

## ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

Oleh:

Arum Puspa Pradhipta<sup>1</sup>  
I Gusti Nyoman Krisnadi Yudiantara<sup>2</sup>

Universitas Udayana

Alamat: Jl. Pulau Bali No.1, Dauh Puri Klod, Kec. Denpasar Bar., Kota Denpasar, Bali  
(80114).

Korespondensi Penulis: [puspapradhipta2003@gmail.com](mailto:puspapradhipta2003@gmail.com),  
[krisnadiyudiantara@unud.ac.id](mailto:krisnadiyudiantara@unud.ac.id).

**Abstract.** *This analysis is concerned with evaluating the effectiveness of the current personal data protection regulations in Indonesia, particularly in handling crucial issues related to data leakage. The main objective is to assess the extent to which the existing legal framework is able to provide adequate protection to individuals' personal data, as well as identify and examine the government's role in resolving and responding to data leakage issues that are increasingly widespread in Indonesia. The methodology applied in this paper is normative law. In this approach, legal issues are analyzed in depth based on established legal theories and the resolution of legal problems is carried out in accordance with applicable legal principles. The main approaches that become the author's reference in answering the formulation of the problem are the statutory approach and the analysis approach. The findings of this analysis are expected to provide a comprehensive insight into the effectiveness of personal data legal protection regulations in Indonesia. In addition, this study will also provide concrete recommendations for the improvement of more comprehensive and adaptive data protection regulations, by considering and building on existing regulations to ensure stronger and more responsive data protection in the future.*

**Keywords:** *Personal Data, Data Leakage, Legal Protection, Personal Data Protection.*

# ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

**Abstrak.** Analisis ini berfokus pada evaluasi efektivitas regulasi perlindungan data pribadi yang berlaku di Indonesia, khususnya dalam menangani isu-isu krusial terkait kebocoran data. Tujuan utamanya adalah untuk mengkaji sejauh mana kerangka hukum yang ada mampu memberikan perlindungan yang memadai terhadap data pribadi individu, serta mengidentifikasi dan menilai peran pemerintah dalam mengatasi dan merespons permasalahan kebocoran data yang semakin marak terjadi di Indonesia. Metodologi yang diterapkan dalam penulisan ini adalah hukum normatif. Dalam pendekatan ini, permasalahan hukum dianalisis secara mendalam berdasarkan pada teori-teori hukum yang telah mapan dan penyelesaian masalah hukum dijalankan sesuai dengan kaidah-kaidah hukum yang berlaku. Pendekatan utama yang menjadi acuan penulis dalam menjawab rumusan masalah adalah pendekatan undang-undang dan pendekatan analisis. Temuan dari analisis ini diharapkan dapat memberikan wawasan yang komprehensif tentang efektivitas regulasi perlindungan hukum data pribadi di Indonesia. Selain itu, studi ini juga akan memberikan rekomendasi konkret untuk peningkatan regulasi perlindungan data yang lebih komprehensif dan adaptif, dengan mempertimbangkan dan membangun dari regulasi yang sudah ada guna memastikan perlindungan data yang lebih kuat dan responsif di masa depan.

**Kata Kunci:** Data Pribadi, Kebocoran Data, Perlindungan Hukum, Perlindungan Data Pribadi.

## LATAR BELAKANG

Seiring dengan berevolusinya zaman, tanpa disadari perkembangan industri digital sudah merambah sangat dalam ke setiap aspek kehidupan masyarakat modern dan sudah menjadi elemen yang tidak terpisahkan dengan kehidupan sehari-hari di masyarakat. Kemajuan industri digital sudah memberikan dampak perubahan yang revolusioner pada kehidupan manusia, mulai dari komunikasi sehari-hari hingga bisnis serta pekerjaan yang kompleks dan rumit. Tidak dapat dipungkiri bahwa dunia digital telah membentuk ulang tatanan sosial dan budaya kita. Dalam era digital yang pesat ini, perusahaan yang tidak mampu bertransformasi secara digital akan tertinggal. Transformasi digital yang mendalam telah mengubah pandangan Masyarakat dan menciptakan peluang-peluang baru, sekaligus menghadirkan tantangan yang kompleks. Perubahan ini tidak hanya memengaruhi cara perusahaan menghasilkan produk dan

