takuana
JURNAL PENDIDIKAN, SAINS, DAN HUMANIORA

e-ISSN: 2829-4831 | p-ISSN: 2829-4955

Vol. 4 No. 3, October-December 2025
Pages 876-887

Urgensi Penerapan UU PDP Nomor 27 Tahun 2022 dalam Pertanggungjawaban Hukum atas Kasus Kebocoran Data NPWP

The Urgency of Implementing Personal Data Protection Law No. 27 of 2022 in Legal Accountability for NPWP Data Leakage Cases

Kaharuddin, Nindia Rifdah Fakhirah*, Cyrill Milanesta Hisyam, Aura Prameswari Wirasmara

Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia

* 2410611042@mahasiswa.upnvj.ac.id (Primary Contact)

A B S T R A C T

Technological advancements and the growing digitalization of public services have significantly increased the processing of citizens' personal data. However, this situation also increases the risk of data leaks, as demonstrated by the leak of Taxpayer Identification Numbers (NPWP) that has affected millions of individuals since September 2024. This study examines the regulatory framework for personal data protection based on Law No. 27 of 2022, evaluates the urgency of its implementation in preventing and responding to data breaches, and analyzes the legal implications for parties that fail to protect personal data. Using a normative juridical method and a statutory approach, the findings show that Law Number 27 of 2022 provides comprehensive regulations for all stages of personal data management and imposes administrative, civil, and criminal sanctions for violations. However, law enforcement still faces challenges in the form of low public legal awareness, weak monitoring mechanisms, limited cross-sector coordination, and the absence of precedents for imposing sanctions and strict legal accountability mechanisms in data breach cases such as NPWP, so that the restoration of data owners' rights has not been optimal. Therefore, strengthening institutional capacity and improving public education are crucial to ensuring effective protection of citizens' privacy in the digital age.

Keywords
Personal Data Protection, Legal Implications, Digitalization, Law Number 27 of 2022

Article History
Received: 2025-11-26
Accepted: 2025-12-09

Published by MAN 4 Kota Pekanbaru
DOI: 10.56113/takuana.v4i3.249

1. PENDAHULUAN

Di era sekarang perkembangan teknologi, informasi, dan komunikasi telah membawa perubahan signifikan terhadap pola aktivitas masyarakat, baik itu dalam bidang ekonomi, sosial, maupun administrasi pemerintahan. Digitalisasi layanan publik telah meningkatkan pengumpulan dan pengolahan data pribadi warga negara. Namun, kemajuan ini diikuti oleh

banyak kasus kebocoran data pribadi, di mana dalam beberapa tahun terakhir di Indonesia terdapat sejumlah kasus kebocoran data yang melibatkan jutaan informasi warga negara, termasuk identitas, rekening, hingga Nomor Pokok Wajib Pajak (NPWP), yang akhirnya menimbulkan keraguan dan menurunkan kepercayaan masyarakat terhadap sistem digital negara.

Dugaan kebocoran data NPWP yang mencakup jutaan data pribadi warga, termasuk pejabat negara, adalah salah satu kasus yang menarik banyak perhatian publik karena menyangkut data sensitif yang dikelola oleh lembaga negara (Rinjani & Firmansyah, 2025). Tepatnya pada tanggal 18–19 September 2024 disebut sebagai tanggal ketika sampel data tersebut mulai tersebar. Meskipun Direktorat Jenderal Pajak (DJP) mengklaim sistem internalnya aman, temuan data seperti NPWP yang tersebar luas menunjukkan masalah dalam pengelolaan data pribadi. Fenomena ini menunjukkan bahwa pengawasan keamanan data di Indonesia masih kurang. Di tengah pesatnya kemajuan teknologi digital, masyarakat mulai mempertanyakan kapasitas negara untuk melindungi data pribadi warganya (Della N, 2025).

Sebelum diberlakukannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), regulasi mengenai perlindungan data pribadi di Indonesia belum memiliki landasan hukum yang komprehensif dan kuat. Ketentuan terkait data pribadi terdapat secara terpisah dalam peraturan sektoral seperti Undang-Undang Informasi dan Transaksi Elektronik, peraturan di sektor perbankan, dan kebijakan internal beberapa lembaga. Namun, pengaturan sektoral tersebut belum memberikan standar pertanggungjawaban hukum yang tegas, termasuk lemahnya sanksi bagi pelanggaran dan belum adanya lembaga pengawas yang secara khusus berwenang dalam mengontrol dan menindak penyalahgunaan data pribadi. Hal ini menyebabkan standar perlindungan serta mekanisme penegakan hukum terhadap pelanggaran data pribadi menjadi tidak konsisten dan seringkali kurang efektif dalam pelaksanaannya.

Ketika UU PDP ditetapkan pada tahun 2022, ini menjadi tonggak penting dalam membangun sistem hukum yang melindungi data pribadi di Indonesia. Undang-undang ini mengatur secara menyeluruh tentang prinsip pemrosesan data, hak subjek data, dan tanggung jawab pengendali dan prosedur data, serta sanksi kepada yang melanggarnya. Regulasi ini menunjukkan bahwa negara berkomitmen untuk melindungi hak privasi warganya dan menyesuaikan standar nasional dengan norma internasional. Namun, meskipun undang-undang sudah ada, hal itu tidak serta merta menjamin perlindungan yang efektif (Setiawan & Najicha 2022). Dalam pelaksanaannya, UU PDP menghadapi beberapa tantangan, seperti tumpang tindih kewenangan antar lembaga, keterbatasan sumber daya, serta rendahnya kesadaran dari instansi publik maupun swasta dalam mengaplikasikan prinsip perlindungan data. Kondisi ini menunjukkan bahwa perlindungan data pribadi masih memerlukan keselarasan dan konsistensi dari institusional maupun aspek teknis (Manurung & Thalib, 2022).

