Sanskara Hukum dan HAM
Vol. 4, No. 03, April 2026, hal. 275-284
ISSN: 2985-7775, DOI: 10.58812/shh.v4.i03

Analisis Yuridis Pasal 26 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap Kebocoran Data Digital di Indonesia

Sri Andrian[1], Arief Fahmi Lubis[2], Abdul Kholiq[3], Tiwuk Herawati[4]
[1] Universitas Islam Kebangsaan Indonesia, andriani30@gmail.com
[2] Sekolah Tinggi Hukum Militer, arieffahmilubis0@gmail.com
[3] Universitas 17 Agustus 1945 Semarang, abdulkholiqsh@gmail.com
[4] Universitas Muhammadiyah Malang, tiwukhera@umm.ac.id

Info Artikel

Article history:

Received Apr, 2026
Revised Apr, 2026
Accepted Apr, 2026

Kata Kunci:

GDPR; Kebocoran Data; Kerangka Hukum; Perlindungan Data Pribadi; Undang-Undang PDP Indonesia

Keywords:

Data Breach; GDPR; Indonesia PDP Law; Legal Framework; Personal Data Protection

ABSTRAK

Penelitian ini mengkaji Pasal 26 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) di Indonesia, dengan fokus pada ketentuan-ketentuannya terkait pelanggaran data digital. Seiring dengan meningkatnya penggunaan platform digital, risiko pelanggaran data pribadi pun semakin besar, sehingga perlindungan data pribadi menjadi isu krusial bagi para pembuat kebijakan. Pasal 26 menguraikan kewajiban pengendali dan pengolah data jika terjadi pelanggaran data, khususnya mewajibkan pemberitahuan segera kepada individu yang terkena dampak dan otoritas pengatur. Makalah ini melakukan analisis hukum normatif untuk menilai efektivitas ketentuan-ketentuan tersebut dalam melindungi data pribadi, dengan membandingkannya dengan standar internasional seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa. Analisis ini mengidentifikasi kelebihan, seperti kewajiban pemberitahuan kebocoran, namun juga menyoroti kelemahan, termasuk kurangnya tenggat waktu yang jelas untuk pelaporan kebocoran dan mekanisme penegakan hukum yang tidak memadai. Studi ini diakhiri dengan rekomendasi untuk memperkuat Undang-Undang Perlindungan Data Pribadi (PDP), termasuk memperjelas tenggat waktu pemberitahuan, meningkatkan sanksi, dan memperbaiki infrastruktur untuk pelaporan kebocoran serta penegakan hukum.

ABSTRACT

This study examines Article 26 of Law No. 27 of 2022 on Personal Data Protection (PDP Law) in Indonesia, focusing on its provisions related to digital data breaches. With the increasing use of digital platforms, the risk of personal data breaches has grown significantly, making data protection a critical issue for policymakers. Article 26 outlines the obligations of data controllers and processors in the event of a data breach, particularly requiring prompt notification to affected individuals and the relevant regulatory authority. This paper employs a normative legal analysis to assess the effectiveness of these provisions in safeguarding personal data, comparing them with international standards such as the European Union's General Data Protection Regulation (GDPR). The analysis identifies strengths, including the obligation to notify breaches, while also highlighting weaknesses, such as the absence of clear deadlines for breach reporting and insufficient enforcement mechanisms. The study concludes with recommendations to strengthen the Personal Data Protection Law, including clarifying notification timelines, enhancing sanctions, and improving infrastructure for breach reporting and law enforcement.

Corresponding Author:

Name: Sri Andrian
Institution: Universitas Islam Kebangsaan Indonesia
Email: andriani30@gmail.com

1. PENDAHULUAN

Di era digital saat ini, kemajuan teknologi yang pesat telah membawa perubahan signifikan di berbagai sektor, terutama dalam cara data pribadi dikumpulkan, diproses, dan disimpan. Peningkatan penggunaan platform digital dan keterhubungan sistem online telah menyebabkan lonjakan eksponensial dalam pelanggaran data pribadi, yang menimbulkan ancaman serius terhadap privasi, keamanan, dan integritas informasi pribadi individu. Akibatnya, perlindungan data pribadi telah menjadi perhatian utama bagi pemerintah, organisasi, dan individu. Menanggapi tantangan ini, Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sebuah langkah krusial dalam upaya melindungi data pribadi di era digital. Undang-undang ini menyediakan kerangka hukum yang komprehensif untuk mengatur tanggung jawab pengendali dan pemroses data, terutama dalam kasus kebocoran data (Lutrianto & Riswaldi, 2025).

Pasal 26 Undang-Undang PDP secara khusus mengatur pelanggaran data digital, mewajibkan pemberitahuan tepat waktu kepada individu yang terdampak dan otoritas terkait. Ketentuan ini meningkatkan transparansi dan akuntabilitas, yang esensial untuk membangun kepercayaan dan memastikan perlindungan data pribadi (Wijayanto & Indrayanti, 2025). Undang-Undang PDP menetapkan tanggung jawab yang jelas bagi pengendali dan pemroses data, memastikan mereka bertanggung jawab atas peran mereka dalam mengelola data pribadi. Kerangka hukum ini sangat penting untuk meningkatkan keamanan informasi pribadi di era ancaman siber yang semakin meningkat. Namun, terlepas dari kelebihannya, terdapat beberapa tantangan dalam penegakan yang efektif, terutama terkait kesiapan Indonesia untuk menerapkan kerangka ini sesuai dengan standar internasional seperti GDPR.

