak kunjung dilakukan oleh pemerintah. Artinya tidak ada proses evaluasi dan mitigasi yang cukup berarti di tubuh pemerintah sendiri.

Dalam konteks kebocoran data Pusat Data Nasional Sementara (PDNs), seharusnya ada sanksi yang diberlakukan terhadap pemerintah sebagaimana pengaturan hukum yang ada dalam UU PDP Pasal 57 berkaitan dengan sanksi administratif. Namun harus ada evaluasi dalam sanksi administratif disini, yaitu pada ayat (3) yang berbunyi denda administratif paling tinggi 2 persen dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran. Bahwa besaran denda sanksi administratif sangat rendah apalagi jika dibebankan pada instansi pemerintah yang melanggar hukum.²⁷ Tentu hal tersebut tidak cukup untuk memberikan efek jera, terlebih bicara upaya preventif dan represif.

Kemudian pada pasal 67 UU PDP berkaitan dengan ketentuan pidana dari ayat 1 sampai ayat 3 hanya mengatur sanksi pidana terhadap perorangan, tetapi tidak diatur dalam pasal tersebut terkait dengan lembaga yang dengan sengaja dan melawan hukum dalam memperoleh, mengungkapkan, dan menggunakan data pribadi, hal tersebut mengindikasikan pemerintah kebal terhadap hukum, terlebih dengan tidak adanya kejelasan penyelesaian kasus tersebut hingga saat ini. Sedangkan pada pasal 70 sudah

²⁵ Pribadi.

²⁶ Dian Dewi Purnamasari, "Lembaga Pengawas Belum Terbentuk, Pengaduan Kebocoran Data Pun Jadi Tak Jelas," 20 Des, 2024, <https://www.kompas.id/artikel/lembaga-pengawas-belum-terbentuk-pengaduan-kebocoran-data-tak-jelas>.

²⁷ Andrew Ardiyanto Dachlan et al., "PERTANGGUNGJAWABAN HUKUM PEMERINTAH DALAM KEBOCORAN DATA PRIBADI PADA PENYELENGGARAAN PUSAT DATA NASIONAL," *Jurnal Hukum Samudra Keadilan* 20, no. 1 (2025): 109–24.

dijelaskan bahwa penjatuhan tindak pidana sebagaimana dimaksud pasal 67 dan 68 dapat dijatuhkan pada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat, atau korporasi.²⁸ Tetapi dalam kenyataannya tidak ada yang bertanggung jawab atas insiden kebocoran data pribadi tersebut.

Oleh karena itu, urgensi atas pengaturan hukum atas korban kebocoran data Pusat Data Nasional Sementara (PDNs) sangat penting. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah memadai, hanya saja perlu sedikit di evaluasi kembali terkait beberapa pasal yang tidak jelas agar tidak menimbulkan kekosongan hukum atau konflik norma. Selain itu, dalam rangka membantu implementasi UU PDP secara optimal penting untuk pemerintah segera membentuk lembaga khusus berupa Otoritas Perlindungan Data Pribadi (OPDP). Dan pertanggung jawaban oleh pemerintah haruslah dilakukan berupa penjatuhan pidana kepada yang bersangkutan.

Pusat Data Nasional Sementara (PDNs) merupakan bagian dari upaya strategis pemerintah Indonesia dalam mendigitalisasi dan menyatukan data lintas kementerian/kelembagaan dalam satu ekosistem data nasional. Namun, pada pertengahan 2024, terjadi insiden kebocoran data Pusat Data Nasional Sementara (PDNs). Serangan siber tersebut melumpuhkan sejumlah layanan publik, dan data pribadi jutaan warga Negara Indonesia diduga terekspos di forum-forum ilegal. Insiden tersebut memicu perhatian publik dan menimbulkan pertanyaan serius tentang tata kelola keamanan data, serta perlindungan hukum bagi warga negara sebagai subjek data. Kebocoran tersebut menjadi sorotan tidak hanya dari aspek teknis keamanan siber, tetapi juga dari aspek hukum khususnya mengenai perlindungan data pribadi yang telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP). Kebocoran data ini tidak hanya menimbulkan kerugian secara materil dan imateril bagi masyarakat sebagai subjek data, tetapi juga menimbulkan implikasi yuridis dalam konteks

²⁸ Pribadi, “Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.”

perlindungan data pribadi.²⁹ Oleh karena itu, penting untuk menganalisis bagaimana perlindungan hukum bagi korban kebocoran data tersebut dapat dijalankan.

Dalam perspektif hukum, kebocoran data pribadi yang terjadi dalam sistem PDNs menimbulkan beberapa konsekuensi yuridis sebagai berikut :

a. Hak Subjek Data

Dalam konteks kebocoran data pada sistem Pusat Data Nasional Sementara (PDNs) subjek data pribadi merupakan seseorang yang dalam dirinya melekat data pribadi, tentu dalam penyelenggaraan perlindungan data pribadi, subjek data sebagai pemilik data memiliki hak-hak tertentu terkait data pribadinya yang diberikan kepada pengelola data. Hak tersebut diatur dalam Pasal 5 Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi yang berbunyi "Subjek data pribadi berhak mendapatkan informasi tentang kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan data pribadi, serta akuntabilitas pihak yang meminta data pribadi".³⁰ Artinya subjek data pribadi harus mengetahui secara detail dan komprehensif terkait maksud, proses pengolahan, serta tujuan dari dimintanya data pribadi seseorang. Serta harus ada akuntabilitas atau pertanggung jawaban dari pihak pengendali data ataupun prosesor data ketika terjadi sesuatu terhadap data pribadi seseorang.