layanan, tetapi juga cara mereka berinteraksi dengan pelanggan, karyawan, dan mitra bisnis. Dapat dipahami bahwa Integrasi teknologi yang semakin dalam ini merupakan alat yang dapat menghadirkan kemudahan dan efisiensi yang tak terbantahkan pada kehidupan sehari-hari masyarakat. Berkembangnya teknologi telah memungkinkan masyarakat untuk melakukan beragam aktivitas secara *virtual* bahkan layanan publik dan pemerintahan pun semakin banyak yang bisa diakses secara *online*.

Dalam prosesnya, untuk menikmati akses ke layanan publik atau fasilitas digital lainnya seringkali diiringi dengan tuntutan untuk memberikan informasi data pribadi baik dari nama, alamat *email*, nomor telepon, ataupun bahkan Nomor Induk Kependudukan (NIK). Akan tetapi banyak Masyarakat yang tidak mengetahui seberapa pentingnya sebuah data pribadi untuk dilindungi. Banyak masyarakat yang kurang peduli terhadap data pribadi nya sendiri yang dengan mudah memberikan informasi data pribadi tanpa mempertimbangkan resiko yang akan didapatkan bahkan tak sedikit perusahaan atau lembaga pelayanan yang kurang paham untuk mengelola data pribadi mereka dengan baik. Ketidapahaman dan kurangnya edukasi masyarakat terkait perlindungan data pribadi itulah yang menyebabkan banyak terjadi serangan siber seperti pembajakan atau penipuan yang dilakukan via SMS. Serangan yang muncul tersebut bisa terjadi karena terdapat kebocoran data pribadi. Adanya kebocoran data merupakan salah satu masalah penting untuk diatasi sebab Masyarakat dikhawatirkan dapat menjadi sasaran kejahatan serangan siber. Di lansir dari *CNN Indonesia*, *SAFEnet* mengatakan bahwa serangan siber di Indonesia mengalami kenaikan sebesar dua kali lipat dengan jumlah 61 kali kasus selama periode Januari hingga Maret pada tahun 2024.

Salah satu masalah terkait kebocoran data terbesar di Indonesia berlangsung pada tahun 2021, bahwa data pribadi 222,5 juta peserta BPJS Kesehatan bocor dan dijual di rate forum akibat celah keamanan pada sistem informasi BPJS memudahkan *hacker* untuk melakukan pembobolan data. Selain itu pada tahun 2018, terjadi kasus kebocoran data KTP elektronik sebanyak 191 juta penduduk di Indonesia. Bahkan Pusat Data Nasional yang dikelola Kominfo sebagai lembaga pemerintahan yang salah satu fungsinya melakukan kepengurusan terkait *Security Operation Center* (SOC) untuk pengamanan informasi dan komunikasi juga sempat diserang *Ransomware* yang menyebabkan banyak layanan publik yang terganggu. Ironisnya, lembaga-lembaga resmi yang seharusnya memiliki standar keamanan data yang sangat tinggi, masih saja menjadi

## ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

sasaran empuk para peretas. Hal ini juga diterangkan oleh Peneliti *Center for Indonesian Policy Studies* (CIPS).

Muhammad Nidhal dalam keterangan resmi yang dilansir dari *Media Indonesia* bahwa “Memang tidak ada sistem IT yang bebas dari ancaman kebocoran data dan serangan siber. Akan tetapi dalam konteks Indonesia, tingginya kejadian kebocoran data, khususnya dalam instansi pemerintah, disebabkan oleh setidaknya tiga hal, yaitu infrastruktur siber yang lemah, pelaksanaan regulasi Perlindungan Data Pribadi (PDP) dan keamanan siber yang belum optimal, serta kurangnya kesadaran pemilik data dan ahli siber.”<sup>1</sup> Sayangnya, baik masyarakat umum maupun lembaga pemerintahan masih belum sepenuhnya memahami implikasi hukum dari pelanggaran data pribadi. Hal ini menunjukkan bahwa pentingnya pemahaman hukum mengenai perlindungan data pribadi. Pada dasarnya, cukup banyak faktor yang bisa menyebabkan kebocoran data. Dari sejumlah literatur, penulis mengkategorikan tiga faktor utama penyebab kebocoran data antara lain kesalahan manusia (*human error*), serangan piranti lunak ilegal, dan tipuan psikologis melalui rekayasa sosial.<sup>2</sup>