Meskipun Undang-Undang PDP selaras dengan standar global, terdapat beberapa celah yang dapat menghambat efektivitasnya. Misalnya, tidak adanya otoritas pengawas independen di Indonesia menjadi tantangan bagi pengawasan dan kepatuhan, yang bertolak belakang dengan mekanisme yang lebih kuat yang terdapat dalam GDPR (Simanjuntak, 2024). Selain itu, undang-undang ini menghadapi tantangan implementasi, termasuk rendahnya kesadaran masyarakat akan masalah perlindungan data dan infrastruktur keamanan data yang tidak memadai (Utomo, 2024). Perusahaan juga mengalami kesulitan dalam mematuhi peraturan, yang menekankan perlunya pendidikan dan pelatihan yang lebih baik untuk membantu mereka memenuhi persyaratan Undang-Undang PDP (Wijayanto & Indrayanti, 2025). Frekuensi serangan siber dan akses tidak sah terhadap data pribadi menekankan pentingnya memahami Pasal 26, memastikan bahwa data individu dilindungi dan bahwa pihak yang bertanggung jawab atas pelanggaran dimintai pertanggungjawaban.

Makalah ini bertujuan untuk melakukan analisis hukum normatif terhadap Pasal 26 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, dengan fokus pada

ketentuan-ketentuannya yang berkaitan dengan pelanggaran data digital. Dengan mengkaji teks hukum, interpretasi yudisial, dan praktik regulasi, studi ini berupaya mengevaluasi efektivitas kerangka hukum saat ini dalam menangani pelanggaran data di Indonesia. Selain itu, makalah ini membandingkan ketentuan Pasal 26 dengan standar perlindungan data internasional, seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, untuk menilai keselarasan dan kecukupan respons hukum Indonesia terhadap isu global pelanggaran data.

Pendahuluan ini menjadi landasan bagi analisis mendalam mengenai kewajiban hukum pengendali dan pengolah data dalam kasus pelanggaran data digital, ruang lingkup Pasal 26, serta implikasinya terhadap perlindungan data pribadi di Indonesia. Makalah ini juga akan mengeksplorasi potensi celah dalam kerangka hukum saat ini dan memberikan rekomendasi untuk meningkatkan pendekatan Indonesia dalam pengelolaan pelanggaran data digital.

2. TINJAUAN PUSTAKA

2.1. Perlindungan Data Pribadi: Perspektif Global

Undang-undang perlindungan data pribadi bertujuan untuk melindungi privasi individu dan memastikan penggunaan informasi pribadi mereka secara aman dan sah (Asija & Nallusamy, 2014; Banisar & Davies, 1999; Olayinka & Win, 2022). Secara internasional, berbagai kerangka hukum telah ditetapkan untuk mengatur pemrosesan data, dengan Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, yang berlaku sejak 2018, menjadi salah satu contoh paling menonjol. GDPR menetapkan standar tinggi untuk perlindungan data, dengan menekankan transparansi, akuntabilitas, dan hak individu untuk mengontrol data mereka, termasuk ketentuan mengenai pemberitahuan pelanggaran data yang mewajibkan pengendali data untuk memberi tahu individu yang terkena dampak dan otoritas regulasi mengenai pelanggaran yang dapat merugikan individu (Komisi Eropa, 2018). Wilayah lain, seperti Amerika Serikat dengan Undang-Undang Privasi Konsumen California (CCPA) dan Singapura dengan Undang-Undang Perlindungan Data Pribadi (PDPA), telah mengembangkan kerangka hukum serupa, yang membentuk wacana global tentang perlindungan data pribadi dan berfungsi sebagai model bagi negara-negara yang sedang menyusun peraturan mereka sendiri.

2.2. Undang-Undang Perlindungan Data Pribadi Indonesia (UU PDP)

Kerangka hukum Indonesia untuk perlindungan data pribadi telah berkembang seiring waktu, dengan berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang menandai tonggak penting. UU PDP bertujuan untuk memberikan perlindungan komprehensif terhadap data pribadi, mengatur pemrosesannya, dan memastikan bahwa hak privasi individu dihormati. Undang-undang ini berlaku bagi entitas publik dan swasta, termasuk yang mengumpulkan, memproses, dan menyimpan data pribadi, serta menetapkan mekanisme penegakan kepatuhan (Dewi, 2015; Yuniarti, 2019). Salah satu fitur utama Undang-Undang PDP adalah fokusnya pada tanggung jawab pengendali dan pemroses data. Entitas-entitas ini diwajibkan untuk mengambil langkah-langkah teknis dan organisasi yang sesuai guna melindungi data pribadi dari akses, penggunaan, atau pengungkapan yang tidak sah (Rosadi, 2018; Yuniarti, 2019). Undang-undang ini juga menetapkan sanksi bagi ketidakpatuhan, termasuk denda dan sanksi administratif lainnya. Pasal 26 secara khusus membahas pelanggaran data, menetapkan kewajiban pengendali dan pengolah data untuk memberitahukan baik individu yang terdampak maupun otoritas terkait mengenai pelanggaran tersebut secara tepat waktu dan transparan.