Selain itu, subjek data pribadi juga memiliki hak untuk melengkapi, memperbaharui, memperbaiki kesalahan, dan ketidak akuratan data pribadinya sesuai dengan tujuan pemrosesan data sebagaimana diatur dalam pasal 6 UU PDP. Karena itu pentingnya kejelasan maksud, proses, hingga tujuan dari dimintanya data terhadap subjek data supaya data yang akan diperoleh pengendali data dapat disesuaikan terlebih dahulu oleh subjek data berdasarkan tujuan dari dimintanya data pribadi seseorang. Tidak cukup hanya dengan keterbukaan informasi, subjek data juga berhak untuk mendapatkan akses dan memperoleh salinan data pribadi dirinya sesuai dengan ketentuan perundang-undangan UU PDP pasal 7.

²⁹ Maichle Delpiero et al., "Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data," *Padjadjaran Law Review* 9, no. 1 (2021).

³⁰ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

Jika subjek data pribadi memberikan datanya kepada pengendali data, maka subjek data juga berhak untuk mengakhiri pemrosesan, menghapus, bahkan memusnahkan data pribadinya atau menarik kembali persetujuan pemrosesan data pribadi yang telah diberikan kepada pengendali data pribadi sesuai dengan ketentuan perundang-undangan UU PDP pasal 8 dan pasal 9. Dalam rangka mengakhiri, menghapus, memusnahkan, serta menarik persetujuan pemrosesan data pribadi, subjek data dijamin dalam pasal 10 UU PDP bahwa subjek data berhak mengajukan keberatan atas tindakan pengambilan keputusan secara otomatis termasuk pemprofilan yang dapat menimbulkan akibat hukum atau berdampak signifikan terhadap subjek data pribadi. Oleh karena itu, subjek data memiliki hak untuk menunda atau membatasi data pribadi yang bisa di proses secara proporsional sesuai dengan tujuan pemrosesan data pribadi, hal itu dijamin dalam pasal 11 UU PDP.³¹

Pada insiden kebocoran data Pusat Data Nasional Sementara (PDNs) dimana dalam hal ini subjek data menjadi korban atas kebocoran data tersebut, maka berhak untuk menggugat dan menerima ganti rugi atas pelanggaran tersebut, hal itu tertera dalam pasal 12 UU PDP. Seharusnya pemerintah dalam hal ini yang telah lalai dalam memberikan perlindungan dan keamanan data pribadi warga negara wajib memberikan ganti rugi dan dapat digugat oleh warga negara atas insiden tersebut. Selain itu di Pasal 13 UU PDP dijelaskan bahwa subjek data pribadi berhak mendapatkan, menggunakan data pribadinya dari pengendali data dalam bentuk yang sesuai yang dapat dibaca oleh sistem elektronik. Serta berhak untuk menggunakan dan mengirimkan data pribadinya ke pengendali data pribadi lainnya selagi sistem yang digunakan saling terintegrasi dengan aman dan sesuai dengan prinsip perlindungan data pribadi.

b. Tanggung Jawab Pengendali Data

Pengendali data pribadi dan prosesor data pribadi dalam pasal 19 UU PDP dapat berupa individu, badan publik, dan organisasi internasional. artinya bahwa

³¹ Pribadi.

pengendali data pribadi merupakan seseorang, badan publik, atau organisasi internasional yang memiliki data pribadi seseorang dan melakukan pemrosesan data pribadi seseorang. Dalam perlindungan data pribadi, pengendali data pribadi memiliki kewajiban dalam mengelola data pribadi seseorang, mengingat sebagaimana Undang-Undang Perlindungan Data Pribadi huruf a di konsideran menyatakan bahwa data pribadi adalah bagian dari hak privasi, yang artinya data pribadi adalah bagian dari Hak Asasi Manusia (HAM) yang harus betul-betul diperhatikan. Oleh karena itu, dalam UU PDP pasal 20, 21, dan 22 mengatur bahwa pengendali data harus memiliki dasar dalam melakukan pemrosesan data pribadi. Dasar pemrosesan data yang dimaksud adalah persetujuan secara eksplisit dari subjek data untuk tujuan tertentu, maka untuk memenuhi unsur persetujuan yang dimaksud, pengendali data wajib menyampaikan informasi tentang legalitas pemrosesan, tujuan, jenis dan relevansi data, jangka waktu, serta hak subjek data pribadi.³²

Persetujuan subjek data pribadi untuk memberikan data pribadinya terhadap pengendali data haruslah secara tertulis baik bersifat elektronik maupun non elektronik. Selain itu, dasar pemrosesan data pribadi juga harus ada pemenuhan kewajiban perjanjian, pemenuhan keajiban hukum dari pengendali data, pemenuhan perlindungan kepentingan vital subjek data pribadi, dalam rangka menjalankan tugas guna kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan sesuai dengan peraturan, serta pemenuhan kepentingan lain yang sah dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan pengendali data pribadi dan hak subjek data pribadi.³³ Sebelum melakukan pemrosesan data, pengendali data wajib menunjukkan bukti persetujuan yang telah diberikan oleh subjek data sesuai dengan pasal 24 UU PDP.³⁴ Ketika melakukan pemrosesan data pribadi sebagaimana pasal 27 dan 28 UU PDP, pengendali data memiliki kewajiban

³² Taufik Hidayat Telaumbanua, "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif," *Lex Privatum* 13, no. 1 (2024).

³³ Dennys Nababan and Sahuri Lasmadi, "Pertanggungjawaban Pidana Terhadap Penyalahgunaan Data Pribadi Pada Tindak Pidana Dunia Maya," *PAMPAS: Journal Of Criminal Law* 4, no. 2 (2023): 232–51.

