



Analisis Yuridis Perlindungan Terhadap Kebocoran Data Nasabah Dalam Perbankan di Era Digital

Mawatulo Ndruru¹, Immanuel Frans Franata Gulo², Andi Martin Hulu³, Trisha Mahsuri Priyanka⁴, Elvira Fitriyani Pakpahan^{5*}

^{1,2,3,4,5} Fakultas Hukum, Universitas Prima Indonesia, Medan, Indonesia

*Corresponding Author: elvirapakpahan@unprimdn.ac.id

Artikel Histori

Direvisi: 12-08-2025

Diterima: 05-09-2025

Diterbitkan: 16-09-2025

Abstrak: Penelitian ini bertujuan menganalisis efektivitas regulasi dan implementasi perlindungan data nasabah dalam perbankan digital, serta evaluasi penegakan hukum terkait kebocoran data. Metode yang digunakan adalah yuridis normatif dengan pendekatan kualitatif deskriptif analitik, meliputi analisis peraturan seperti Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Data dikumpulkan melalui studi dokumen dan analisis kualitatif untuk mengevaluasi regulasi, mengidentifikasi tantangan, dan merumuskan solusi. Hasil menunjukkan kekurangan dalam implementasi perlindungan data di perbankan digital, dengan kasus seperti kebocoran data di Bank Syariah Indonesia (BSI) menyoroti perlunya pengawasan dan penegakan hukum yang lebih ketat. Rekomendasi mencakup peningkatan kebijakan keamanan data, kolaborasi antara bank, otoritas pengawas, dan nasabah, serta penegakan hukum yang lebih efektif. Penelitian ini diharapkan dapat membantu pemerintah, bank, dan nasabah dalam meningkatkan perlindungan data pribadi serta berkontribusi pada pengembangan model penegakan hukum.

Kata Kunci: Perlindungan Data, Perbankan Digital, Regulasi, Implementasi Keamanan Data, Penegakan Hukum.

Abstract: This study aims to analyze the effectiveness of regulations and the implementation of customer data protection in digital banking, as well as to evaluate law enforcement related to data breaches. The research employs a normative juridical method with a descriptive-analytical qualitative approach, encompassing the analysis of legal frameworks such as Law Number 19 of 2016 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection. Data were collected through document studies and qualitative analysis to assess regulations, identify challenges, and formulate solutions. The results reveal shortcomings in the implementation of data protection in digital banking, with cases such as the data breach at Bank Syariah Indonesia (BSI) highlighting the need for stricter oversight and law enforcement. The study recommends strengthening data security policies, enhancing collaboration between banks, regulatory authorities, and customers, and improving the effectiveness of law enforcement. This research is expected to assist the government, banks, and customers in enhancing personal data protection and contribute to the development of law enforcement models.

Keywords: Data Protection, Digital Banking, Regulation, Data Security Implementation, Law Enforcement.

PENDAHULUAN

Perkembangan teknologi informasi di era digital telah mendorong transformasi besar dalam industri perbankan, dari sistem konvensional menuju layanan digital yang cepat dan efisien seperti mobile banking dan internet banking. Namun, seiring meningkatnya digitalisasi dan pencurian identitas merusak kepercayaan publik terhadap sistem perbankan digital.¹ Selain itu lemahnya implementasi peraturan dan pengawasan terhadap keamanan data menjadi akar permasalahan yang belum tertangani secara optimal. Kondisi ini menciptakan celah yang dapat dimanfaatkan oleh pihak-pihak tidak bertanggung jawab untuk melakukan pelanggaran data atau kejahatan siber lainnya. Dalam konteks perbankan, hal ini menjadi sangat penting mengingat sektor ini mengelola data pribadi dan keuangan nasabah dalam skala besar. Dikarenakan itu bank memiliki tanggung jawab besar untuk meningkatkan sistem keamanan siber yang canggih serta manajemen risiko digital yang terintegrasi.²