2.3. Pelanggaran Data Digital: Tantangan dan Tanggapan Hukum

Pelanggaran data digital telah menjadi masalah yang meluas di era digital, seiring meningkatnya frekuensi dan tingkat kerumitan serangan siber serta akses tidak sah terhadap data. Pelanggaran data terjadi ketika informasi pribadi diakses, diungkapkan, atau diperoleh tanpa izin, yang sering kali mengakibatkan kerugian signifikan bagi

individu, termasuk pencurian identitas, kerugian finansial, dan kerusakan reputasi (Natamiharja et al., 2022; Yuniarti, 2019). Tantangan yang ditimbulkan oleh pelanggaran data sangat terasa di negara-negara dengan ekonomi digital yang berkembang pesat, seperti Indonesia, di mana infrastruktur keamanan siber mungkin tertinggal dari laju kemajuan teknologi.

Tanggapan hukum terhadap pelanggaran data bervariasi di berbagai yurisdiksi, namun unsur-unsur umum meliputi persyaratan pemberitahuan, ganti rugi bagi individu yang terdampak, dan sanksi bagi yang tidak mematuhi. Seperti disebutkan sebelumnya, GDPR berfungsi sebagai model utama bagi undang-undang perlindungan data, dengan ketentuan ketatnya mengenai pemberitahuan pelanggaran dan sanksi bagi kegagalan melaporkan pelanggaran dalam waktu 72 jam setelah ditemukan. Undang-undang tersebut juga menekankan perlunya organisasi menerapkan langkah-langkah keamanan proaktif untuk mencegah terjadinya pelanggaran sejak awal.

Di Indonesia, meskipun Undang-Undang PDP menetapkan kerangka hukum untuk pemberitahuan pelanggaran data, implementasi praktis dari ketentuan-ketentuan ini tetap menjadi area yang perlu diperhatikan. Para peneliti mencatat bahwa meskipun kerangka hukum telah ada, mekanisme penegakan hukum dan kepatuhan bisa lemah, serta terdapat kurangnya kesadaran di kalangan organisasi dan masyarakat umum mengenai pentingnya perlindungan data (Rosadi, 2018; Yuniarti, 2019). Selain itu, digitalisasi ekonomi Indonesia yang pesat telah menimbulkan tantangan dalam memastikan kepatuhan organisasi terhadap undang-undang perlindungan data, terutama di sektor-sektor seperti e-commerce, perbankan, dan telekomunikasi, di mana data pribadi diproses dalam volume besar.

2.4. Analisis Perbandingan dengan Standar Internasional

Untuk menilai efektivitas Pasal 26 Undang-Undang PDP, akan bermanfaat untuk membandingkannya dengan standar internasional seperti GDPR. Ketentuan pemberitahuan pelanggaran dalam GDPR termasuk yang paling ketat di dunia, mewajibkan pengendali data untuk memberitahukan otoritas pengawas yang relevan dalam waktu 72 jam setelah mengetahui adanya pelanggaran. Selain itu, GDPR memberikan hak kepada individu untuk diberi tahu mengenai pelanggaran yang mungkin memengaruhi hak dan kebebasan mereka, serta menyediakan pedoman untuk memitigasi kerugian (Komisi Eropa, 2018). Tingkat transparansi dan akuntabilitas ini sangat penting dalam membangun kepercayaan publik terhadap undang-undang perlindungan data. Sebaliknya, Undang-Undang PDP Indonesia, khususnya Pasal 26, mewajibkan pemberitahuan pelanggaran tetapi kurang memiliki kejelasan prosedural dan kekuatan penegakan hukum yang terlihat pada standar internasional seperti GDPR.

Persyaratan GDPR bagi pengendali data untuk memberitahukan otoritas dalam waktu 72 jam setelah terjadi pelanggaran merupakan contoh kerangka kerja yang kokoh yang meningkatkan transparansi dan akuntabilitas, sehingga membangun kepercayaan publik. Sebaliknya, implementasi Undang-Undang PDP telah dikritik karena tenggat waktu yang tidak jelas dan rincian prosedural yang tidak memadai, yang menimbulkan ketidakpastian bagi organisasi dan individu. Kesenjangan ini menyoroti kebutuhan Indonesia untuk menyempurnakan mekanisme perlindungan datanya agar lebih selaras dengan standar global. Meskipun Pasal 26 mewajibkan pengendali data untuk memberitahukan individu dan otoritas mengenai pelanggaran, kurangnya batas waktu yang jelas dan langkah-langkah penanganan pelanggaran telah menyebabkan penegakan hukum yang tidak konsisten dan kurangnya kesadaran (Karnedi & Alam, 2025; Taufiq & Kenyo, 2025). Tidak adanya peraturan yang terperinci dan otoritas pengawas independen semakin mempersulit penegakan yang efektif (Raib et al., 2025; Simanjuntak, 2024).