Penerapan UU PDP dalam konteks kebocoran data NPWP menjadi sangat penting karena data pajak berkaitan dengan informasi yang bersifat pribadi dan rahasia karena memuat identitas serta kondisi ekonomi seseorang. Ketika data sampai bocor, risikonya sangat besar, tidak hanya potensi penyalahgunaan oleh pihak yang tidak bertanggung jawab tetapi juga dapat menggoyahkan kepercayaan masyarakat terhadap sistem perpajakan dan institusi pemerintah yang mengelolanya. Oleh karena itu, setiap pengendali data, termasuk lembaga pemerintah, harus mematuhi prinsip-prinsip dalam UU PDP, seperti keabsahan

dalam pengumpulan dan pemrosesan data, penerapan keamanan yang ketat untuk melindungi data, serta akuntabilitas dalam bertanggung jawab atas pengelolaan data tersebut.

Dengan demikian, perlindungan data pribadi dapat lebih optimal dan kepercayaan publik terhadap lembaga terkait tetap terjaga. Melalui penerapan UU PDP yang efektif, diharapkan dapat memperkuat dasar hukum dalam melindungi hak privasi setiap individu sekaligus berperan sebagai alat penting dalam meningkatkan kepercayaan masyarakat terhadap sistem digital nasional. Berdasarkan latar belakang tersebut, penelitian ini berfokus pada pengaturan perlindungan data pribadi sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022, urgensi penerapannya terhadap kasus kebocoran data NPWP, serta implikasi hukum bagi pihak yang lalai melindungi data pribadi sesuai ketentuan yang berlaku (Purnama & Alhakim 2021).

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan yang akan dikaji dalam penelitian ini dapat dirumuskan sebagai berikut; Pertama, bagaimana pengaturan kewajiban pengendali data dan sanksi atas kebocoran data pribadi dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi; kedua, mengapa penerapan Undang-Undang Perlindungan Data Pribadi menjadi penting dalam menangani kasus kebocoran data NPWP; ketiga, bagaimana implikasi hukum terhadap instansi atau pihak yang lalai melindungi data pribadi menurut ketentuan dalam UU PDP.

2. METODE

Penelitian ini menggunakan metode yuridis normatif, yaitu penelitian hukum yang berfokus pada pengkajian norma-norma hukum positif yang berlaku. Pendekatan yang digunakan meliputi pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*). Pendekatan perundang-undangan digunakan untuk menelaah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Informasi dan Transaksi Elektronik, serta peraturan pelaksanaan terkait lainnya. Sementara itu, pendekatan konseptual digunakan untuk memahami prinsip-prinsip dasar perlindungan data pribadi serta urgensi penerapan UU PDP dalam konteks kebocoran data NPWP.

Selain itu, penelitian ini secara khusus mengkaji asas akuntabilitas sebagai prinsip utama dalam pertanggungjawaban hukum atas pengelolaan data pribadi oleh instansi negara. Asas ini menegaskan bahwa pengendali data wajib memastikan seluruh proses pengumpulan, penyimpanan, pemanfaatan, hingga penghapusan data pribadi dilakukan sesuai ketentuan perundang-undangan serta standar keamanan yang memadai. Dalam konteks kebocoran data NPWP, asas akuntabilitas menjadi dasar untuk menilai apakah instansi yang mengelola data telah memenuhi kewajibannya dalam melindungi hak subjek data dan melakukan langkah-langkah pencegahan maupun penanganan atas insiden kebocoran data. Dengan demikian, pengkajian asas akuntabilitas dalam penelitian ini bertujuan untuk menilai efektivitas implementasi UU PDP dalam memberikan perlindungan dan kepastian hukum bagi pemilik data pribadi.

Sumber bahan hukum dalam penelitian ini terdiri dari bahan hukum primer, yakni peraturan perundang-undangan yang relevan, dan bahan hukum sekunder seperti buku, jurnal ilmiah, artikel, dan berita terkait kebocoran data. Seluruh bahan hukum tersebut dianalisis menggunakan teknik analisis deskriptif-analitis, yaitu dengan mendeskripsikan

ketentuan hukum yang berlaku dan menganalisis implikasinya terhadap penerapan perlindungan data pribadi di Indonesia.

3. HASIL DAN PEMBAHASAN

3.1. Pengaturan Perlindungan Data Pribadi Dalam Uu Nomor 27 Tahun 2022

Kasus dugaan kebocoran data Nomor Pokok Wajib Pajak (NPWP) yang terjadi pada September 2024 bahwa sistem perlindungan data pribadi di Indonesia masih kurang. Terdapat lebih dari enam juta data NPWP yang diyakini telah bocor, termasuk yang dimiliki pejabat negara. Subitmele membuat artikel berita yang dimuat di Liputan6.com dengan judul "6 Juta Data NPWP Bocor, Benarkah Pejabat Pemerintah Jadi Sasaran?" menjelaskan bahwa, meskipun pihak Direktorat Jenderal Pajak menyatakan bahwa sistem internal mereka aman, faktanya bahwa data tersebut tersebar luas sehingga menimbulkan pertanyaan tentang bagaimana mekanisme keamanan dan tanggung jawab pengelolaan data yang dijalankan oleh lembaga pemerintahan.