³⁴ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

untuk memproses data tersebut secara terbatas dan spesifik, sah secara hukum, dan juga transparan sesuai dengan tujuan pemrosesan data pribadi.

Selain memastikan adanya persetujuan dan pemrosesan data yang sah secara perundang-undangan, pengendali data juga memiliki kewajiban untuk mengukur keabsahan data yang telah diberikan oleh subjek data pribadi sebagaimana pasal 29 dan 30 UU PDP. Dimana pengendali data wajib memastikan akurasi data pribadi sesuai undang-undang dengan melakukan verifikasi.³⁵ Dari proses verifikasi tersebut dapat menjadi acuan keakuratan data subjek data pribadi, dan pengendali data pribadi wajib memperbarui atau memperbaiki kesalahan atau ketidakakuratan data pribadi paling lambat 3x24 jam terhitung sejak permintaan pembaruan dan perbaikan data pribadi dari subjek data pribadi. Dan setelah itu pengendali data wajib memberikan hasil perbaikan dan pembaruan data pribadi kepada subjek data pribadi.

Berkaitan dengan transparansi pemrosesan data, maka pengendali data wajib melakukan perekaman terhadap seluruh kegiatan pemrosesan data sebagaimana yang telah diatur dalam pasal 31 UU PDP. Setelah itu, pengendali data pribadi wajib memberikan akses kepada subjek data pribadi dan juga wajib melakukan penolakan akses perubahan terhadap data pribadi kepada subjek data pribadi apabila dinilai membahayakan terhadap data pribadi, hal tersebut diatur dalam pasal 32 dan 33 UU PDP.³⁶ Karena itu sesuai dengan pasal 34 UU PDP, pengendali data pribadi wajib melakukan penilaian dampak perlindungan data pribadi dalam hal pemrosesan data pribadi yang memiliki potensi risiko tinggi terhadap subjek data pribadi. Maka kemudian pengendali data memiliki kewajiban untuk melindungi dan memastikan keamanan data pribadi, menjaga kerahasiaan data pribadi, melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data sesuai pasal 35, 36, dan 37 UU PDP. Dalam rangka melindungi data pribadi, pengendali data memiliki

³⁵ Sandryones Palinggi and Lutma Ranta Allolinggi, "Analisa Deskriptif Industri Fintech Di Indonesia: Regulasi Dan Keamanan Jaringan Dalam Perspektif Teknologi Digital," *Ekonomi Dan Bisnis* 6, no. 2 (2019): 177–92.

³⁶ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

kewajiban melindungi data pribadi dari proses yang tidak sah sesuai dengan pasal 38 dan 39 UU PDP.

Pasal 40 ayat (1) dan (2) Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi menyatakan bahwa pengendali data pribadi wajib menghentikan pemrosesan data pribadi dalam hal subjek data pribadi telah menggunakan haknya untuk menarik kembali persetujuan pemrosesan data pribadi. kewajiban pemberhentian pemrosesan data tersebut diatur lebih lanjut dalam ayat (2) yaitu pemberhentian pemrosesan data pribadi yang telah ditarik kembali oleh subjek data dilakukan dalam kurun waktu 3x24 jam setelah pengendali data menerima permintaan penarikan kembali persetujuan untuk memproses data pribadi milik subjek data pribadi. Pada pasal 41 ayat (1), (2), dan (3) UU Perlindungan Data Pribadi menjelaskan tentang penundaan dan pembatasan terhadap pemrosesan data, dimana pengendali data wajib menunda dan membatasi pemrosesan data pribadi baik hanya sebagian data ataupun keseluruhan data paling lambat dalam kurun waktu 3x24 jam terhitung sejak pengendali data menerima permintaan penundaan atau pembatasan pemrosesan data pribadi. Setelah pengendali data menerima permintaan penundaan dan pembatasan pemrosesan data pribadi, pengendali data wajib memberitahukan kepada subjek data pribadi bahwa telah dilaksanakan penundaan dan pembatasan pemrosesan data pribadi.³⁷

Dalam UU PDP, tidak hanya mengatur tentang pemberhentian, penundaan dan pembatasan pemrosesan data pribadi, melainkan juga diatur tentang kewajiban pengendali data pribadi untuk mengakhiri pemrosesan data pribadi ketika sudah mencapai masa retensi, tujuan pemrosesan data telah dicapai, dan terdapat permintaan dari subjek data. Hal tersebut tertuang dalam pasal 42 Undang-Undang Perlindungan Data Pribadi. Kemudian dalam pasal 43 dan 44 UU PDP juga mengatur kewajiban pengendali data untuk menghapus dan memusnahkan data pribadi yang telah selesai masa retensinya, tercapai tujuannya, terdapat permintaan oleh subjek data pribadi untuk di hapus, ditarik persetujuannya oleh subjek data

³⁷ Pribadi.

pribadi, dan data pribadi yang diperoleh atau diproses dengan cara melawan hukum. Pengendali data pribadi yang telah melakukan penghapusan atau pemusnahan data pribadi harus memberitahukan kepada subjek data pribadi bahwa data pribadi telah dihapus dan/atau dimusnahkan sebagaimana bunyi pasal 45 UU PDP.