Meskipun telah terdapat regulasi perlindungan data pribadi, namun pelaksanaannya masih menghadapi berbagai kendala. Hal ini menunjukkan adanya gap antara norma hukum dan praktik di kenyataannya. Analisis penelitian ini diharapkan dapat memberikan rekomendasi perbaikan terhadap regulasi yang ada, sehingga perlindungan data pribadi di Indonesia dapat lebih efektif. Kurangnya kesadaran masyarakat dan pelaku bisnis akan pentingnya perlindungan data pribadi, serta lemahnya penegakan hukum, menyebabkan Undang-Undang Perlindungan Data Pribadi belum mampu mencegah maraknya pelanggaran data pribadi dan serangan siber. Meskipun Indonesia sudah memiliki Undang-Undang Perlindungan Data Pribadi, namun permasalahan pelanggaran data pribadi serta serangan siber masih terus terjadi, mengindikasikan adanya kesenjangan antara regulasi, penegakan hukum yang lemah, dan kurangnya kesadaran masyarakat terhadap pentingnya perlindungan data pribadi. Pada analisis ini, penulis terfokus pada kasus kebocoran data dan analisis yang lebih mendalam

---

<sup>1</sup> Atalya Puspa. (2024). *Media Indonesia*. Kebocoran Data Imbas Minimnya Sanksi Tegas untuk Instansi Pemerintah. 24 November 2025.

<sup>2</sup> Mahmud Ashari. (2022). *DJKN Kemenkeu*. Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berhaga adalah Data Pribadi. 24 November 2025.

bagaimana UU PDP yang sudah disahkan dapat ditingkatkan agar lebih efektif dengan mengidentifikasi apakah ada kekosongan norma, kekaburan norma ataupun konflik norma.

## **METODE PENELITIAN**

Metodologi penelitian yang diterapkan dalam analisis adalah dengan menerapkan metode penelitian normatif. Metode normatif merupakan pendekatan yang melibatkan analisis dan pendekatan terhadap norma-norma hukum yang berlaku dan relevan dalam konteks perlindungan data pribadi. Dalam uraian, penulis melakukan analisis terhadap norma yang memiliki relevansi dengan persoalan yang diangkat penulis yaitu Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi guna memahami tujuan, ruang lingkup, dan persyaratan yang terkandung di dalamnya serta untuk mengidentifikasi apakah terdapat kekosongan norma, kekaburan norma, dan konflik norma yang mungkin terjadi.

## **HASIL DAN PEMBAHASAN**

### **Peran Kementerian Komunikasi dan Informasi sebagai Regulator, Fasilitator dan Pelindung dalam Dunia Digital.**

Kementerian Komunikasi dan Informasi memiliki peran utama untuk mengurus pemerintahan di bidang komunikasi dan informatika yang meliputi segala hal yang berkenaan dengan pengelolaan, pengembangan, dan utilisasi teknologi informasi dan komunikasi (TIK) salah satunya mengelola serta melindungi data pribadi masyarakat. Dilansir dari *website* resmi Kominfo, menjelaskan bahwa Kemkominfo memiliki kewajiban untuk menetapkan kebijakan dan merumuskan regulasi di bidang pengelolaan sumber daya perangkat informatika termasuk penyelenggaraan dan penatakelolaan aplikasi serta pengelolaan informasi dan komunikasi publik. Selain menetapkan regulasi, Kemkominfo juga bertugas untuk melaksanakan dan mengawasi kebijakan tersebut serta melakukan pelaksanaan bimbingan serta *supervise* atas pelaksanaannya. Terkait pengelolaan barang milik atau kekayaan negara merupakan kewajiban dari Kementerian komunikasi dan informatika.

