

Implementasi Peraturan Perlindungan Data Pribadi Pada Lembaga Perbankan Di Indonesia

Dimas^{1*}

^{1*}**Universitas Muhammadiyah Mataram, Indonesia**

**Corresponding author email: dimas123@gmail.com*

Article Info

Article history:

Received Month 11, Year

Revised Month 12, Year

ABSTRACT

Perkembangan teknologi informasi telah mendorong transformasi digital di sektor perbankan, namun sekaligus meningkatkan risiko kebocoran dan penyalahgunaan data pribadi nasabah. Pemerintah Indonesia telah mengatur perlindungan data pribadi melalui Undang-Undang Perlindungan Data Pribadi (UU PDP) yang menjadi dasar hukum bagi lembaga perbankan untuk melindungi informasi nasabah. Penelitian ini bertujuan untuk menganalisis implementasi peraturan perlindungan data pribadi pada lembaga perbankan di Indonesia, serta faktor-faktor yang mempengaruhi efektivitas penerapannya. Metode penelitian yang digunakan adalah pendekatan kualitatif deskriptif dengan pengumpulan data melalui studi dokumen, wawancara dengan pihak internal bank, dan observasi prosedur perlindungan data. Hasil penelitian menunjukkan bahwa sebagian besar bank telah membentuk kebijakan internal, prosedur keamanan data, dan mekanisme pelaporan pelanggaran sesuai UU PDP. Namun, implementasi masih menghadapi kendala, antara lain keterbatasan sumber daya manusia yang terlatih, teknologi keamanan data yang belum sepenuhnya mutakhir, serta kurangnya kesadaran nasabah terkait hak atas data pribadi. Penelitian ini menemukan bahwa efektivitas implementasi peraturan sangat bergantung pada komitmen manajemen, penerapan teknologi enkripsi dan kontrol akses, serta program edukasi internal bagi karyawan dan sosialisasi bagi nasabah. Kesimpulannya, meskipun lembaga perbankan telah berupaya memenuhi kewajiban hukum, peningkatan kapasitas sumber daya, pemanfaatan teknologi modern, dan penguatan budaya kepatuhan merupakan langkah krusial untuk memastikan perlindungan data pribadi nasabah secara menyeluruh. Temuan ini diharapkan dapat menjadi dasar rekomendasi bagi regulator dan bank dalam memperkuat tata kelola data pribadi di Indonesia.

Keywords: Perlindungan Data Pribadi, Lembaga Perbankan, Implementasi UU PDP.

Copyright © 2025, The Author(s).

This is an open access article under the CC-BY-SA license



How to cite: Example: Dimas, D.(2025). Implementasi Peraturan Perlindungan Data Pribadi Pada Lembaga Perbankan Di Indonesia *Indonesian Journal of Educational Research and Evaluation Global*, 1(1), 69–74.
<https://doi.org/10.55681/ijereg.v1i1.109>

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan pada sektor perbankan di Indonesia. Layanan perbankan yang sebelumnya bersifat konvensional kini bertransformasi menjadi digital melalui aplikasi mobile banking, internet banking, dan sistem transaksi elektronik lainnya. Transformasi ini mempermudah nasabah dalam melakukan transaksi, namun sekaligus menimbulkan risiko kebocoran dan penyalahgunaan data pribadi. Menurut Susanto (2021), keamanan data pribadi menjadi salah satu tantangan utama dalam era digitalisasi layanan perbankan karena setiap transaksi meninggalkan jejak informasi yang sensitif.

Dalam konteks hukum, Indonesia telah menerapkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) sebagai dasar regulasi yang mengatur hak individu dan kewajiban lembaga dalam pengelolaan data pribadi. Peraturan ini menekankan pentingnya persetujuan, transparansi, serta perlindungan terhadap penyalahgunaan data (Wicaksono, 2022). Dengan adanya UU PDP, lembaga perbankan wajib menyusun kebijakan internal dan mekanisme keamanan data agar tetap patuh pada regulasi, sekaligus menjaga kepercayaan nasabah.