Peristiwa tersebut terjadi hampir bersamaan dengan berlakunya Undang-Undang Nomor 27 Tahun 2022 yaitu tentang Perlindungan Data Pribadi (UU PDP) yang mulai berlaku pada Oktober 2024. Hal ini menunjukkan bahwa UU PDP sangat penting untuk memastikan adanya kepastian hukum mengenai siapa yang bertanggung jawab, apa yang harus dilakukan pengendali data, serta bagaimana sanksi yang diberikan ketika terjadi kebocoran. Lebih dari sekadar penegakan sanksi, UU PDP juga menekankan bentuk pertanggungjawaban hukum yang terukur, seperti kewajiban pemberitahuan insiden kebocoran data kepada pemilik data dan otoritas terkait paling lambat dalam waktu 3 x 24 jam, kewajiban memastikan keamanan pengolahan data pribadi melalui standar teknis yang jelas, serta penyediaan mekanisme pemulihan bagi pemilik data terdampak. Sebelum hadirnya UU PDP, ketentuan tersebut tidak diatur secara tegas sehingga pemilik data tidak memiliki jaminan atas haknya ketika terjadi pelanggaran. Kemudian, UU ini sebenarnya telah disusun jauh sebelum kasus NPWP terjadi sebagai bagian dari penyesuaian terhadap perkembangan global, mengingat banyak negara telah terlebih dahulu memiliki regulasi perlindungan data pribadi seperti *General Data Protection Regulation* (GDPR) di Uni Eropa (Saly et al., 2023).

Secara substansial, UU PDP mengatur secara menyeluruh proses yang berkaitan dengan data pribadi, termasuk pengumpulan, penyimpanan, pemrosesan, dan penyebaran data pribadi. Setiap pengendali data, baik itu pemerintah maupun swasta wajib melaksanakan dan mematuhi prinsip-prinsip pengelolaan data secara sah, terbuka, dan bertanggung jawab. Prinsip-prinsip yang tercantum dalam Pasal 16 sampai dengan Pasal 21 UU PDP meliputi keabsahan data, pembatasan tujuan, keakuratan, keamanan, dan akuntabilitas. Di samping itu, UU PDP memberikan jaminan perlindungan terhadap hak-hak subjek data pribadi, termasuk hak untuk memperoleh informasi, memperbaiki data yang tidak akurat, menghapus data pribadi, serta menarik persetujuan atas penggunaan datanya. Sebaliknya, pengendali data berkewajiban menjaga kerahasiaan data pribadi dan wajib melaporkan setiap terjadi kebocoran kepada pihak berwenang paling lambat 3 hari kerja setelah diketahuinya pelanggaran tersebut.

Dalam rangka memastikan kepatuhan, UU PDP mengatur dua jenis pertanggungjawaban hukum, yaitu sanksi administratif dan sanksi pidana. Sanksi administratif tercantum dalam Bab XI Pasal 57–60, yang antara lain meliputi teguran

tertulis, penghentian sementara kegiatan pengolahan data, penghapusan data pribadi, denda administratif, hingga kewajiban pemulihan hak subjek data. Sementara itu, Bab XII mengatur sanksi pidana terhadap pihak yang dengan sengaja dan melawan hukum mengungkapkan atau menyebarluaskan data pribadi. Misalnya, Pasal 67 mengancam pidana penjara maksimal 6 (enam) tahun dan/atau denda maksimal Rp6 miliar terhadap pelaku yang membocorkan data pribadi (Mamonto, 2024).

Pengaturan ini mempertegas asas akuntabilitas, di mana setiap pengendali data memiliki kewajiban hukum menjaga keamanan data pribadi serta memberikan notifikasi insiden kebocoran paling lambat 3×24 jam kepada pemilik data sebagaimana diatur dalam ketentuan mengenai kewajiban perlindungan data (Pasal 46 jo. Pasal 51). Oleh karena itu, keberadaan UU PDP memberikan landasan hukum yang komprehensif untuk menentukan siapa yang bertanggung jawab dan bagaimana mekanisme penegakan hukum dilakukan ketika terjadi pelanggaran. Kasus kebocoran data NPWP menjadi bukti bahwa sebelum adanya ketegasan pengaturan ini, proses penanganan pelanggaran cenderung lambat dan tidak jelas kedudukan tanggung jawab hukumnya. Dengan berlakunya UU PDP, masyarakat kini memiliki dasar yuridis yang kuat untuk menuntut perlindungan serta pemulihan atas hak privasinya.