Pada era digital yang semakin pesat ini, peran kominfo sangat dibutuhkan sebagai regulator, fasilitator, dan pelindung dalam dunia digital yang semakin kompleks dan

## ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

rumit. Adanya Kominfo memastikan bahwa pemanfaatan teknologi digital di Indonesia dilakukan secara bertanggung jawab, aman, dan memberikan manfaat bagi masyarakat luas. Akan tetapi hal ini tidak menjamin terciptanya suatu keamanan dan manfaat bagi Masyarakat. Berdasarkan laporan *Data Breach Investigation Report* mendefinisikan kebocoran data sebagai peristiwa gangguan keamanan yang menyebabkan terungkapnya data data tertentu kepada pihak yang tidak berwenang. Di Indonesia, kasus kebocoran data sudah sangat marak terjadi. Bahkan setingkat lembaga resmi negara seperti Kominfo yang mengelola Pusat Data Nasional juga pernah mengalami kasus kebocoran data. Institusi pemerintah yang seharusnya memiliki tingkat keamanan data yang tinggi, nyatanya masih rentan terhadap serangan siber apalagi masyarakat.

Dalam menghadapi kasus kebocoran data yang sudah marak terjadi itulah yang mendasari Kemkominfo sebagai lembaga yang memiliki kewenangan dalam mengawasi dan mengelola data negara untuk merumuskan Undang-Undang tentang Perlindungan Data Pribadi, sebab masalah kebocoran data atau dikenal sebagai *data breach* tidak bisa dibiarkan begitu saja dan penting untuk dilindungi. Dalam Naskah Akademik UU PDP, menerangkan “Hak atas privasi melalui perlindungan data pribadi adalah elemen kunci bagi kebebasan dan martabat individu”.<sup>3</sup> Terkait Rancangan Undang-Undang Perlindungan Data Pribadi sudah didiskusikan mulai tahun 2016. Akan tetapi pembahasan terkait Rancangan UU PDP baru dimulai pada tahun 2020. Rancangan UU PDP sangat ditunggu-tunggu Masyarakat lantaran hampir seluruh aktivitas masyarakat tidak dapat dipisahkan dari kehidupan digital. Pada 20 September 2022, Rancangan UU PDP disahkan menjadi Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) dan mulai diundangkan pada 17 Oktober 2022.

Dilansir dari Katadata Indonesia, Menurut Menkominfo Johnny G. Plate dalam konferensi persnya menyatakan bahwa UU PDP disiapkan untuk seluruh pihak yang memproses data Masyarakat. Dengan kata lain, UU PDP berlaku kepada seluruh pihak yang memproses data masyarakat baik perseorangan maupun korporasi. Selain itu dilansir dari *Ditjen IKP Kominfo*, Ketua Komisi 1 DPR Meutya Viada Hafid mengharapkan dengan adanya UU PDP dapat menghentikan kasus-kasus kebocoran data

---

<sup>3</sup> Muhammad Yudistira dan Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang Undang No. 27 Tahun 2022 Oleh Kominfo”. *UNES Law Review*. 2(4).9-10

yang terjadi di Masyarakat. Idealisme hukum dari UU PDP diwujudkan melalui tujuan pengaturan yang tercantum dalam Naskah Akademik yakni: Pertama, untuk melindungi dan memberikan jaminan atas hak pokok warga negara yang berhubungan dengan privasi data pribadi; kemudian, membangkitkan kesadaran hukum masyarakat agar menghormati hak atas privasi setiap individu; Ketiga, memberikan jaminan kepada masyarakat untuk dapat memperoleh jasa layanan dari pemerintah, pelaksana usaha, hingga organisasi kemasyarakatan lainnya; Keempat, menghindarkan rakyat Indonesia dari seluruh aspek eksploitasi pemanfaatan negara lain terhadap keberadaan data pribadi warga negara Indonesia; Kelima, mengembangkan laju tumbuhnya industri teknologi, informasi, dan komunikasi.<sup>4</sup>