2.5. Kesenjangan dalam Penelitian Saat Ini dan Kebutuhan akan Studi Lebih Lanjut

Meskipun telah banyak ditulis mengenai undang-undang perlindungan data pribadi dan pelanggaran data, masih diperlukan penelitian lebih lanjut mengenai ketentuan-ketentuan spesifik dalam Undang-Undang PDP, khususnya yang berkaitan dengan pelanggaran data digital. Sebagian besar literatur yang ada berfokus pada kerangka kerja perlindungan data secara umum, sehingga meninggalkan kesenjangan dalam memahami implikasi praktis Undang-Undang PDP Indonesia jika dibandingkan dengan standar internasional. Selain itu, diperlukan lebih banyak studi empiris mengenai efektivitas prosedur pemberitahuan pelanggaran berdasarkan Undang-Undang PDP, serta tantangan yang dihadapi organisasi dalam mematuhi persyaratan tersebut.

Makalah ini berupaya mengatasi kesenjangan tersebut dengan menyajikan analisis hukum normatif terperinci mengenai Pasal 26 Undang-Undang PDP, dengan fokus pada penerapannya terhadap pelanggaran data digital di Indonesia. Analisis ini juga akan mengeksplorasi area-area potensial yang perlu diperbaiki dalam undang-undang tersebut, terutama dalam hal kejelasan dan penegakan hukum, serta akan memberikan rekomendasi untuk menyelaraskan kerangka hukum Indonesia secara lebih erat dengan praktik terbaik internasional.

3. METODE PENELITIAN

3.1. Desain Penelitian

Desain penelitian untuk studi ini bersifat kualitatif dan normatif, karena bertujuan untuk menafsirkan dan menganalisis ketentuan hukum serta implikasinya terhadap pengelolaan pelanggaran data. Penelitian hukum normatif ditandai dengan mengkaji undang-undang, peraturan, dan doktrin hukum yang ada dalam kerangka hukum tertentu. Dalam hal ini, studi ini berfokus pada teks hukum Undang-Undang PDP Indonesia, khususnya Pasal 26, dan mengevaluasi bagaimana pasal tersebut menangani masalah pelanggaran data digital dalam konteks hukum perlindungan data Indonesia.

Penelitian ini mengikuti metodologi tradisional penelitian hukum doktrinal, yang umum dalam studi hukum di mana peneliti terutama mengkaji aturan hukum, undang-undang, peraturan, dan dokumen hukum otoritatif lainnya. Teks hukum utama yang menjadi fokus dalam penelitian ini adalah Pasal 26 Undang-Undang PDP, yang menguraikan kewajiban pengendali dan pengolah data jika terjadi pelanggaran data. Melalui analisis doktrinal, penelitian ini mengeksplorasi kejelasan, kecukupan, dan penerapan praktis ketentuan ini dalam menangani pelanggaran data digital.

3.2. Pengumpulan Data

Pengumpulan data untuk penelitian ini melibatkan sumber primer dan sekunder. Sumber data primer untuk penelitian ini adalah teks hukum itu sendiri, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Akan dilakukan pemeriksaan menyeluruh terhadap UU PDP, khususnya Pasal 26, yang mengatur pemberitahuan pelanggaran dan prosedur setelah terjadinya pelanggaran data digital. Teks hukum akan dianalisis untuk mengekstrak ketentuan yang relevan, mengidentifikasi kewajiban hukum, dan menilai struktur kerangka hukum seputar perlindungan data. Analisis ini akan menjadi landasan untuk memahami pendekatan hukum Indonesia terhadap perlindungan data pribadi.

Sumber data sekunder akan mencakup komentar hukum, artikel akademis, buku, yurisprudensi, dan laporan dari otoritas regulasi terkait. Sumber-sumber ini akan memberikan konteks bagi analisis hukum, menawarkan interpretasi, dan memungkinkan perbandingan antara kerangka hukum Indonesia dan standar internasional, seperti Peraturan Perlindungan Data Umum (GDPR) Uni Eropa. Selain itu, laporan dari badan pemerintah, seperti Kementerian Komunikasi dan Informatika (Kominfo) Indonesia, serta lembaga perlindungan data akan dirujuk untuk memahami praktik penegakan hukum dan

kepatuhan di Indonesia. Data perbandingan dari undang-undang perlindungan data internasional, khususnya GDPR, akan digunakan untuk mengevaluasi kecukupan Undang-Undang PDP Indonesia dan menyoroti potensi celah dalam mekanisme pemberitahuan pelanggaran yang dimilikinya.