Pengendali data pribadi tidak hanya memiliki kewajiban memberitahukan terkait penghapusan dan/atau pemusnahan data pribadi, melainkan diatur juga pada pasal 46 UU PDP bahwa pengendali data juga memiliki kewajiban memberitahukan kepada subjek data pribadi dan lembaga secara tertulis terkait bahwa telah terjadi insiden kegagalan dalam melindungi data pribadi selama kurun waktu 3x24 jam. Pemberitahuan secara tertulis yang dimaksud harus memuat data pribadi yang terungkap, kapan dan bagaimana data pribadi terungkap, upaya penanganan dan pemulihan atas terungkapnya data pribadi oleh pengendali data pribadi dan dalam hal tertentu, pengendali data pribadi wajib menginformasikan kepada masyarakat bahwa telah terjadi kebocoran data. Sedangkan fakta yang terjadi pada insiden kebocoran data Pusat Data Nasional Sementara (PDNs) tidak ada kejelasan atau pemberitahuan informasi kepada subjek data pribadi secara tertulis yang memuat poin-poin sebagaimana diatur dalam pasal 46 ayat (2) UU PDP.³⁸

Jika mengikuti aturan UU PDP, maka sangat jelas bahwa tindakan yang dilakukan pemerintah dengan tidak adanya pemberitahuan secara tertulis kepada subjek data selama kurun waktu 3x 24 jam merupakan tindakan melawan hukum dan menimbulkan konsekuensi yuridis sebagaimana diatur dalam UU PDP. Diatur lebih lanjut dalam pasal 47 UU PDP bahwa pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggung jawaban dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi, Sedangkan pada insiden kebocoran data pada sistem Pusat Data Nasional Sementara (PDNs) tidak ada bentuk pertanggung jawaban bahkan kegagalan dalam menunjukkan pertanggungjawaban melaksanakan prinsip perlindungan data pribadi

³⁸ Jonathan Riko Mono, "Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi Dalam Insiden Serangan Siber Pusat Data Nasional Sementara.," *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 5, no. 1 (2024).

sebagaimana diatur dalam pasal 3 UU PDP dari pemerintah yang dalam hal ini merupakan tanggung jawab KEMENKOMINFO, yang terjadi justru Menteri KEMENKOMINFO mengundurkan diri dari jabatannya. Pengunduran diri secara sepihak jelas merupakan bentuk dari pertanggung jawaban dan bukanlah bentuk dari konsekuensi yuridis sebagaimana aturan dalam Undang-Undang Perlindungan Data Pribadi.

Kewajiban pengendali data kemudian diatur lebih lanjut dalam pasal 48, 49, dan 50 Undang-Undang Perlindungan Data Pribadi yang didalamnya memuat tentang kewajiban pengendali data menginformasikan adanya penggabungan, pemusahan, pengambilalihan, peleburan, atau pembubaran badan hukum kepada subjek data pribadi. Pengendali data pribadi atau prosesor data pribadi wajib melaksanakan perintah lembaga dalam rangka penyelenggaraan perlindungan data pribadi sesuai UU PDP dan di Pasal 50 UU PDP kemudian dikecualikan kewajiban dari pengendali data pribadi.

c. Sanksi Hukum Terhadap Pelanggaran

Dalam Undang-Undang Perlindungan Data Pribadi (UU PDP) sebagai kekuatan hukum yang menjamin tentang perlindungan data pribadi juga mengatur terkait sanksi hukum terhadap pengendali data pribadi yang melakukan tindakan melawan hukum sebagaimana diatur dalam bab XIII tentang larangan dalam penggunaan data pribadi. Sanksi hukum terhadap pelanggaran dalam perlindungan data pribadi diatur dalam pasal 57 tentang sanksi administratif, pasal 67 tentang sanksi pidana dan pasal 68 tentang sanksi pidana penjara dan denda terhadap seseorang yang memalsukan data pribadi. Diatur lebih lanjut dalam pasal 69 bahwa selain sanksi pidana denda maupun penjara, juga dapat dijatuhi pidana tambahan berupa perampasan keuntungan atau aset yang diperoleh dari tindak pidana dan pembayaran ganti rugi.

Dalam konteks kebocoran data Pusat Data Nasional Sementara (PDNs) masih belum ada kejelasan pidana yang dibebankan kepada pengendali data pribadi yang telah lalai dalam memberikan jaminan perlindungan dan keamanan data pribadi. Salah satu faktor yang menyebabkan belum adanya kejelasan terkait konsekuensi yuridis dalam kasus tersebut dikarenakan tidak adanya kejelasan siapa yang akan

bertanggung jawab dalam insiden tersebut, kesulitan dalam mendeteksi dan menemukan alat bukti yang sah menurut Undang-Undang, tidak adanya lembaga khusus yang bergerak dalam Otoritas Perlindungan Data Pribadi (OPDP), dan belum ada aturan turunan berupa Peraturan Pemerintah (PP), tidak adanya panduan teknis dalam peraturan perlindungan data pribadi berupa Standart Operasional Perusahaan (SOP) dan standart keamanan dalam menjamin perlindungan dan keamanan data pribadi.³⁹ Padahal keseluruhan hal tersebut telah diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.⁴⁰

Peraturan lain yang dapat dijadikan perangkat tambahan dalam mendukung aspek penegakan hukum terhadap pelanggaran kebocoran data juga diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP), walaupun tidak secara eksplisit mengatur mengenai pelanggaran perlindungan data pribadi namun terdapat beberapa pasal yang bisa dijadikan landasan yuridis untuk menjerat pelaku pelanggaran perlindungan data pribadi terutama jika terdapat unsur pidana yang terpenuhi yaitu:

- 1) Pasal 258, setiap orang yang secara melawan hukum mendengarkan, mereka, membelokkan, mengubah, menghambat, dan/atau mencatat transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik, baik menggunakan jaringan kabel komunikasi maupun jaringan nirkabel, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau pidana denda paling banyak kategori VI.
- 2) Pasal 332 ayat (3), setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan, dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau pidana denda paling banyak kategori VI.

³⁹ Alza Gabriel, "PERLINDUNGAN HUKUM ATAS DATA PRIBADI DALAM KASUS KEBOCORAN DATA PUSAT DATA NASIONAL SEMENTARA (PDNS) DALAM PERSPEKTIF HUKUM PIDANA," in *Seminar Nasional-Hukum Dan Pancasila*, vol. 3, 2024, 18–26.