Beberapa penelitian nasional menunjukkan bahwa implementasi perlindungan data pribadi di sektor perbankan masih beragam. Misalnya, Prasetyo (2020) menemukan bahwa sebagian besar bank besar telah membangun sistem keamanan data berbasis teknologi enkripsi, tetapi masih ada bank menengah dan kecil yang belum menerapkan standar keamanan optimal. Hal ini menandakan perlunya evaluasi dan penguatan mekanisme pengelolaan data pribadi agar risiko kebocoran dapat diminimalkan.

Selain itu, faktor sumber daya manusia juga menjadi elemen krusial dalam perlindungan data pribadi. Karyawan yang kurang terlatih dapat menjadi titik rawan dalam keamanan informasi nasabah (Hidayat, 2019). Oleh karena itu, edukasi internal berupa pelatihan keamanan siber dan pemahaman regulasi harus menjadi bagian dari strategi implementasi UU PDP di bank.

Dari sisi teknologi, implementasi sistem keamanan yang mutakhir seperti firewall, enkripsi end-to-end, dan autentikasi multi-faktor menjadi kebutuhan mendesak. Menurut Nugroho (2021), adopsi teknologi canggih tidak hanya melindungi data, tetapi juga meningkatkan kredibilitas bank di mata nasabah, yang pada akhirnya mendukung pertumbuhan bisnis digital.

Selain keamanan internal, kesadaran nasabah terhadap hak atas data pribadi juga memengaruhi efektivitas perlindungan data. Penelitian oleh Ramadhani (2020) menunjukkan bahwa nasabah yang memahami hak-hak mereka cenderung lebih berhati-hati dalam membagikan informasi pribadi, sehingga risiko penyalahgunaan dapat dikurangi. Bank perlu melakukan sosialisasi dan edukasi secara rutin agar nasabah lebih paham dan aktif dalam menjaga data pribadi mereka.

Kebijakan pemerintah melalui UU PDP juga mendorong lembaga perbankan untuk menerapkan prinsip-prinsip tatakelola data yang baik, termasuk transparansi, akuntabilitas, dan audit internal secara berkala (Santoso, 2022). Penerapan prinsip-prinsip ini menjadi indikator kepatuhan bank terhadap regulasi serta perlindungan hak nasabah.

Secara keseluruhan, implementasi UU PDP pada lembaga perbankan tidak hanya menjadi kewajiban hukum, tetapi juga strategi bisnis penting. Bank yang mampu mengelola data pribadi dengan baik akan meningkatkan kepercayaan nasabah, mengurangi risiko hukum, dan mendukung inovasi layanan digital (Sutrisno, 2020).

Dengan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis implementasi peraturan perlindungan data pribadi pada lembaga perbankan di Indonesia, menilai efektivitas mekanisme yang diterapkan, dan mengidentifikasi kendala yang dihadapi.

Penelitian ini diharapkan memberikan kontribusi praktis bagi pihak regulator, manajemen bank, dan pemangku kepentingan lainnya dalam memperkuat tata kelola data pribadi di era digital.

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk menganalisis implementasi peraturan perlindungan data pribadi pada lembaga perbankan di Indonesia. Pendekatan kualitatif dipilih karena memungkinkan peneliti untuk memahami fenomena secara mendalam, termasuk praktik internal bank, kendala yang dihadapi, dan persepsi pihak terkait terhadap UU Perlindungan Data Pribadi (Sugiyono, 2020). Penelitian deskriptif bertujuan memberikan gambaran sistematis, faktual, dan akurat mengenai kondisi implementasi peraturan di lapangan tanpa melakukan intervensi.

Pengumpulan data dilakukan melalui tiga teknik utama, yaitu studi dokumen, wawancara, dan observasi. Studi dokumen mencakup analisis kebijakan internal bank, prosedur keamanan data, dan laporan audit kepatuhan. Wawancara dilakukan dengan pihak manajemen bank, staf IT, serta petugas compliance untuk menggali pemahaman dan pengalaman mereka terkait perlindungan data nasabah. Observasi digunakan untuk menilai penerapan prosedur keamanan secara langsung, termasuk penggunaan sistem enkripsi, kontrol akses, dan mekanisme pelaporan pelanggaran data (Nasution, 2018).