3.2. Urgensi Penerapan UU PDP Terhadap Kasus Kebocoran Data NPWP

Rangkaian insiden kebocoran data dalam beberapa tahun terakhir membuat posisi negara sebagai pengelola data publik dipertanyakan. Ketika jutaan data NPWP beredar di forum gelap pada 2024, situasi ini menjadi lebih serius, bukan hanya karena jumlah data yang besar tetapi karena jenis data ini sangat sensitif dan terkait langsung dengan aktivitas ekonomi dan juga identitas seseorang. Oleh karena itu, publik melihat bahwa sistem yang harusnya dipakai untuk menjaga informasi, justru malah tidak memberikan perlindungan yang memadai. Selain itu, lembaga yang bertanggung jawab atas data juga tidak memberikan penjelasan yang jelas tentang sumber kebocoran dan metode apa yang harus dilakukan untuk menanganinya. Dari sini terlihat bahwa selama mekanisme hukum dan teknisnya tidak menyatu dengan baik, maka kebocoran data bukan hanya mungkin terjadi tapi juga dapat sulit diselesaikan secara transparan. Situasi seperti ini menunjukkan bahwa ketiadaan standar penanganan insiden membuat penyelesaian kasus berjalan lambat dan tidak ada kejelasan kepada pemilik data. Karena itu, kebutuhan akan aturan yang tegas tidak dapat lagi ditunda.

Untuk itu, banyak analisis keamanan digital termasuk karya Kazee dan CISSReC, menunjukkan bahwa Indonesia telah berada di posisi lemah selama bertahun-tahun karena kurangnya standar keamanan data yang konsisten. Setiap lembaga, baik pemerintah maupun swasta, menggunakan metodenya sendiri. Tidak ada standar minimum, tidak ada sanksi yang jelas, dan tidak ada kewajiban untuk melaporkan pelanggaran. Akibatnya, setiap kali terjadi kebocoran, tidak jelas bagaimana menanganinya. Masyarakat hanya dapat menunggu dan melihat apa yang terjadi dengan data mereka. Ini adalah celah yang menunjukkan bahwa undang-undang yang kuat adalah kebutuhan penting untuk mempertahankan kepercayaan masyarakat, bukan sekadar tambahan. Dalam kondisi seperti ini, UU PDP menjadi penting karena untuk pertama kalinya Indonesia memiliki kerangka hukum yang mewajibkan kehati-hatian, transparansi, dan akuntabilitas dalam pengelolaan data. Maka dari itu, saat ini sangat penting untuk menerapkan UU PDP.

Dengan undang-undang ini, pengendali data memiliki tanggung jawab yang jelas, sesuatu yang sebelumnya tidak pernah ada di Indonesia karena UU PDP mewajibkan penerapan prinsip keamanan dari awal hingga akhir pemrosesan data, mewajibkan pemberitahuan insiden paling lambat tiga hari kerja, dan menyediakan mekanisme bagi pemilik data untuk menuntut penjelasan dan pemulihan, yang di mana lembaga tidak lagi dapat mengatakan "sedang menelusuri". Regulasi ini tidak hanya mengatur prosedur, tetapi juga mendorong budaya baru di dalam organisasi: pengelolaan data harus dianggap sebagai hak dasar yang dilindungi sebagai tugas administratif biasa. UU PDP juga memastikan bahwa pemilik data tidak lagi berada pada posisi pasif karena mereka memiliki hak memperoleh informasi, menolak pemrosesan tertentu, dan menuntut perbaikan ketika terjadi pelanggaran (Puspitasari et al., 2023).

Kasus NPWP menunjukkan betapa pentingnya hal ini. Tanpa UU PDP, sulit untuk menentukan siapa yang bertanggung jawab atas penyebaran data. Tidak ada standar minimum yang dapat digunakan untuk mengevaluasi seberapa baik sistem keamanan sebuah organisasi; audit juga tidak diperlukan. Situasi seperti ini menyebabkan penyelesaian kasus seperti NPWP lamban dan tidak pasti. Dengan keluarnya UU PDP, semua lembaga tidak lagi dapat berlindung di balik pernyataan umum. Jika kelalaian terbukti, ada risiko administratif dan pidana yang menanti, serta tanggung jawab hukum yang harus dipenuhi. Kehadiran UU PDP membuat setiap tindakan melalaikan keamanan data dapat ditindak dan tidak lagi dapat dianggap sebagai kesalahan prosedural biasa. Oleh karena itu, penerapan UU PDP sangat penting karena ada banyak kebocoran yang telah terjadi, bukan hanya satu kasus besar. Menurut UU PDP, setiap pengelola data harus bekerja dalam kerangka kerja yang sama, memiliki standar keamanan yang sama, dan memikul tanggung jawab yang sama. Dalam hal NPWP, UU PDP memberikan arahan tentang bagaimana peristiwa harus dilaporkan, hak pemilik data, dan bagaimana negara memastikan bahwa kebocoran tidak terulang lagi. Selain itu, UU PDP membuat Indonesia lebih sejalan dengan praktik global seperti GDPR, sehingga tata kelola data nasional tidak tertinggal dari standar internasional. Tanpa implementasi yang serius, negara hanya akan terus berada dalam posisi reaktif bertindak setelah kerusakan terjadi, bukan mencegahnya.