⁴⁰ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

- 3) Pasal 333 huruf c dan d, dipidana dengan pidana penjara 7 tahun atau pidana denda paling banyak kategori VI, setiap orang yang tanpa hak atau melampaui wewenangnya menggunakan atau mengakses komputer atau sistem elektronik, baik dari dalam maupun luar negeri untuk memperoleh informasi dari komputer atau sistem elektronik yang dilindungi oleh negara atau sistem elektronik milik negara.
- 4) Pasal 335, setiap orang yang tanpa hak menggunakan atau mengakses komputer atau sistem elektronik dengan cara apapun dengan maksud memperoleh, mengubah, merusak, atau menghilangkan informasi milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi, dipidana dengan pidana penjara paling lama 12 tahun atau denda kategori VII.
- 5) Pasal 362, barang siapa mengambil keseluruhan atau sebagian kepunyaan orang lain dengan maksud untuk dimiliki dengan cara melawan hukum, dapat dikenakan pidana penjara paling lama 5 tahun atau denda maksimal 900 ribu rupiah.⁴¹

Kemudian sebagai landasan bagi korban kebocoran data sebagai upaya untuk mendapatkan keadilan dalam insiden tersebut dapat menggunakan Kitab Undang-Undang Hukum Acara Pidana yang didalamnya memuat prosedur-prosedur hukum yang bisa ditempuh oleh korban kebocoran data PDNs, yaitu:

- 1) Pasal 77-83, yang memuat tentang pra peradilan untuk menjamin hak-hak korban jika proses hukum tidak dijalani secara adil.
- 2) Pasal 108 ayat (1), setiap orang yang mengalami, melihat, menyaksikan, dan/atau menjadi korban peristiwa yang merupakan tindak pidana berhak untuk mengajukan laporan atau pengaduan kepada penyelidik dan/atau penyidik baik secara lisan maupun tertulis.⁴²

Walaupun di Indonesia sudah terdapat payung hukum untuk memberikan jaminan kepastian, keadilan, serta kebermanfaatan atas perlindungan data pribadi

⁴¹ UNDANG-UNDANG REPUBLIK INDONESIA et al., “UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 1 TAHUN 2023 TENTANG KITAB UNDANG-UNDANG HUKUM PIDANA,” no. 16100 (2023).

⁴² UNDANG-UNDANG REPUBLIK INDONESIA et al., “UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 8 TAHUN 1981 TENTANG HUKUM ACARA PIDANA,” 1981.

yaitu dengan adanya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, walaupun dalam proses implementasi dan penegakan hukumnya masih belum menemukan kejelasan yang pasti terlebih ketika menyangkut instansi pemerintahan. Dalam teori Lawrence M. Friedman berpendapat bahwa keefektifan serta tingkat keberhasilan atau tidaknya suatu proses implementasi penegakan hukum dapat dilihat dari 3 unsur sistem hukum yang ada, yaitu:

a. Struktur hukum,

Struktur hukum adalah kerangka permanen dari suatu sistem hukum yang menjaga setiap proses hukum tetap berada dalam batas-batas pengaturannya. struktur hukum terdiri atas jumlah dan ukuran pengadilan, yurisdiksi, termasuk peraturan perundang-undangan.⁴³ Dalam teori ini, juga dijelaskan tentang sistem struktural yang juga menjadi salah satu penentu baik atau buruknya suatu penerapan hukum, ditambah dengan buruknya mentalitas penegakan hukum juga menyebabkan penegakan hukum tidak sesuai sebagaimana mestinya. Oleh karena itu, penegakan hukum harus mampu mengimbangi regulasi yang sudah ada, sebab regulasi yang bagus akan seolah tidak berdampak apa-apa ketika penegakan hukumnya buruk, begitupun sebaliknya.

Permasalahan dalam struktur hukum di Indonesia adalah maraknya penyalahgunaan wewenang oleh Aparat Penegak Hukum (APH) yang banyak melakukan pelanggaran.⁴⁴ Hukum progresif tidak hanya mengacu pada hukum secara konseptual, melainkan juga harus mengacu pada rasa keadilan yang hidup di dalam masyarakat.

b. Substansi hukum,

Dalam hukum terdapat istilah "produk hukum" yang merupakan susunan berbagai keputusan yang ^{belum} diambil serta menekankan penerapan undang-undang jika melalui acara. Sistem tersebut kemudian mempengaruhi sistem hukum di Indonesia sebagaimana yang tertuang dalam pasal 1 KUHP yang

⁴³ Jan S Maringka, *Reformasi Kejaksaan Dalam Sistem Hukum Nasional* (Sinar Grafika, 2022).

⁴⁴ Widhy Andrian Pratama, "Penegakan Hukum Terhadap Korupsi Di Era Modernisasi Digital," *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (2024): 91–104.

menyatakan bahwa "tidak ada tindak pidana yang dapat dipidanakan kecuali ada aturan yang mengaturnya". Hal tersebut dapat menjadi celah bagi seseorang yang melanggar hukum untuk menghindari sanksi atas perbuatannya.

c. Budaya hukum

Budaya hukum adalah suasana pemikiran sosial dan kekuatan sosial yang menentukan bagaimana hukum diterapkan, dihindari atau disalahgunakan.⁴⁵

Friedman juga mengartikan bahwa budaya hukum sebagai sikap dan nilai yang mempunyai dampak positif dan negatif terhadap perilaku hukum. Selain itu, tingkat kepuasan terhadap litigasi juga merupakan bagian dari budaya hukum. Oleh karena itu, budaya hukum tidak lain adalah seluruh faktor yang menentukan bagaimana sistem hukum memperoleh tempat logisnya dalam kerangka budaya masyarakat. Artinya bahwa budaya hukum adalah sikap umum anggota masyarakat dan sistem nilai yang ada dalam masyarakat yang menentukan bagaimana hukum harus diterapkan dalam masyarakat.