3.3. Pendekatan Analisis Hukum

Analisis hukum untuk penelitian ini mengikuti pendekatan doktrinal, dimulai dengan analisis tekstual Pasal 26 Undang-Undang PDP. Langkah ini akan melibatkan pembacaan dan interpretasi mendalam terhadap ketentuan tersebut, dengan fokus pada kejelasan dan kelengkapannya terkait pemberitahuan pelanggaran data. Aspek-aspek utama yang akan dievaluasi meliputi tenggat waktu pemberitahuan, tanggung jawab pengendali data, serta prosedur untuk memberitahu individu yang terdampak dan otoritas terkait. Analisis ini akan memberikan pemahaman terperinci mengenai struktur kerangka hukum dan efektivitasnya dalam mengelola pelanggaran data.

Selanjutnya, penelitian ini akan mencakup analisis kontekstual, yang menempatkan Undang-Undang PDP dalam lanskap yang lebih luas dari undang-undang perlindungan data pribadi. Hal ini akan melibatkan pertimbangan terhadap lingkungan hukum di Indonesia dan membandingkannya dengan standar internasional, khususnya GDPR. Efektivitas undang-undang dalam menangani ancaman yang muncul, seperti serangan siber dan akses tidak sah terhadap data pribadi, juga akan dikaji. Analisis evaluatif akan menyusul, menilai implikasi praktis Pasal 26 dalam hal perlindungan data pribadi serta mengevaluasi kecukupan sanksi dan mekanisme penegakan hukum. Terakhir, perbandingan dengan kerangka kerja internasional akan menyoroti apakah Undang-Undang PDP Indonesia selaras dengan praktik terbaik global dan di mana perbaikan mungkin diperlukan, terutama dalam prosedur pemberitahuan pelanggaran dan kewajiban hukum bagi pengendali data.

3.4. Ruang Lingkup Penelitian

Ruang lingkup penelitian ini terbatas pada analisis hukum Pasal 26 Undang-Undang PDP. Meskipun Undang-Undang PDP mencakup berbagai isu perlindungan data, studi ini akan berfokus secara khusus pada ketentuan yang berkaitan dengan pelanggaran data, termasuk kewajiban pemberitahuan pengendali dan pemroses data. Studi ini akan terutama berfokus pada kerangka hukum domestik Indonesia, namun juga akan memasukkan analisis hukum komparatif untuk mengevaluasi sejauh mana pendekatan Indonesia selaras atau berbeda dari norma internasional.

Studi ini tidak akan mendalami aspek teknis pelanggaran data, seperti langkah-langkah keamanan siber spesifik yang diperlukan untuk mencegah pelanggaran atau tantangan operasional yang dihadapi organisasi dalam mematuhi undang-undang. Sebaliknya, studi ini berfokus pada kerangka hukum dan efektivitasnya dalam menangani isu-isu hukum dan regulasi yang terkait dengan pelanggaran data.

3.5. Teknik Analitis

Untuk memastikan evaluasi yang menyeluruh dan sistematis, teknik analitis berikut akan digunakan: Analisis Doktrinal Hukum, yang melibatkan pemeriksaan mendalam terhadap teks-teks hukum, termasuk Undang-Undang PDP dan undang-undang perlindungan data internasional yang relevan, dengan fokus pada pemahaman maksud di balik ketentuan-ketentuan tersebut, kerangka pembentukannya, dan keselarasan dengan praktik terbaik global. Analisis Hukum Komparatif akan dilakukan untuk membandingkan ketentuan perlindungan data Indonesia dengan kerangka kerja internasional seperti GDPR, mengidentifikasi kekuatan dan kelemahan dalam kerangka hukum Indonesia serta mengusulkan area potensial untuk reformasi. Studi ini juga akan mencakup Tinjauan Putusan Pengadilan dan Yurisprudensi, menganalisis tindakan penegakan hukum dan putusan hukum di Indonesia yang terkait dengan pelanggaran data, jika tersedia. Terakhir, Evaluasi Kritis terhadap Undang-Undang PDP akan dilakukan

untuk mengidentifikasi celah atau ambiguitas apa pun, dengan rekomendasi untuk amandemen legislatif atau perbaikan dalam penegakan hukum guna menyelaraskan kerangka hukum Indonesia dengan standar internasional dalam mencegah dan mengelola pelanggaran data digital.

4. HASIL DAN PEMBAHASAN

4.1. Gambaran Umum Pasal 26 Undang-Undang PDP

Pasal 26 Undang-Undang PDP menguraikan kerangka hukum untuk menangani pelanggaran data, dengan menekankan tanggung jawab pengendali dan pengolah data dalam memastikan perlindungan data pribadi. Pasal tersebut mewajibkan pengendali data untuk memberitahukan baik individu yang terdampak maupun otoritas terkait ketika terjadi pelanggaran data. Pemberitahuan ini harus mencakup rincian mengenai sifat pelanggaran, jenis data yang terkompromi, dan langkah-langkah yang diambil untuk memitigasi dampak pelanggaran. Namun, meskipun undang-undang mewajibkan pemberitahuan ini, undang-undang tidak secara eksplisit menentukan batas waktu pengirimannya, sehingga berpotensi menimbulkan penundaan dalam respons terhadap pelanggaran dan berdampak pada perlindungan konsumen (Amaro, 2020).