Selain karena kasus kebocoran NPWP memerlukan penjelasan tentang siapa yang bertanggung jawab, UU Nomor 27 Tahun 2022 sangat penting untuk diterapkan. Ini juga ditunjukkan oleh substansi undang-undangnya sendiri. UU PDP memasukkan fitur yang sebelumnya tidak ada di Indonesia, seperti definisi data pribadi yang jelas, kewajiban pengendali data untuk menjaga keamanan data, mekanisme pelaporan insiden dalam tiga puluh empat jam, hak subjek data untuk mendapatkan penjelasan dan meminta penghapusan data, dan sanksi administratif dan pidana untuk pelanggaran. Ketika terjadi kebocoran, struktur ini memberikan kepastian prosedural dan hukum, sehingga kasus tidak lagi bergantung pada kebijakan internal masing-masing instansi. Dengan kata lain, UU PDP dimaksudkan untuk memastikan bahwa penanganan kebocoran data termasuk NPWP dilakukan secara transparan, terukur, dan dapat dipertanggungjawabkan (Cenyvesta & Gunadi, 2024).

3.3. Implikasi Hukum Terhadap Instansi Yang Lalai Melindungi Data Pribadi

Implikasi hukum merupakan konsekuensi yang harus ditanggung oleh setiap pihak yang lalai dalam melindungi data pribadi sebagaimana diatur dalam peraturan perundang-undangan, termasuk UU Perlindungan Data Pribadi. Dalam konteks dugaan kebocoran data

NPWP, lemahnya sistem pengamanan informasi dan ketidaksiapan respons insiden menunjukkan kegagalan pengendali data dalam menerapkan prinsip keamanan data secara konsisten (Salsabila & Wiraguna, 2025). Kondisi ini mencerminkan adanya kelemahan institusional yang bersifat struktural, seperti keterbatasan teknologi keamanan, rendahnya kompetensi sumber daya manusia dalam tata kelola data digital, serta belum adanya standar keamanan terpadu yang berlaku seragam di seluruh lingkungan pengelola data perpajakan. Kegagalan tersebut menimbulkan potensi pertanggungjawaban hukum, karena pengendali data wajib menjamin kerahasiaan, integritas, dan ketersediaan data setiap warga negara, serta memastikan bahwa seluruh pemrosesan data berjalan sesuai ketentuan hukum. Dengan demikian, dugaan kebocoran NPWP menjadi ilustrasi konkret bahwa meningkatnya pemanfaatan teknologi digital belum diimbangi penerapan asas akuntabilitas dan keamanan data yang memadai, sehingga sanksi administratif maupun pidana dapat dikenakan apabila kelalaian terbukti terjadi.

Kelalaian dalam menjamin keamanan data dapat menimbulkan pertanggungjawaban hukum karena dianggap gagal memenuhi asas akuntabilitas dan kehati-hatian. UU PDP sendiri menempatkan pengendali data sebagai pihak utama yang dapat dimintai pertanggungjawaban atas kebocoran data, meskipun kebocoran tersebut terjadi karena kelemahan teknis atau serangan eksternal. Hal ini menunjukkan bahwa standar perlindungan data tidak lagi sekadar bersifat administratif, tetapi memiliki implikasi hukum yang mengikat sehingga setiap instansi dituntut mempersiapkan infrastruktur, prosedur darurat, dan mekanisme audit internal yang komprehensif (Sitorus et al., 2025).

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menetapkan sanksi administratif sebagai bentuk teguran dan peringatan bagi pengelolaan data pribadi yang dilakukan tanpa dasar yang sah. Sanksi tersebut juga dikenakan atas pelanggaran terkait kesesuaian tujuan pengelolaan data pribadi, serta pelanggaran dalam proses memperoleh persetujuan dari subjek data pribadi. Namun, ketika kelalaian dalam pengelolaan data pribadi menimbulkan kerugian nyata bagi masyarakat, misalnya pencurian identitas, kerugian finansial, ataupun penyebaran data sensitif, tanggung jawab dapat beralih ke ranah perdata. Subjek data berhak menuntut ganti rugi atas setiap kerugian yang ditimbulkan oleh pelanggaran, sehingga instansi harus menyediakan mekanisme kompensasi atau pemulihan. Dalam kondisi tertentu, terutama ketika ditemukan adanya unsur kelalaian berat atau pembiaran terhadap celah keamanan yang telah lama diketahui, tanggung jawab pidana dapat diberlakukan. Sanksi pidana tidak hanya ditujukan pada instansi sebagai entitas hukum, tetapi juga pejabat atau individu yang bertanggung jawab dalam proses pengelolaan data. Dengan demikian, sistem sanksi ini memberikan dorongan kuat agar suatu instansi benar-benar mengutamakan perlindungan data pribadi sebagai kewajiban utama.

Kasus-kasus kebocoran data yang terjadi di sejumlah negara memperlihatkan pola yang hampir serupa, yaitu lemahnya kesiapan lembaga publik dalam menjaga data masyarakat. Dalam jurnal Serambi Hukum, disebutkan bahwa instansi pemerintahan kerap menghadapi tantangan berupa keterbatasan anggaran keamanan siber, ketergantungan pada sistem yang sudah usang, dan kurangnya integrasi dalam pengelolaan data. Ketika terjadi kebocoran, dampaknya cenderung jauh lebih besar karena data yang dikelola oleh lembaga publik umumnya bersifat sensitif dan mencakup informasi dasar seluruh warga negara. Jika dicermati, kebocoran data pajak, kesehatan, atau data kependudukan di berbagai negara menunjukkan bahwa kelalaian institusi publik berdampak langsung pada menurunnya kepercayaan masyarakat terhadap pemerintah. Dalam konteks Indonesia,

tanggung jawab lembaga publik semakin berat karena UU PDP mewajibkan instansi pemerintah untuk menerapkan standar keamanan yang sama ketatnya dengan sektor swasta. Ketika lembaga publik gagal melindungi data pribadi, hal ini bukan hanya menimbulkan implikasi hukum, tetapi juga menciptakan krisis legitimasi dan memperlemah posisi negara dalam menjamin hak konstitusional warga atas privasi. Oleh sebab itu, studi kasus perbandingan yang dibahas dalam jurnal menegaskan pentingnya penguatan kapasitas kelembagaan, pembaruan perangkat digital, serta peningkatan pengawasan independen terhadap seluruh instansi pengelola data.