Adanya UU PDP untuk mendorong masyarakat agar memiliki pemikiran bahwa pentingnya perlindungan terkait data pribadi. Dengan memiliki landasan hukum yang jelas tentu setidaknya dapat memberikan dampak kepada masyarakat untuk lebih waspada. Walaupun sebelum adanya UU PDP, juga sudah berlaku Undang-Undang yang relevan dengan perlindungan data pribadi antara lain ketentuan yang terdapat di dalam Pasal 26 UU No. 19 Tahun 2016 tentang Perubahan Atas UU No. 11 Tahun 2008 UU ITE, Permen Kominfo No 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, serta PP No. 80 Tahun 2019 terkait Perdagangan Melalui Sistem Elektronik.<sup>5</sup> Akan tetapi regulasi-regulasi yang sudah ada faktanya belum dapat mengatasi kasus kasus kebocoran data dengan baik.

Hisbulloh (2021) menekankan bahwa dengan memiliki undang-undang yang spesifik dan komprehensif, Indonesia dapat menciptakan dasar yang kuat untuk perlindungan data pribadi dalam menghambat kebocoran data, dan menjamin keamanan informasi pribadi warga negara. Bukan hanya untuk melindungi privasi individu, namun juga untuk menumbuhkan kepercayaan masyarakat terhadap pemanfaatan teknologi digital juga mendukung pembangunan ekonomi digital di Indonesia.<sup>6</sup>

---

<sup>4</sup> Naufal Rizqiyanto, Azmi Fathu Rohman, dan Faiz Al-Haq Maulabeta Raya. (2024). Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Media Hukum Indonesia (MHI). (2) 2. Hlm 9

<sup>5</sup> Inaz Indra Nugroho, Reza Pratiwi, dan Salsabila Rahma Az Zahro. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia. PMHI Law Journal. 1 (2) 10-13

<sup>6</sup> Naylawati Bahtiar. (2022). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. Development Policy and Management Review (DPMR). 2 (1): 91

# ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

## UU PDP sebagai Solusi dalam Menghadapi Kasus Kebocoran Data di Indonesia

Resmi disahkannya UU PDP sebagai naungan hukum utama perlindungan terhadap data pribadi masyarakat Indonesia pada 20 September 2022 merupakan tonggak Sejarah kemajuan di Indonesia terkait perlindungan data pribadi. UU PDP memuat 16 BAB serta 76 Pasal mencakup kejelasan rumusan mengenai definisi data pribadi, menjelaskan prinsip, dasar hukum, perlindungan mengenai hak subjek data pribadi dan kewajiban bagi pengendali dan pengolah data. Pada pasal 1 UU PDP menjabarkan bahwa yang dapat dikatakan sebagai data pribadi ialah “Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non elektronik.” Terdapat dua kategori yang dapat dikatakan sebagai data pribadi yaitu spesifik dan umum. Terkait artian dari sistem elektronik itu adalah suatu data diproses atau dikelola melalui sistem elektronik seperti ponsel ataupun komputer sedangkan non elektronik itu sendiri menggunakan dokumen fisik yang lebih manual. Dengan kata lain sistem itu sendiri mengacu pada bagaimana suatu data dapat diproses ataupun diakses.

Sedangkan Perlindungan data pribadi itu sendiri dijelaskan dalam Pasal 1 ayat 2 yaitu “Perlindungan data pribadi adalah keseluruhan upaya untuk melindungi data pribadi dalam rangkaian pemrosesan data pribadi guna menjamin hak konstitusional subjek data pribadi.” Konsep perlindungan data mengimplikasikan bahwa subjek data pribadi mempunyai suatu hak khusus yang dapat menentukan suatu Keputusan terkait data yang ingin dibagikan atau ditukarkan.<sup>7</sup> Subjek data pribadi tersebut adalah seseorang atau korporasi yang memiliki data pribadi.