Salah satu ketentuan utama Pasal 26 adalah kewajiban pemberitahuan, yang mewajibkan pengendali data untuk memberitahukan individu yang terdampak dan otoritas terkait secara segera setelah menemukan pelanggaran. Pemberitahuan ini harus mencakup informasi rinci mengenai sifat pelanggaran, jenis data yang terdampak, dan langkah-langkah yang diambil untuk menangani pelanggaran tersebut (Chushairi et al., 2025). Namun, ketidakhadiran batas waktu yang jelas untuk pemberitahuan dapat menyebabkan ketidakpatuhan yang tidak konsisten dan penundaan, seperti yang terlihat dalam kasus nyata seperti insiden PDNs, di mana kegagalan dalam pemberitahuan tepat waktu dan transparansi melemahkan perlindungan hukum bagi korban (Arief & Purwanto, 2025).

Undang-Undang Perlindungan Data Pribadi (PDP) juga menetapkan kewajiban bagi pengendali data untuk melaporkan pelanggaran kepada otoritas regulasi yang berwenang, seperti Kementerian Komunikasi dan Informatika (Kominfo), guna memastikan penyelidikan dan penegakan hukum yang tepat. Namun, ketidakhadiran Otoritas Perlindungan Data Pribadi yang khusus menghambat pengawasan yang efektif, sehingga penegakan hukum dan pertanggungjawaban menjadi sulit (Chushairi et al., 2025; Wijayanto & Indrayanti, 2025). Oleh karena itu, pengawasan yang ditingkatkan dan kesadaran publik yang lebih besar diperlukan untuk memastikan kepatuhan dan melindungi hak-hak konsumen dengan lebih baik (Arief & Purwanto, 2025).

4.2. Efektivitas Pasal 26 dalam Menangani Pelanggaran Data Digital

Efektivitas Pasal 26 Undang-Undang Perlindungan Data Pribadi (UU PDP) Indonesia dapat dievaluasi secara kritis melalui kejelasan, jaminan prosedural, mekanisme penegakan hukum, dan kesesuaiannya dengan standar internasional. Meskipun UU PDP menetapkan kerangka kerja untuk pemberitahuan pelanggaran, undang-undang ini memiliki ambiguitas, terutama tidak adanya batas waktu yang ditentukan untuk pemberitahuan, yang sangat kontras dengan persyaratan 72 jam dalam GDPR. Ketidakjelasan ini dapat menyebabkan penundaan yang mungkin merugikan individu yang terkena dampak. UU PDP menguraikan kewajiban pelaporan pelanggaran data namun kurang memiliki pedoman prosedural yang rinci, sehingga mempersulit kepatuhan bagi pengendali data (Arief & Purwanto, 2025). Perusahaan seringkali gagal memenuhi batas waktu hukum untuk pemberitahuan kepada pengguna, yang menunjukkan kesenjangan antara harapan regulasi dan praktik aktual (Kriswandaru et al., 2024).

Penegakan Pasal 26 terhambat oleh infrastruktur regulasi yang tidak memadai dan kesadaran publik yang terbatas, terutama di sektor seperti e-commerce (Kriswandaru et al.,

2024). Meskipun undang-undang menyebutkan sanksi atas ketidakpatuhan, ketentuan yang samar-samar membuatnya sulit bagi regulator untuk menjatuhkan sanksi yang efektif (Arief & Purwanto, 2025). Kurangnya mekanisme penegakan hukum yang kuat berarti bahwa lembaga pengatur kesulitan memastikan kepatuhan, terutama di industri dengan aliran data yang kompleks seperti e-commerce, keuangan, dan telekomunikasi. Selain itu, undang-undang tidak menentukan cakupan sanksi secara tepat, yang mempersulit proses penegakan hukum dan kemampuan pengendali data untuk menilai konsekuensi potensial dari pelanggaran.

Jika dibandingkan dengan standar internasional, terutama GDPR, Undang-Undang PDP Indonesia menunjukkan kelebihan dan kelemahan. GDPR menyediakan kerangka kerja terperinci untuk pemberitahuan pelanggaran data, termasuk batas waktu pemberitahuan 72 jam, sanksi atas keterlambatan pelaporan, dan pembentukan otoritas perlindungan data untuk mengawasi kepatuhan. Sebaliknya, Undang-Undang PDP Indonesia kurang spesifik dalam hal tenggat waktu dan penegakan hukum, yang dapat melemahkan efektivitasnya secara keseluruhan dalam menangani pelanggaran data. Namun, Undang-Undang PDP sejalan dengan standar internasional dengan mewajibkan pengendali data untuk memberitahukan baik kepada individu yang terkena dampak maupun badan pengatur, yang mencerminkan tren global menuju pemberitahuan pelanggaran yang tepat waktu dan transparan. Meskipun demikian, mekanisme penegakannya perlu diperkuat untuk memastikan kepatuhan dan meningkatkan kemampuannya dalam menangani pelanggaran secara efektif (Arief & Purwanto, 2025; Kriswandaru et al., 2024).