Subjek data berhak memperoleh perlindungan dan pemulihan ketika kebocoran data terjadi, dan hak tersebut harus diwujudkan melalui mekanisme yang transparan serta mudah diakses. Jurnal Serambi Hukum menjelaskan bahwa upaya perlindungan tidak hanya berhenti pada tahap pencegahan, tetapi juga mencakup tindakan korektif setelah insiden. Perlindungan bagi pemilik data meliputi hak untuk mengetahui bahwa datanya telah bocor, hak untuk meminta informasi mengenai penyebab pelanggaran, serta hak untuk mendapatkan langkah-langkah mitigasi dari instansi pengendali data. Selain notifikasi, instansi wajib menyediakan sarana pemulihan seperti pemulihan identitas digital, penonaktifan sementara akun yang berisiko, hingga bantuan teknis untuk mencegah penyalahgunaan lebih lanjut. Apabila kerugian telah terjadi, instansi juga harus memberi akses kepada subjek data untuk menempuh jalur pengaduan hukum, baik melalui proses administratif, gugatan perdata, maupun laporan pidana. Pemulihan hak subjek data sangat bergantung pada kesiapan lembaga dalam menindaklanjuti insiden secara cepat, terbuka, dan bertanggung jawab. Jurnal menegaskan bahwa tanpa mekanisme pemulihan yang kuat, perlindungan data pribadi akan kehilangan makna, sehingga implementasi UU PDP harus memastikan bahwa hak-hak masyarakat dijamin secara penuh dalam setiap tahapan penanganan insiden (Salsabila & Wiraguna, 2025).

3.4. Rekomendasi Penguatan Implementasi UU PDP

Kasus kebocoran data NPWP mengungkap masih adanya celah serius dalam penerapan UU PDP, terutama pada bagian-bagian yang seharusnya diatur lebih rinci melalui peraturan pelaksana. Banyak kewajiban yang tercantum dalam UU PDP bersifat normatif dan belum dibarengi petunjuk teknis yang dapat digunakan instansi pengendali data sebagai pedoman kerja. Ketiadaan standar keamanan yang terukur membuat setiap lembaga menerapkan sistem pengamanan data dengan kualitas berbeda-beda, sehingga risiko kebocoran menjadi lebih besar. Selain itu, mekanisme pelaporan insiden, cara melakukan audit internal, serta langkah-langkah mitigasi ketika terjadi kebocoran belum dibakukan dalam bentuk SOP lintas sektor. Kondisi ini menandakan bahwa sejumlah pasal dalam UU PDP membutuhkan turunan peraturan yang lebih spesifik agar implementasinya dapat berjalan konsisten dan tidak sekadar bergantung pada interpretasi masing-masing lembaga. Peraturan turunan tersebut juga diperlukan untuk menutup kesenjangan antara ketentuan hukum yang ideal dengan keadaan teknis di lapangan, terutama dalam hal pengamanan data yang dikelola institusi publik.

Beberapa dokumen menunjukkan bahwa beberapa institusi yang memproses data pribadi dalam jumlah besar ternyata belum mampu memenuhi standar perlindungan data yang layak. Hal ini memperlihatkan bahwa keberadaan lembaga pengawas data pribadi yang kuat dan berwenang adalah kebutuhan mendesak. Agar UU PDP dapat ditegakkan secara efektif, lembaga pengawas harus berdiri secara independen, bebas dari konflik

kepentingan, dan mempunyai otoritas melakukan pemeriksaan lapangan untuk memastikan seluruh entitas baik pemerintah maupun swasta benar-benar memenuhi standar yang ditetapkan. Lembaga ini idealnya juga memiliki kemampuan memberikan sanksi administratif, mewajibkan perbaikan sistem, dan melakukan evaluasi berkala terhadap mekanisme keamanan data. Tanpa struktur kelembagaan yang kuat, penegakan UU PDP berisiko tidak berjalan konsisten karena hanya mengandalkan itikad baik pengendali data. Penguatan kelembagaan ini juga penting untuk memastikan adanya tanggung jawab jelas apabila terjadi pelanggaran, sehingga perlindungan data pribadi masyarakat tidak lagi bergantung pada kemampuan internal lembaga masing-masing, tetapi dikawal oleh otoritas pengawas yang bekerja secara profesional dan terstandar.