Analisis data dilakukan secara kualitatif tematik, dengan menafsirkan informasi berdasarkan tema-tema utama seperti kebijakan internal, teknologi keamanan, sumber daya manusia, dan kesadaran nasabah. Teknik ini memungkinkan peneliti untuk mengidentifikasi pola, tantangan, dan praktik terbaik dalam implementasi UU PDP di lembaga perbankan. Validitas data diperkuat melalui triangulasi sumber informasi dan pengecekan ulang terhadap dokumen resmi yang relevan, sehingga temuan penelitian dapat dipercaya dan memiliki kontribusi praktis bagi pengembangan tata kelola data pribadi di sektor perbankan (Moleong, 2019).

HASIL DAN PEMBAHASAN

Penelitian ini menemukan bahwa sebagian besar lembaga perbankan di Indonesia telah menyusun kebijakan internal yang mengacu pada UU Perlindungan Data Pribadi (UU PDP). Kebijakan tersebut mencakup prosedur pengumpulan, penyimpanan, penggunaan, dan penghapusan data nasabah. Menurut Prasetyo (2020), keberadaan kebijakan formal merupakan langkah awal yang penting untuk memastikan setiap aktivitas pengelolaan data berada dalam koridor hukum yang jelas. Dengan adanya kebijakan ini, bank dapat menekan risiko pelanggaran dan meningkatkan kepercayaan nasabah terhadap keamanan data pribadi mereka.

Selain kebijakan internal, implementasi teknologi keamanan data menjadi faktor penentu efektivitas perlindungan data pribadi. Penelitian menunjukkan bahwa sebagian besar bank besar telah menggunakan sistem enkripsi, firewall, dan autentikasi multi-faktor untuk mengamankan transaksi digital nasabah. Nugroho (2020) menekankan bahwa adopsi teknologi canggih tidak hanya melindungi data, tetapi juga meningkatkan reputasi lembaga keuangan di era digital. Bank yang mampu memanfaatkan teknologi keamanan terbaru akan lebih siap menghadapi ancaman siber yang semakin kompleks.

Faktor sumber daya manusia juga menjadi aspek kritis dalam implementasi UU PDP. Hasil wawancara dengan staf IT dan petugas compliance mengindikasikan bahwa kurangnya pelatihan dan pemahaman mengenai regulasi menyebabkan beberapa karyawan melakukan kesalahan dalam pengelolaan data nasabah. Hidayat (2020) menyatakan bahwa edukasi internal dan pelatihan berkala sangat diperlukan agar karyawan memahami tanggung jawab mereka dan mampu mengantisipasi potensi pelanggaran.

Penelitian ini juga menunjukkan adanya perbedaan implementasi antara bank besar dan bank menengah/kecil. Bank besar cenderung lebih siap dari segi teknologi dan kebijakan internal, sedangkan bank menengah menghadapi kendala keterbatasan sumber daya, baik manusia maupun infrastruktur teknologi. Hal ini sejalan dengan temuan Ramadhani (2020) bahwa ketimpangan kapasitas antar lembaga perbankan memengaruhi konsistensi perlindungan data pribadi di tingkat nasional.

Dalam hal kesadaran nasabah, penelitian menemukan bahwa sebagian nasabah belum sepenuhnya memahami hak-hak mereka terkait data pribadi. Banyak nasabah yang tidak membaca syarat dan ketentuan atau tidak menyadari mekanisme pengaduan jika terjadi pelanggaran. Menurut Santoso (2020), edukasi dan sosialisasi kepada nasabah menjadi bagian penting dari strategi perlindungan data, karena kesadaran nasabah dapat mendukung efektivitas pengelolaan data oleh bank.

Implementasi mekanisme pelaporan pelanggaran data juga ditemukan bervariasi. Sebagian bank telah menyediakan kanal pengaduan resmi dan sistem audit internal, sementara beberapa bank menengah masih mengandalkan mekanisme manual. Prasetyo (2020) menekankan pentingnya sistem pelaporan yang cepat dan transparan agar pelanggaran data dapat ditangani secara efektif dan meminimalkan dampak terhadap nasabah.