4.3. Tantangan dalam Penerapan Pasal 26

Salah satu tantangan utama dalam menerapkan Pasal 26 Undang-Undang Perlindungan Data Pribadi adalah kurangnya kesadaran dan kapasitas di kalangan pengendali data, terutama di kalangan usaha kecil dan menengah (UKM) di Indonesia. Banyak organisasi mungkin belum sepenuhnya memahami kewajiban mereka berdasarkan undang-undang tersebut atau tidak memiliki sumber daya dan keahlian yang diperlukan untuk mematuhi persyaratan pemberitahuan pelanggaran. Masalah ini sangat terasa di perusahaan-perusahaan kecil yang mungkin tidak memiliki petugas perlindungan data atau tim hukum khusus untuk menangani pelanggaran data secara efektif. Untuk mengatasi tantangan ini, program pelatihan dan kesadaran yang ditargetkan sangatlah penting, terutama di sektor-sektor yang menangani data pribadi dalam volume besar.

Pelaksanaan program kesadaran dan pelatihan harus berfokus pada kebutuhan spesifik UKM, dengan menekankan kewajiban hukum mereka berdasarkan Undang-Undang PDP (Wijayanto & Indrayanti, 2025). Selain itu, panduan dan sumber daya yang disesuaikan dengan sektor-sektor dengan volume data tinggi dapat meningkatkan pemahaman dan memperbaiki kepatuhan (Astuti et al., 2024). Badan regulasi harus memainkan peran kunci dalam memastikan aksesibilitas sumber daya ini serta menyediakan langkah-langkah yang jelas dan dapat ditindaklanjuti bagi organisasi untuk diikuti jika terjadi pelanggaran data.

Masalah lain adalah kurangnya infrastruktur terpusat untuk pelaporan dan pengelolaan pelanggaran data. Meskipun Pasal 26 mewajibkan pengendali data untuk melaporkan pelanggaran kepada otoritas terkait, belum ada mekanisme pelaporan digital yang terintegrasi, yang dapat menyebabkan penundaan dan inefisiensi dalam pengelolaan pelanggaran. Pembentukan platform pelaporan terpusat akan mengurangi penundaan ini, meningkatkan efisiensi, dan memastikan bahwa baik regulator maupun pengendali data dapat merespons pelanggaran dengan lebih efektif (Rinjani & Firmansyah, 2025). Platform digital akan memfasilitasi waktu respons yang lebih cepat dan mengelola dampak pelanggaran data dengan lebih baik (Simanjuntak, 2024).

4.4. Rekomendasi untuk Perbaikan

1. Memperjelas Batas Waktu Pemberitahuan

   Untuk meningkatkan kejelasan dan efektivitas Pasal 26, direkomendasikan agar undang-undang secara eksplisit menetapkan batas waktu yang jelas untuk pemberitahuan pelanggaran data. Persyaratan pemberitahuan dalam waktu 72 jam, serupa dengan GDPR, akan memberikan kerangka kerja yang terstandarisasi untuk kepatuhan dan memastikan bahwa individu serta badan pengatur segera diberi tahu mengenai pelanggaran tersebut.
2. Penguatan Penegakan Hukum dan Sanksi

   Mekanisme penegakan hukum berdasarkan Undang-Undang PDP perlu diperkuat dengan menyediakan ketentuan yang lebih rinci mengenai sanksi atas ketidakpatuhan. Sanksi yang jelas untuk pelaporan terlambat atau kegagalan memberitahukan individu yang terdampak dan otoritas akan menciptakan insentif yang lebih kuat bagi organisasi untuk mematuhi persyaratan undang-undang. Selain itu, peningkatan kapasitas lembaga pengawas untuk memantau dan menegakkan kepatuhan sangat penting bagi efektivitas undang-undang.
3. Meningkatkan Kesadaran dan Pelatihan

   Program kesadaran dan pelatihan yang komprehensif harus diperkenalkan untuk membantu organisasi memahami kewajiban mereka berdasarkan Undang-Undang PDP, terutama terkait pemberitahuan pelanggaran data. Program ini harus menargetkan berbagai pemangku kepentingan, mulai dari korporasi besar hingga UMKM, dan memberikan panduan praktis tentang cara menangani pelanggaran data.
4. Pembentukan Platform Pelaporan Pelanggaran Data Terpusat

   Platform terpusat untuk pelaporan pelanggaran data akan mempermudah proses pemberitahuan dan memastikan bahwa baik individu yang terdampak maupun otoritas terkait segera mendapat informasi. Platform semacam ini dapat memfasilitasi pengumpulan dan analisis data pelanggaran, membantu regulator mengidentifikasi tren, meningkatkan respons, dan mengalokasikan sumber daya secara lebih efektif.