Dijelaskan dalam BAB IV terkait hak yang dimiliki oleh subjek data pribadi bahwa berhak untuk melengkapi data, memperoleh informasi terkait transparansi identitas, tujuan permohonan dan kebutuhan suatu data pribadi, serta akuntabilitas para pihak yang mengajukan permintaan informasi data pribadi. Serta memiliki hak mendapatkan akses salinan informasi terkait data pribadi dan memiliki hak mengakhiri atau menghapus data pribadi. Dalam Pasal 12 ayat 1 juga diterangkan bahwa Undang-

---

<sup>7</sup> Sekaring Ayumeida Kusnadi, Andy Usmina Wijaya. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. JA: Jurnal Al-Wasath. 2(1) 22

Undang-Undang Perlindungan Data Pribadi (UU PDP) mengatur hak untuk menuntut secara hukum serta meminta kompensasi atau ganti rugi jika data pribadinya dilanggar. Namun, undang-undang ini belum menjelaskan secara rinci kepada siapa gugatan tersebut dapat diajukan, misalnya apakah ke pengadilan, lembaga perlindungan data pribadi, atau pihak lain. Selain itu, mekanisme atau prosedur yang harus dilalui dalam proses gugatan juga belum dijelaskan secara spesifik.

Berdasarkan pendapat Warren dan Brandeis, privasi merupakan hak individu untuk menikmati hidup dan menuntut perlindungan privasi.<sup>8</sup> Dalam hal ini, yang melindungi dan mengatur data para subjek data pribadi disebut dengan pengendali data pribadi yang menentukan tujuan data pribadi digunakan (menetapkan tujuan dan cara). Sedangkan prosesor atau pengolah data ialah pihak yang mengolah data sesuai dengan instruksi dari pengendali data pribadi. Pada Pasal 19 diterangkan bahwa subjek pengendali data itu termasuk individu, lembaga publik dan lembaga internasional. Terkait kewajiban dalam pemrosesan data dapat dilihat pada BAB VI UU PDP yang dimana mewajibkan pengendali data atau prosesor data untuk menerapkan tahapan langkah teknis dan organisasional yang memadai untuk melindungi suatu data pribadi. Selain itu, pengendali data dan pengolah data memiliki kewajiban memilih pejabat atau petugas yang memiliki fokus fungsi pada perlindungan data pribadi. Dengan kata lain bahwa saat pengendali dan prosesor melaksanakan tugasnya harus ada pejabat pelindung data pribadi yang bertanggung jawab untuk memastikan dan memantau bahwa semua aktivitas pengolahan data pribadi dilakukan sesuai dengan ketentuan UU PDP dan harus memiliki profesionalitas dalam hal melindungi data pribadi.

Namun, dalam UU ini tidak dispesifikasikan secara detail terkait petugas atau pejabat pelindung data pribadi tersebut. Hal ini dapat menimbulkan multitafsir dan bisa siapa saja tergantung lembaganya. Jika setiap lembaga memiliki interpretasi yang berbeda-beda mengenai kualifikasi dan tanggung jawab seorang Pejabat pelindung data pribadi, maka kualitas perlindungan data yang diberikan oleh masing-masing lembaga juga akan berbeda-beda. Terkait batas-batas tanggung jawab pejabat pelindung data pribadi dapat menjadi tidak jelas, Sehingga menimbulkan kesulitan untuk menentukan siapa yang bertanggung jawab jika terjadi pelanggaran perlindungan data. Pemerintah

---

<sup>8</sup> *Ibid.*

## ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

perlu segera mengeluarkan peraturan pelaksana yang lebih detail, yang mengatur secara spesifik mengenai kualifikasi, tugas, dan tanggung jawab Pejabat pelindung data pribadi.

Dalam rangka penegakan hukum, UU PDP menjelaskan terkait sanksi administratif dan sanksi pidana bagi pelanggar<sup>9</sup>. Dalam hal ini, sanksi merupakan alat untuk mendorong kepatuhan terhadap suatu norma dan merupakan sebuah pertanggungjawaban akibat melakukan pelanggaran terhadap regulasi yang berlaku. Akan tetapi sanksi dalam UU PDP ini tidak didefinisikan secara rinci dan dapat menimbulkan multitafsir. Sanksi administratif pada UU PDP diatur pada BAB VIII pasal 57 merupakan sebuah acuan hukum dalam menjatuhkan sanksi dalam bentuk administratif yang berupa peringatan tertulis, penghentian sementara proses pengolahan data, penghapusan data pribadi dan denda administratif. Hal ini tercantum dalam Pasal 57 ayat 2 BAB VIII.