Dalam konteks kebocoran data Pusat Data Nasional Sementara (PDNs), struktur hukum menyangkut Aparat Penegak Hukum (APH) seperti kepolisian, selain kepolisian juga ada Kejaksaan bagian pidana umum yang menindaklanjuti prosedur tindak pidana dari kepolisian. Setelah prosedur dari Kejaksaan dilimpahkan ke pengadilan yang fungsi utamanya adalah menerima, memeriksa, dan memutuskan setiap perkara yang diajukan.

Substansi hukum adalah perangkat perundang-undangan yang dalam insiden kebocoran data Pusat Data Nasional Sementara (PDNs) adanya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.⁴⁶ Dengan maraknya kasus kebocoran data di Indonesia, sangat penting untuk adanya suatu bentuk perlindungan hukum bagi korban atas kebocoran data yang secara konstitusional bahwa negara berkewajiban melindungi privasi dan data

⁴⁵ KURNIA GANDA PUTRI NASUTION, "ANALISIS YURIDIS PENJATUHAN HUKUMAN TERHADAP PELAKU TINDAK PIDANA TANPA HAK MEMPERDAGANGKAN NARKOTIKA JENIS SABU-SABU (Studi Putusan Mahkamah Agung Republik Indonesia Nomor 1866 K/Pid. Sus/2021)" (Fakultas Hukum, universitas islam sumatera utara, 2025).

⁴⁶ Pribadi, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi."

masyarakat umum sebagaimana diatur dalam Undang-Undang Perlindungan Data Pribadi. Oleh karena itu, hukum diharuskan dapat memberikan perlindungan terhadap negara, individu, dan masyarakat untuk menciptakan rasa aman dari berbagai gangguan dan ancaman.

Perlindungan hukum kepada rakyat dibedakan menjadi 2 (dua), yaitu perlindungan hukum preventif dan perlindungan hukum represif.⁴⁷ Perlindungan hukum preventif adalah upaya perlindungan hukum yang dilakukan untuk mencegah sebelum terjadinya suatu perbuatan melawan dan/atau melanggar hukum. Sedangkan perlindungan hukum represif adalah perlindungan hukum berupa sanksi denda, penjara, atau hukuman terhadap suatu pelanggaran. Dalam hal ini, kedua upaya perlindungan hukum tersebut merupakan representasi dari fungsi hukum untuk memberikan keadilan, kepastian, kebermanfaatan, dan ketertiban.

4. KESIMPULAN

Berdasarkan hasil pembahasan pada bab sebelumnya, dapat disimpulkan bahwa urgensi pengaturan hukum bagi korban kebocoran data Pusat Data Nasional Sementara (PDNs) sangatlah mendesak. Meskipun Indonesia telah memiliki Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) sebagai payung hukum, implementasi dan pelaksanaan perlindungan terhadap korban kebocoran data, khususnya pada insiden PDNs, masih belum optimal.

Beberapa temuan penting dari penelitian ini antara lain, Hak-hak korban sebagaimana diatur dalam UU PDP seperti hak untuk mendapatkan pemberitahuan atas pelanggaran data, hak atas informasi, dan hak atas ganti rugi belum dilaksanakan secara nyata oleh pemerintah sebagai pengendali data dalam kasus PDNs, tidak adanya transparansi dan pertanggungjawaban dari pemerintah dalam menangani kebocoran data menimbulkan ketidakpastian hukum bagi masyarakat sebagai subjek data pribadi, belum terbentuknya Otoritas Pelindungan Data Pribadi (OPDP) dan ketiadaan peraturan teknis

⁴⁷ Tita Nurdinna, "ANALISIS HUKUM TENTANG PERLINDUNGAN NASABAH PENYIMPAN DALAM LAYANAN INTERNET BANKING," *LEGAL OPINION* 13, no. 1 (2025): 56–63.

pelaksanaan menyebabkan lemahnya pengawasan serta penegakan hukum terhadap pengendali data, termasuk instansi negara, serta konsekuensi yuridis terhadap pelanggaran kewajiban pengendali data (termasuk instansi pemerintah) telah diatur dalam UU PDP, baik dalam bentuk sanksi administratif (Pasal 57–60) maupun tuntutan ganti rugi secara perdata oleh korban. Namun, dalam praktiknya, konsekuensi yuridis ini belum dijalankan secara transparan dan akuntabel dalam kasus PDNs, dan konsekuensi yuridis lainnya adalah potensi gugatan dari korban secara individual maupun kolektif, sebagaimana diatur dalam Pasal 58 dan 60 UU PDP.