5. KESIMPULAN

Sebagai kesimpulan, Pasal 26 Undang-Undang PDP menandai kemajuan penting dalam perlindungan data pribadi di Indonesia, menanggapi kebutuhan akan transparansi dan akuntabilitas dalam kasus pelanggaran data. Namun, meskipun ketentuan tersebut menetapkan pedoman dasar untuk pemberitahuan pelanggaran, beberapa masalah tetap ada yang menghambat efektivitasnya secara penuh. Ketidakjelasan tenggat waktu pemberitahuan, ketidakhadiran mekanisme penegakan hukum yang rinci, serta potensi kebingungan di kalangan organisasi mengenai tanggung jawab mereka, semuanya berkontribusi pada tantangan dalam implementasi undang-undang ini. Perbandingan dengan standar internasional, khususnya GDPR, menyoroti kebutuhan akan kejelasan lebih lanjut, terutama terkait aspek prosedural pengelolaan pelanggaran. Untuk meningkatkan efektivitas undang-undang ini, studi ini merekomendasikan definisi yang lebih jelas mengenai batas waktu pemberitahuan pelanggaran, penguatan sanksi bagi ketidakpatuhan, serta peningkatan pengawasan regulasi melalui pembentukan platform pelaporan terpusat. Perubahan-perubahan ini tidak hanya akan meningkatkan kepatuhan tetapi juga berkontribusi pada perlindungan privasi individu yang lebih baik di era digital.

DAFTAR PUSTAKA

Amaro, M. C. (2020). La seguridad de los datos personales y la obligación de notificar las brechas de seguridad. *Revista de Derecho, Empresa y Sociedad (REDS)*, *16*, 151–162.

Arief, L. S., & Purwanto, R. (2025). Tinjauan Yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam Menangani Kebocoran Data Pelanggan E-Commerce. *Pemuliaan Keadilan*, *2*(3), 85–102.

Asija, R., & Nallusamy, R. (2014). Data model to enhance the security and privacy of healthcare data. *2014 IEEE Global Humanitarian Technology Conference-South Asia Satellite (GHTC-SAS)*, 237–244.

Astuti, E. F., Hidayanto, A. N., Nurwardani, S., & Salsabila, A. Z. (2024). Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001: 2013. *International Journal of Safety & Security Engineering*, *14*(5).

Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *J. Marshall J. Computer & Info. L.*, *18*, 1.

Chushairi, S. M., Fithry, A., & Rusfandi, R. (2025). Perlindungan Hukum Bagi Korban Atas Kebocoran Pusat Data Nasional Sementara (PDNs) Perspektif Perlindungan Data Pribadi. *Jurnal Jendela Hukum*, *12*(2), 89–122.

Dewi, S. (2015). Privasi atas Data Pribadi: Perlindungan Hukum dan Bentuk Pengaturan di Indonesia. *Jurnal De Jure*, *15*(2), 165.

Karnedi, G., & Alam, R. G. (2025). Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa. *El-Mujtama J. Pengabdi. Masy*, *5*(3), 610–622.

Kriswandaru, A. S., Pratiwi, B., & Suwardi, S. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 740–756.

Lutrianto, I., & Riswaldi, R. (2025). Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia. *Greenation International Journal of Law and Social Sciences*, *3*(2), 345–350.

Natamiharja, R., Sabatira, F., Fakih, M., Davey, O. M., & Anam, H. (2022). Patient Rights During the Covid-19 Pandemic: The Dilemma between Data Privacy and Transparency in Indonesia. *The Age of Human Rights Journal*, *19*, 121–136.

Olayinka, O., & Win, T. (2022). Cybersecurity and Data Privacy in the Digital Age: Two Case Examples. In *Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies* (pp. 117–131). IGI Global.

Raib, M. I. E., Rosadi, S. D., & Cahyadini, A. (2025). Perbandingan penerapan prinsip transparansi antara Indonesia dengan Irlandia dalam hal terjadinya kegagalan pelindungan data pribadi. *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, *3*(2), 51–71.

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83.

Rosadi, S. D. (2018). Protecting privacy on personal data in digital economic era: Legal framework in Indonesia. *Brawijaya Law Journal*, *5*(1), 143–157.

Simanjuntak, P. H. (2024). Perlindungan hukum terhadap data pribadi pada era digital di Indonesia: Studi undang-undang perlindungan data pribadi dan general data protection regulation (gdpr). *Esensi Hukum*, *6*(2), 105–124.

Taufiq, M., & Kenyo, A. S. (2025). The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR. *International Journal of Business, Law, and Education*, *6*(2), 1260–1268.

Utomo, S. (2024). Personal data protection through law number 27 of 2022: challenges of cybercrime in the era of globalization and digital. *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, *23*(2), 2967–2975.

Wijayanto, D. D., & Indrayanti, K. W. (2025). Personal Data Protection in Digital Business Based on the Law on Personal Data Protection. *International Journal of Research in Social Science and Humanities (IJRSS) ISSN: 2582-6220, DOI: 10.47505/IJRSS*, *6*(8), 6–12.

Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. *Business Economic, Communication, and Social Sciences (BECOSS) Journal*, *1*(1), 147–154. https://doi.org/10.21512/becossjournal.v1i1.6030