Dalam BAB VIII ini tidak dijelaskan secara rinci lagi mengenai kriteria penetapan atau standar tertentu yang harus dipenuhi agar seseorang atau korporasi dapat ditetapkan melakukan suatu pelanggaran terhadap UU PDP. Tujuan dari adanya penerapan sanksi administratif itu sendiri adalah sebagai bentuk penegakan hukum untuk para pelanggar. Terkait pasal pemidanaan dalam UU PDP memiliki sedikit kemiripan terutama pada objek hukum nya dibandingkan dengan UU ITE. akan tetapi UU ITE memiliki cakupan yang lebih luas dibandingkan dengan UU PDP yang lebih berfokus pada perlindungan data pribadi individu atau korporasi.

Jika dilihat dari substansi substansi pada UU PDP dapat dilihat bahwa UU PDP pada dasarnya sudah sesuai dengan standar dan prinsip umum perlindungan data pribadi. Akan tetapi, kunci dari efektivitas UU PDP terletak pada lembaga yang mengawasi dan menjamin hak subjek serta kepatuhan pengendali. Pentingnya sebuah independensi dalam sebuah otoritas yang dibentuk dalam memastikan ketegasan dan keadilan dalam suatu penegakan hukum perlindungan data pribadi.

Pada BAB IX mengenai kelembagaan dijelaskan bahwa UU PDP juga akan mengatur bahwa akan ada lembaga otoritas yang merealisasikan perlindungan data

---

<sup>9</sup> Muhammad Yudistira dan Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang Undang No. 27 Tahun 2022 Oleh Kominfo. *UNES Law Review*. 2(4): 7

pribadi yang ditetapkan dan memiliki pertanggungjawaban kepada presiden. Pada Pasal 59 disebutkan bahwa tugas Lembaga adalah:

- a. perumusan dan penetapan kebijakan dan strategi perlindungan data pribadi yang menjadi panduan bagi subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi;
- b. pengawasan terhadap penyelenggaraan Perlindungan Data Pribadi;
- c. penegakan hukum administratif terhadap pelanggaran Undang-Undang ini; dan
- d. fasilitas penyelesaian sengketa di luar pengadilan.

Akan tetapi letak permasalahannya belum ada kejelasan apakah lembaga penegakan ini akan dibentuk sebagai lembaga baru yang independen atau konversi lembaga yang sudah ada. Negara-negara berkembang cenderung tidak memiliki kerangka kerja regulasi yang kuat untuk mengatur perlindungan data, sehingga memicu timbulnya dilema etika. Tidak tersedianya pedoman yang tegas mengakibatkan individu dan organisasi lebih rentan terhadap pelanggaran privasi dan penyalahgunaan data (Tovi dan Utama, 2013).<sup>10</sup> Pada hakikatnya pentingnya suatu otoritas penegak hukum untuk memastikan kepatuhan lembaga terhadap UU PDP serta memberikan sanksi jika suatu perseorangan atau korporasi melakukan pelanggaran dalam pemrosesan data. Dalam permasalahan ini, pentingnya suatu Lembaga independen yang kuat untuk memeriksa Lembaga dan tidak berpihak saat mengawala Lembaga.

## **KESIMPULAN DAN SARAN**

Indonesia menghadapi tantangan serius terkait perlindungan data pribadi. Pada tahun 2024, kasus kebocoran data meningkat drastis hingga dua kali lipat, menyoroti pentingnya kerangka hukum yang kuat untuk mengatasi pelanggaran data. Merespons kondisi ini, Kementerian Komunikasi dan Informatika (Kominfo), sebagai garda terdepan di sektor digital, menginisiasi perumusan regulasi yang kemudian disahkan menjadi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Kehadiran UU ini diharapkan menjadi fondasi hukum yang kokoh untuk menjamin keamanan data pribadi masyarakat. Secara substansi, UU PDP telah mencakup prinsip

---

<sup>10</sup> Naylawati Bahtiar .(2022). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*. 2 ( 1): 92