Konsekuensi yuridis atas kebocoran data pribadi telah diatur secara eksplisit dalam UU PDP, baik dalam bentuk sanksi administratif, gugatan perdata, maupun sanksi pidana. Hal ini menunjukkan bahwa secara normatif, hukum Indonesia telah menyediakan perangkat untuk melindungi korban pelanggaran data pribadi. Negara sebagai pengendali data tidak dikecualikan dari konsekuensi hukum, sebagaimana ditegaskan dalam Pasal 36 UU PDP. Instansi pemerintahan yang melakukan kelalaian dalam pengelolaan data tetap dapat dimintai pertanggungjawaban secara hukum. Korban kebocoran data memiliki hak hukum untuk menggugat secara perdata (Pasal 58), memperoleh pemberitahuan atas kegagalan perlindungan data (Pasal 14 ayat (1)), serta berhak atas kompensasi atas kerugian yang ditimbulkan akibat kebocoran data. Namun demikian, dalam praktiknya konsekuensi yuridis belum ditegakkan secara nyata dalam kasus kebocoran PDNs. Tidak adanya pemberitahuan resmi kepada korban, belum diberikannya ganti rugi, serta tidak dijatuhkannya sanksi terhadap instansi pemerintah menunjukkan ketimpangan antara norma hukum dan pelaksanaannya. Ketidakefektifan penegakan konsekuensi hukum ini menimbulkan kekosongan perlindungan nyata terhadap korban, yang bertentangan dengan semangat konstitusi dan prinsip negara hukum. Hal ini menandakan perlunya reformasi kelembagaan dan operasional dalam sistem perlindungan data di Indonesia.

Akibat belum efektifnya penerapan konsekuensi yuridis tersebut, maka prinsip akuntabilitas dan keadilan dalam perlindungan data pribadi tidak tercapai, dan hak konstitusional warga negara atas perlindungan diri dan privasi sebagaimana dijamin dalam Pasal 28G ayat (1) UUD 1945 menjadi terabaikan. Dengan demikian,

perlindungan hukum terhadap korban kebocoran data dalam kasus PDNs masih bersifat normatif dan belum operasional, karena belum adanya langkah konkret dari pemerintah dalam memenuhi kewajiban sebagai pengendali data yang amanah dan bertanggung jawab, negara perlu segera bertindak untuk menjamin keadilan dan perlindungan nyata bagi korban kebocoran data, sebagai bentuk penghormatan terhadap hak privasi warga negara yang dilindungi oleh konstitusi.

Pemerintah harus segera membentuk Otoritas Pelindungan Data Pribadi (OPDP) sebagai lembaga independen yang bertugas mengawasi pengendalian data pribadi, menerima pengaduan, serta memastikan pemulihan dan kompensasi bagi korban pelanggaran data. Perlu dibuat peraturan turunan dari UU PDP yang secara rinci mengatur standar keamanan siber, mekanisme pemberitahuan pelanggaran data, hak korban, dan prosedur ganti rugi, termasuk jika pelanggaran dilakukan oleh instansi negara. Dan korban kebocoran data perlu diberikan akses terhadap jalur hukum yang sederhana dan terjangkau, baik melalui pengadilan maupun penyelesaian sengketa alternatif, untuk menuntut ganti rugi atas kerugian yang dialami.

Pemerintah perlu menunjukkan komitmen terhadap perlindungan data pribadi melalui transparansi penanganan insiden seperti kebocoran PDNs, termasuk mengumumkan hasil investigasi, pihak yang bertanggung jawab, dan langkah-langkah pemulihan. Pemerintah harus menjalankan konsekuensi yuridis terhadap pelanggaran kebocoran data, tanpa terkecuali terhadap instansi negara, untuk memberikan kepastian hukum dan efek jera, sebagaimana diatur dalam Pasal 57–60 (sanksi administratif), Pasal 67–70 (sanksi pidana), dan Pasal 58 (tanggung jawab perdata) UU PDP. Dengan langkah-langkah tersebut, diharapkan kepercayaan publik terhadap sistem digital pemerintah dapat dipulihkan, serta tercipta tata kelola data yang adil, aman, dan bertanggung jawab di Indonesia.

5. DAFTAR PUSTAKA

Ahdiat, Adi. “Indonesia Masuk 10 Negara Dengan Kebocoran Data Terbesar.” 02 Juli, 2024.
APJII. “APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang.” 07 Februari, 2024.

- Christine, Bella, and Christine S T Kansil. "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Syntax Literate; Jurnal Ilmiah Indonesia* 7, no. 9 (2022): 16331–39.
- Dachlan, Andrew Ardiyanto, Alya Nabila, Nabilatul Alimah Putri, and Nabilah Nurmasitha. "PERTANGGUNGJAWABAN HUKUM PEMERINTAH DALAM KEBOCORAN DATA PRIBADI PADA PENYELENGGARAAN PUSAT DATA NASIONAL." *Jurnal Hukum Samudra Keadilan* 20, no. 1 (2025): 109–24.
- Delpiero, Maichle, Farah Azzahra Reynaldi, Istiawati Utami Ningdiah, and Nafisah Muthmainnah. "Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data." *Padjajaran Law Review* 9, no. 1 (2021).
- DISKOMINFO. "BSSN Identifikasi Pusat Data Nasional Sementara Diserang Ransomware." 04 Juli, 2024.
- Estiningtyas, Kirana Putri. "Pengaruh Kapabilitas Teknologi Informasi Dan Kualitas Sumber Daya Manusia Terhadap Keamanan Sistem Informasi Akuntansi (Studi Pada Bank Bjb Pusat Kota Bandung)." STIE Ekuitas, 2022.
- Gabriel, Alza. "PERLINDUNGAN HUKUM ATAS DATA PRIBADI DALAM KASUS KEBOCORAN DATA PUSAT DATA NASIONAL SEMENTARA (PDNS) DALAM PERSPEKTIF HUKUM PIDANA." In *Seminar Nasional-Hukum Dan Pancasila*, 3:18–26, 2024.
- Hadjon, P M. *Perlindungan Hukum Bagi Rakyat Di Indonesia: Sebuah Studi Tentang Prinsip-Prinsipnya, Penanganannya Oleh Pengadilan Dalam Lingkungan Peradilan Umum Dan Pembentukan Peradilan Administrasi Negara*. Bina Ilmu, 1987.
- INDONESIA, UNDANG-UNDANG REPUBLIK, NOMOR 8 TAHUN 1981, TENTANG, and HUKUM ACARA PIDANA. "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 8 TAHUN 1981 TENTANG HUKUM ACARA PIDANA," 1981.
- INDONESIA, UNDANG-UNDANG REPUBLIK, NOMOR 1 TAHUN 2023, TENTANG, and KITAB UNDANG-UNDANG HUKUM PIDANA. "UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 1 TAHUN 2023 TENTANG KITAB UNDANG-