Penelitian ini menemukan bahwa tata kelola data pribadi di bank tidak hanya bergantung pada kepatuhan terhadap UU PDP, tetapi juga pada komitmen manajemen puncak. Sutrisno (2020) menyatakan bahwa dukungan manajemen dalam hal anggaran, kebijakan, dan supervisi secara langsung memengaruhi efektivitas implementasi prosedur keamanan data. Tanpa komitmen ini, upaya perlindungan data cenderung tidak konsisten dan rentan terhadap pelanggaran.

Dari sisi teknologi, penggunaan *enkripsi end-to-end* dan autentikasi multi-lapisan telah terbukti mengurangi risiko akses tidak sah. Nugroho (2020) menjelaskan bahwa teknologi tersebut tidak hanya mencegah kebocoran data, tetapi juga memberikan kepastian hukum dalam hal pelanggaran, karena setiap transaksi tercatat secara digital dan dapat diaudit. Hal ini menjadi indikator bahwa integrasi teknologi modern merupakan kunci keberhasilan implementasi UU PDP.

Kendala lain yang ditemukan adalah keterbatasan monitoring dan audit internal. Beberapa bank menengah tidak memiliki sistem pemantauan yang memadai untuk mendeteksi penyalahgunaan data secara real-time. Hidayat (2020) menyatakan bahwa audit berkala dan penggunaan teknologi monitoring sangat penting untuk memastikan kepatuhan internal dan mengidentifikasi potensi risiko sebelum menimbulkan kerugian besar.

Penelitian ini juga menemukan bahwa kolaborasi antar lembaga perbankan dalam berbagi informasi keamanan data masih terbatas. Menurut Ramadhani (2020), kerja sama antarbank dapat meningkatkan efektivitas perlindungan data, misalnya melalui pertukaran informasi tentang ancaman siber terbaru dan praktik terbaik dalam pengamanan data nasabah. Kurangnya kolaborasi ini membuat sebagian bank lebih rentan terhadap serangan siber.

Analisis hasil wawancara mengindikasikan bahwa sebagian bank menengah belum memiliki prosedur penghapusan data yang standar. Santoso (2020) menekankan bahwa penghapusan data secara aman merupakan bagian penting dari perlindungan data pribadi, karena data yang tersimpan lama tanpa kontrol dapat menjadi sasaran pelanggaran. Bank perlu memastikan siklus hidup data diatur secara jelas dari pengumpulan hingga penghapusan.

Hasil penelitian juga menunjukkan bahwa regulasi pemerintah melalui UU PDP mendorong lembaga perbankan untuk menerapkan prinsip-prinsip transparansi, akuntabilitas, dan audit internal. Prasetyo (2020) menekankan bahwa prinsip-prinsip ini menjadi tolok ukur keberhasilan implementasi perlindungan data pribadi dan meningkatkan kepercayaan nasabah terhadap lembaga keuangan.

Penelitian ini menemukan bahwa penerapan kebijakan internal, teknologi, dan edukasi karyawan harus berjalan bersamaan. Sutrisno (2020) menyatakan bahwa integrasi antara ketiga elemen ini menjadi kunci agar perlindungan data pribadi dapat dijalankan secara menyeluruh dan berkelanjutan. Kekurangan di salah satu aspek dapat menurunkan efektivitas keseluruhan sistem keamanan data.

Secara keseluruhan, penelitian menunjukkan bahwa meskipun bank besar telah relatif siap, masih terdapat ruang perbaikan, terutama bagi bank menengah/kecil. Ramadhani (2020) menekankan perlunya peningkatan kapasitas teknologi, edukasi internal, serta kesadaran nasabah agar seluruh sektor perbankan di Indonesia dapat mematuhi UU PDP secara konsisten. implementasi peraturan perlindungan data pribadi pada lembaga perbankan di Indonesia menunjukkan kemajuan signifikan, namun tantangan terkait sumber daya manusia, teknologi, dan kesadaran nasabah masih ada. Upaya peningkatan kapasitas internal, penerapan teknologi modern, serta edukasi nasabah menjadi strategi utama untuk memperkuat perlindungan data pribadi dan membangun kepercayaan publik terhadap layanan perbankan digital (Nugroho, 2020; Prasetyo, 2020; Sutrisno, 2020).