# ANALISIS REGULASI PERLINDUNGAN DATA PRIBADI TERHADAP KASUS KEBOCORAN DATA DI INDONESIA

dan standar penting dalam perlindungan data pribadi, termasuk hak dan kewajiban subjek, pengendali, serta pengolah data. Namun, efektivitas implementasinya masih memerlukan penyempurnaan, terutama terkait spesifikasi lembaga otoritas penegak hukum. UU PDP belum merinci secara jelas karakter, kedudukan, dan struktur kelembagaan otoritas ini, bahkan tidak menjelaskan secara spesifik pejabat yang berwenang menjadi penegak hukum atau pejabat perlindungan data pribadi. Ketiadaan kejelasan ini dapat berujung pada inkonsistensi praktik perlindungan data di berbagai institusi, melemahkan daya paksa UU PDP dalam melindungi data pribadi

Untuk mengatasi kelemahan ini dan memastikan UU PDP memiliki "taring" yang kuat, pembentukan lembaga otoritas yang independen menjadi krusial. Lembaga ini harus memiliki wewenang, struktur, dan personel yang jelas untuk menegakkan hukum secara efektif. Selain itu, diperlukan peraturan pelaksana yang lebih rinci dan komprehensif untuk menjabarkan mekanisme implementasi UU PDP di lapangan. Meskipun UU PDP telah ada, fakta bahwa pelanggaran data masih terus terjadi, bahkan di lembaga pemerintahan. Hal ini menunjukkan urgensi mekanisme implementasi dan penegakan hukum yang lebih kuat. Pemerintah dan seluruh pihak terkait harus memastikan bahwa regulasi tidak hanya berhenti pada tataran teks, tetapi juga diaplikasikan secara konsisten dan tegas untuk melindungi hak-hak privasi setiap individu.

## DAFTAR REFERENSI

### Artikel Jurnal

- Inaz Indra Nugroho, Reza Pratiwi, dan Salsabila Rahma Az Zahro. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber Di Indonesia. *PMHI Law Journal*. 1 (2) 10-13
- Indriana Firdaus. 2022. Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, 4(2).
- Mahmud Ashari. (2022). DJKN Kemenkeu. Belajar Dari Kebocoran Data Kredensial: Data Yang Paling Berharga adalah Data Pribadi. 24 November 2025.
- Muhammad Yudistira dan Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang Undang No. 27 Tahun 2022 Oleh Kominfo. *UNES Law Review*. 2(4). 9-10

- Naufal Rizqiyanto, Azmi Fathu Rohman, dan Faiz Al-Haq Maulabeta Raya. (2024). Politik Hukum Pembentukan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Media Hukum Indonesia (MHI)*. (2) 2. Hlm 9
- Naylawati Bahtiar .(2022). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*. 2 ( 1): 92
- Naylawati Bahtiar. (2022). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR)*. 2 (1): 91
- Nela Mardiana & Meilan Arsanti S.Pd., M.Pd. (2023). Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*. 16 (1)
- Nurhidayati, Sugiyah, dan Kartika Yuliantari. 2021. Pengaturan Perlindungan Data Pribadi dalam Penggunaan Aplikasi PeduliLindungi. *Widya Cipta: Jurnal Sekretari dan Manajemen*, 5(1).
- Sekaring Ayumeida Kusnadi, Andy Usmina Wijaya. (2021). Perlindungan Hukum Data Pribadi Sebagai Hak Privasi. *JA: Jurnal Al-Wasath*. 2(1) 22
- Muhammad Yudistira dan Ramadani. (2023). Tinjauan Yuridis Terhadap Efektivitas Pennanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang Undang No. 27 Tahun 2022 Oleh Koinfo. *UNES Law Review*. 2(4): 7

### **Sumber Dari Internet Dengan Nama Penulis**

- Atalya Puspa. (2024). Media Indonesia. Kebocoran Data Imbas Minimnya Sanksi Tegas untuk Instansi Pemerintah. [Kebocoran Data Imbas Minimnya Sanksi Tegas untuk Instansi Pemerintah](#) yang diakses pada 24 November 2025.