- UNDANG HUKUM PIDANA,” no. 16100 (2023).
- Kautsar, T. Rahmat. “Kajian Literatur Terstruktur Terhadap Kebocoran Data Pribadi Dan Regulasi Perlindungan Data Pribadi,” 2022, 1–101.
- Kusuma, Anita Dian Eka. “Regulasi Kejahatan Siber Menurut Hukum Internasional (Studi Kasus: Peretasan Pusat Data Nasional).” Universitas Jambi, 2025.
- Maringka, Jan S. *Reformasi Kejaksaan Dalam Sistem Hukum Nasional*. Sinar Grafika, 2022.
- Miftahussurur, Miftahussurur. “Peretasan Data Website Perusahaan Dalam Perspektif Hukum Pidana.” Universitas Wiraraja, 2024.
- Mono, Jonathan Riko. “Perlindungan Hukum Terhadap Hak Privasi Subjek Data Pribadi Dalam Insiden Serangan Siber Pusat Data Nasional Sementara.” *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)* 5, no. 1 (2024).
- Muliati, Armyelia. “PERLINDUNGAN HUKUM TERHADAP ANAK JALANAN DITINJAU DARI PERATURAN DAERAH KOTA MALANG No. 9 TAHUN 2013 TENTANG PENANGANAN ANAK JALANAN, GELANDANGAN DAN PENGEMIS (STUDI DINAS SOSIAL P3AP2KB KOTA MALANG),” 2024, 18–50.
- Nababan, Dennys, and Sahuri Lasmadi. “Pertanggungjawaban Pidana Terhadap Penyalahgunaan Data Pribadi Pada Tindak Pidana Dunia Maya.” *PAMPAS: Journal Of Criminal Law* 4, no. 2 (2023): 232–51.
- Nababan, Willy Medi Christian. “Korupsi PDNS Perburuk Kondisi Keamanan Data Nasional.” 25 Mei, 2025.
- NASUTION, KURNIA GANDA PUTRI. “ANALISIS YURIDIS PENJATUHAN HUKUMAN TERHADAP PELAKU TINDAK PIDANA TANPA HAK MEMPERDAGANGKAN NARKOTIKA JENIS SABU-SABU (Studi Putusan Mahkamah Agung Republik Indonesia Nomor 1866 K/Pid. Sus/2021).” Fakultas Hukum, universitas islam sumatera utara, 2025.
- NEGARA, UNDANG-UNDANG DASAR, REPUBLIK INDONESIA, and 1945. “UNDANG-UNDANG DASAR NEGARA REPUBLIK INDONESIA 1945” 1, no. 1 (1945).
- Nurdinna, Tita. “ANALISIS HUKUM TENTANG PERLINDUNGAN NASABAH PENYIMPAN DALAM LAYANAN INTERNET BANKING.” *LEGAL OPINION* 13,

- no. 1 (2025): 56–63.
- Palinggi, Sandryones, and Lutma Ranta Allolinggi. “Analisa Deskriptif Industri Fintech Di Indonesia: Regulasi Dan Keamanan Jaringan Dalam Perspektif Teknologi Digital.” *Ekonomi Dan Bisnis* 6, no. 2 (2019): 177–92.
- Pratama, Widhy Andrian. “Penegakan Hukum Terhadap Korupsi Di Era Modernisasi Digital.” *SEIKAT: Jurnal Ilmu Sosial, Politik Dan Hukum* 3, no. 1 (2024): 91–104.
- Pribadi, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data. “Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi,” no. 016999 (2022).
- Purnamasari, Dian Dewi. “Lembaga Pengawas Belum Terbentuk, Pengaduan Kebocoran Data Pun Jadi Tak Jelas.” 20 Des, 2024.
- Rahman, Rakhmadi, Sutedi Sutedi, Zunan Setiawan, Budanis Dwi Meilani, Shah Khadafi, Sulistyowati Sulistyowati, Ruli Utami, et al. *BUKU AJAR PENGANTAR SISTEM INFORMASI*. Edited by Efitra. Pertama. PT. Sonpedia Publishing Indonesia, 2023.
- Ramadhani, Eka Hero, I Ketut Agung Enriko, and Erika Lety Istikhomah Puspita Sari. “Kajian Strategik Manajemen Keamanan Siber Terhadap Proyek Telematika Di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional.” *Jurnal Indonesia: Manajemen Informatika Dan Komunikasi* 6, no. 1 (2025): 570–80.
- Salwa, Nikita Dewi Kurnia. “Tantangan & Hambatan Besar Yang Dihadapi CSIRT-BSSN Indonesia.” 18 Nov, 2024.
- Sulaeman, Diyu, and Anyelir Puspa Kemala. “Analisis Hukum Terhadap Tindak Pidana Pencurian Identitas Di Indonesia.” *ALADALAH: Jurnal Politik, Sosial, Hukum Dan Humaniora* 3, no. 2 (2025): 133–48.
- Telaumbanua, Taufik Hidayat. “Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif.” *Lex Privatum* 13, no. 1 (2024).
- UNIVERSAL, DEKLARASI, and HAK-HAK ASASI MANUSIA. “DEKLARASI UNIVERSAL HAK-HAK ASASI MANUSIA,” no. Iii (1948): 1–6.