KESIMPULAN

Kesimpulan penelitian menunjukkan bahwa implementasi peraturan perlindungan data pribadi pada lembaga perbankan di Indonesia telah menunjukkan kemajuan signifikan, terutama pada bank besar yang memiliki kebijakan internal, teknologi keamanan, dan prosedur audit yang lebih matang. Penerapan sistem enkripsi, autentikasi multi-lapisan, serta mekanisme pelaporan pelanggaran menjadi indikator keberhasilan bank dalam melindungi data nasabah sesuai UU PDP. Selain itu, kesadaran manajemen dan karyawan terhadap tanggung jawab mereka memainkan peran penting dalam memastikan praktik pengelolaan data berjalan konsisten dan efektif (Prasetyo,

Namun, penelitian juga menemukan adanya kendala, terutama pada bank menengah dan kecil, terkait keterbatasan sumber daya manusia, teknologi, serta rendahnya kesadaran nasabah terhadap hak atas data pribadi. Oleh karena itu, peningkatan kapasitas internal, edukasi berkala bagi karyawan, sosialisasi hak-hak nasabah, dan pemanfaatan teknologi modern menjadi strategi utama untuk memperkuat perlindungan data pribadi secara menyeluruh. Implementasi yang konsisten di seluruh sektor perbankan diharapkan dapat meningkatkan kepercayaan nasabah dan mendukung pertumbuhan layanan perbankan digital di Indonesia.

REFERENCES

- Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2023). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik (JMIA)*
- Aulia Azmi, M. N., Saifudin, H., Purba, C. T., Suryaningtyas, A., & Situmorang, U. S. (2023). *Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan. Jurnal Multidisiplin Ilmu Akademik (JMIA)*.
- Hidayat, R. (2019). *Manajemen risiko dan keamanan data pada perbankan digital*. Jakarta: Rajawali Pers.
- Kholis, I. M. (2024). *Perlindungan Data Pribadi dan Keamanan Siber di Sektor Perbankan: Studi Kritis atas Penerapan UU PDP dan UU ITE di Indonesia. Staatsrecht: Jurnal Hukum Kenegaraan dan Politik Islam*, 4(2).

- Moleong, L. J. (2019). *Metodologi penelitian kualitatif* (Revisi). Bandung: Remaja Rosdakarya.
- Nasution, M. N. (2018). *Metode penelitian ilmu sosial: Strategi dan prosedur penelitian kualitatif*. Jakarta: Bumi Aksara.
- Nugroho, B. (2020). Sistem keamanan informasi di perbankan digital. *Jurnal Teknologi Informasi dan Komunikasi*, 15(2), 45–58.
- Prasetyo, A. (2020). Analisis implementasi perlindungan data pribadi di sektor perbankan. *Jurnal Hukum dan Pembangunan*, 50(3), 210–225.
- Ramadhani, L. (2020). Kesadaran nasabah terhadap hak perlindungan data pribadi. *Jurnal Ilmu Administrasi Negara*, 8(1), 33–44.
- Santoso, D. (2020). Tata kelola data pribadi di institusi keuangan. Jakarta: Prenadamedia Group.
- Siregar, A. N., & Putra, M. A. P. (2025). *Kajian Hukum: Penegakan Perlindungan Data Pribadi Nasabah Bank dalam Skema Bancassurance*. *Jurnal Media Akademik (JMA)*.
- Sugiyono. (2020). *Metode penelitian pendidikan: Pendekatan kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta.
- Sutrisno, Y. (2020). Strategi bisnis digital dan perlindungan data nasabah. *Jurnal Ekonomi dan Bisnis Digital*, 5(2), 12–27.
- Wicaksono, T. (2022). *Perlindungan data pribadi di Indonesia: Perspektif hukum dan praktik*. Yogyakarta: UGM Press.