Rendahnya tingkat pemahaman masyarakat mengenai keamanan data pribadi menjadi faktor yang memperbesar dampak insiden kebocoran data NPWP. Banyak individu yang tidak menyadari risiko penyalahgunaan data dan tidak mengetahui bagaimana cara melindungi informasi pribadinya ketika beraktivitas di ruang digital. Minimnya pemahaman tersebut membuat masyarakat lebih mudah menjadi korban kejahatan siber, seperti penipuan, phishing, serta pencurian identitas. Oleh karena itu, perlu dilakukan upaya sistematis untuk meningkatkan literasi hukum dan literasi digital masyarakat melalui edukasi publik, kampanye sosial, serta kurikulum pendidikan yang memasukkan aspek perlindungan data pribadi. Masyarakat harus diberi pemahaman mengenai hak-hak yang dilindungi dalam UU PDP serta bagaimana meminta pertanggungjawaban jika data mereka disalahgunakan. Dengan meningkatnya kesadaran dan keberdayaan masyarakat, pengendali data akan menghadapi tekanan sosial untuk menerapkan standar perlindungan data yang lebih baik. Peran aktif masyarakat juga dapat menjadi bentuk kontrol publik terhadap instansi pemerintah agar tidak mengabaikan prinsip akuntabilitas dalam mengelola informasi pribadi.

Ancaman kebocoran data memiliki karakter yang kompleks dan sering kali melibatkan banyak pihak, sehingga diperlukan suatu mekanisme pengawasan terpadu lintas sektor. Pemerintah, lembaga bisnis yang mengelola data pengguna, dan masyarakat sebagai pemilik data perlu bekerja dalam satu ekosistem yang saling mengawasi dan melengkapi. Model pengawasan ini dapat berupa audit bersama, pelibatan masyarakat sipil dalam memantau insiden kebocoran data, serta kerja sama antar lembaga dalam menyusun standar keamanan yang berlaku nasional. Pendekatan lintas sektor ini penting karena masing-masing pihak memiliki peran strategis: pemerintah memiliki kewenangan regulasi, sektor swasta memiliki kemampuan teknologi, dan publik memiliki fungsi kontrol sosial. Dengan pengawasan yang terintegrasi, implementasi UU PDP dapat berlangsung lebih transparan dan efektif, serta mampu menekan terjadinya kelalaian pengelolaan data pribadi di kemudian hari (Wibowo et al., 2025).

4. KESIMPULAN

Kasus kebocoran lebih dari enam juta data NPWP pada September 2024 mengungkap lemahnya perlindungan data pribadi di Indonesia dan menegaskan pentingnya keberlakuan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang mulai berlaku penuh pada Oktober 2024. Undang-Undang ini mengatur secara komprehensif seluruh proses pengelolaan data pribadi, mewajibkan pengendali data baik pemerintah maupun swasta, untuk mematuhi dan melaksanakan prinsip-prinsip pengelolaan data secara sah, transparan, dan bertanggung jawab, serta memberikan

perlindungan terhadap hak-hak subjek data pribadi. Regulasi tersebut juga menetapkan kewajiban pelaporan kebocoran dalam waktu tiga hari kerja dan memuat sanksi administratif hingga pidana, termasuk ancaman penjara enam tahun dan denda enam miliar rupiah. Dengan demikian, UU PDP menjadi payung hukum penting guna memastikan akuntabilitas pengelola data dan memberikan dasar hukum kuat bagi masyarakat untuk menuntut perlindungan atas data pribadinya.

Pemanfaatan teknologi digital yang semakin luas menuntut pengendali data untuk memiliki tanggung jawab hukum yang kuat, namun banyak instansi masih belum mampu menjamin keamanan data pribadi. UU PDP mengatur sanksi administratif bagi pelanggaran dasar pengelolaan data, sementara kerugian nyata akibat kelalaian dapat menimbulkan tanggung jawab perdata yang salah satunya berupa kewajiban ganti rugi. Dalam kasus kelalaian berat atau pembiaran terhadap celah keamanan, sanksi pidana bahkan dapat dikenakan kepada sebuah instansi maupun individu yang bertanggung jawab. Dengan struktur sanksi berlapis ini, UU PDP mendorong setiap pengendali data untuk benar-benar memprioritaskan perlindungan data pribadi.

Kasus kebocoran data NPWP menunjukkan bahwa implementasi UU PDP masih menghadapi banyak kelemahan, terutama karena ketiadaan peraturan pelaksana yang rinci, standar keamanan yang terukur, serta prosedur operasi standar lintas sektor untuk pelaporan dan mitigasi insiden. Kondisi ini semakin diperburuk oleh rendahnya kapasitas sejumlah instansi dalam memenuhi standar perlindungan data pribadi, minimnya literasi keamanan data di masyarakat, serta belum terbentuknya lembaga pengawas yang independen, berwenang, dan mampu menegakkan kepatuhan secara konsisten. Oleh karena itu, meskipun pengaturan dalam UU PDP telah memberikan landasan hukum yang kuat, efektivitasnya masih sangat bergantung pada kehadiran otoritas pengawas yang memiliki kemampuan untuk mengawasi, mengevaluasi, dan menjatuhkan sanksi secara tegas kepada setiap pelanggaran hukum. Dengan demikian, pembentukan lembaga pengawas independen menjadi langkah paling mendesak dan strategis untuk memastikan perlindungan data pribadi berjalan efektif, konsisten, serta memberikan kepastian hukum bagi seluruh masyarakat.

DAFTAR PUSTAKA

Kaharuddin. (2025). *Ilmu peraturan perundang-undangan: Pemahaman dasar dan struktur hukum* (1st ed.). Kencana.

Cenyvesta, M., & Gunadi, A. (2024). Konsep tanggung jawab negara terhadap kewajiban melindungi data pribadi masyarakat di Indonesia (studi kasus kebocoran data NPWP masyarakat Indonesia). *Jurnal Hukum Lex Generalis, 5*(12), 1–14.

Della N, D. T. (2025). Pengaruh kebocoran data wajib pajak terhadap kepercayaan dan kepatuhan perpajakan wajib pajak orang pribadi. *Jurnal Ilmiah Global Education, 6*(2), 436–446. https://doi.org/10.55681/jige.v6i2.3795

Mamonto, D. F. (2024). Analisis perlindungan hukum terhadap penyalahgunaan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Lex Privatum, 13*(4).

Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan yuridis perlindungan data pribadi berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati, 4*(2), 139–148. https://doi.org/10.36733/jshs.v4i2.5941

Purnama, T. D., & Alhakim, A. (2021). Pentingnya Undang-Undang perlindungan data pribadi sebagai bentuk perlindungan hukum terhadap privasi di Indonesia. *Jurnal Komunitas Yustisia, 4*(3), 1056–1064.

Puspitasari, D., Izzatusholekha, I., Haniandaresta, S. K., & Afif, D. (2023). Urgensi Undang-Undang perlindungan data pribadi dalam mengatasi masalah keamanan data penduduk. *Journal of Administrative and Social Science, 4*(2), 195–205. https://doi.org/10.55606/jass.v4i2.403

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan implementasi Undang-Undang Nomor 27 Tahun 2022 dan strategi penguatan perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum, 8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Salsabila, S., & Wiraguna, S. A. (2025). Pertanggungjawaban hukum atas pelanggaran data pribadi dalam perspektif Undang-Undang pelindungan data pribadi Indonesia. *Konsensus: Jurnal Ilmu Pertahanan, Hukum, dan Ilmu Komunikasi, 2*(2), 145–157. https://doi.org/10.62383/konsensus.v2i2.736

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., & Christie, M. (2023). Analisis perlindungan data pribadi terkait Undang-Undang Nomor 27 Tahun 2022. *Jurnal Serina Sosial Humaniora, 1*(3), 145–153.

Setiawan, H. B., & Najicha, F. U. (2022). Perlindungan data pribadi warga negara Indonesia terkait dengan kebocoran data. *Jurnal Kewarganegaraan, 6*(1), 976–982. https://doi.org/10.31316/jk.v6i1.2657

Sitorus, H. R. P., Lumbanbatu, D. P., Sidebang, D. D., Pratama, D. E., & Gaol, R. S. L. (2025). Tinjauan hukum dan upaya pencegahan terhadap kasus kebocoran data NPWP. *Aspirasi: Publikasi Hasil Pengabdian dan Kegiatan Masyarakat, 3*(4), 14–18. https://doi.org/10.61132/aspirasi.v3i4.1851

Wibowo, Y., Wulan, I. A. D. P., & Ismiyanto, I. (2025). Tinjauan yuridis tentang perlindungan data pribadi masyarakat pada era digitalisasi. *Jurnal Penelitian Serambi Hukum, 18*(1), 1–6. https://doi.org/10.59582/sh.v18i01.1216

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. https://peraturan.bpk.go.id/Details/238631

Subitmele, S. E. (2024, September 20). 6 juta data NPWP bocor, benarkah pejabat pemerintah jadi sasaran? *Liputan6.com*. https://www.liputan6.com/hot/read/5706751/6-juta-data-npwp-bocor-benarkah-pejabat-pemerintah-jadi-sasaran

Septian, B. (2022, August 26). Urgensi RUU PDP atas rentetan kasus kebocoran data. *Kazee Insight Blog*. https://blog.kazee.id/urgensi-ruu-pdp-atas-rentetan-kasus-kebocoran-data

Fajrin, Z. (2024, September 19). CISSReC tegaskan urgensi UU PDP setelah kebocoran data NPWP. *Gizmologi*. https://gizmologi.id/news/cissrec-urgensi-uu-pdp-kebocoran-data-npwp/

Dinas Komunikasi, Informatika dan Statistik Kota Cirebon. (2025, August 25). *UU PDP Nomor 27 Tahun 2022: Hak masyarakat dan urgensi mencegah kebocoran data pribadi*. https://dkis.cirebonkota.go.id/artikel/uu-pdp-nomor-27-tahun-2022-hak-masyarakat-dan-urgensi-mencegah-kebocoran-data-pribadi

Lembaga Studi dan Advokasi Masyarakat. (2024, September 19). *Dugaan kebocoran data pribadi subjek pajak, kesiapan pelaksanaan kepatuhan UU PDP mengkhawatirkan* [Press release]. https://www.elsam.or.id/siaran-pers/dugaan-kebocoran-data-pribadi-subjek-pajak–kesiapan-pelaksanaan-kepatuhan-uu-pdp-mengkhawatirkan

Sugangga, F. (2024, April 23). Mengoptimalkan keamanan data untuk perusahaan besar berdasarkan UU PDP (#1–Pembukaan). *SharingVision Insight*. https://sharingvision.com/insight/mengoptimalkan-keamanan-data-perusahaan-berdasarkan-uu-pdp/

Hardafi, S. N. (2025, July 9). Ketiadaan lembaga PDP: Celah hukum dalam perlindungan data pribadi. *HukumOnline*. https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp–celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/