Bank memiliki tanggung jawab besar untuk berinvestasi secara berkelanjutan dalam sistem keamanan dan manajemen risiko digital guna menjaga integritas, kerahasiaan, dan ketersediaan data nasabah serta stabilitas sistem keuangan secara keseluruhan. Investasi ini mencakup implementasi teknologi keamanan mutakhir seperti enkripsi data, sistem deteksi intrusi, dan autentikasi multi-faktor, serta pengembangan kapasitas internal melalui pelatihan staf dan pembentukan unit manajemen risiko yang tangguh. Tidak hanya itu, bank juga perlu melakukan evaluasi berkala terhadap sistem keamanan mereka agar mampu merespons ancaman siber yang terus berkembang.³

Penerapan manajemen risiko digital yang berbasis pada Cetak Biru Transformasi Digital Perbankan sangat penting dalam menciptakan sistem perbankan yang tangguh dan mampu menghadapi berbagai bentuk ancaman siber. Cetak biru ini berfungsi sebagai panduan strategis bagi bank untuk menjalankan transformasi digital secara menyeluruh, dengan memastikan bahwa keamanan dan perlindungan data menjadi bagian integral dari setiap proses. Melalui pendekatan ini, bank dapat secara sistematis mengidentifikasi, menilai, dan mengelola risiko yang terkait dengan teknologi digital, seperti serangan siber, kebocoran data, dan gangguan operasional. Manajemen risiko digital yang baik membantu menjaga keberlangsungan layanan perbankan, melindungi kepercayaan nasabah, dan mendorong stabilitas sistem keuangan secara keseluruhan.⁴

Kasus besar seperti peretasan yang dialami Bank Syariah Indonesia (BSI) oleh kelompok ransomware LockBit pada Mei 2023 menjadi bukti nyata lemahnya sistem pertahanan siber di sektor perbankan nasional. Serangan ini menyebabkan lumpuhnya layanan digital BSI selama hampir sepekan penuh, yang berdampak langsung terhadap nasabah dalam hal akses transaksi, layanan mobile banking, hingga sistem pembayaran internal. Insiden ini bukan hanya mengganggu operasional bank, tetapi juga meruntuhkan kepercayaan publik terhadap kemampuan lembaga keuangan dalam melindungi data dan dana

¹ Naswa Salsabila Lubis and Muhammad Irwan Padli Nasution, "Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat," *KOHESI: Jurnal Multidisplin Saintek* 1, no. 12 (2023): 41–50, <https://ejournal.warunayama.org/index.php/kohesi/article/view/1311>.

² Aluf Ra'syiah Rabah and Kharista Dewi Antisha Shakeab, "Problematisasi Regulasi Lembaga Penjamin Simpanan Dalam Program Penjaminan Simpanan Nasabah Bank Digital," *Jurnal Lex Renaissance* 8, no. 1 (2023): 129–46, <https://doi.org/10.20885/jlr.vol8.iss1.art8>.

³ Dian Ediana Rae, "TATA KELOLA KECERDASAN ARTIFISIAL PERBANKAN INDONESIA," Otoritas Jasa Keuangan, 2025, Hal 7, [https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Tata Kelola Kecerdasan Artifisial Perbankan Indonesia.pdf](https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Tata%20Kelola%20Kecerdasan%20Artifisial%20Perbankan%20Indonesia.pdf).

⁴ Yohanes Ngamal and Maximus Ali Perajaka, "PENERAPAN MODEL MANAJEMEN RISIKO TEKNOLOGI DIGITAL DI LEMBAGA PERBANKAN BERKACA PADA CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN INDONESIA," *JURNAL MANAJEMEN RISIKO* 2, no. 2 (2021): 59–74, <https://doi.org/10.33541/mr.v2iiv.4099>.

nasabah.⁵ Kelompok LockBit, yang dikenal sebagai salah satu geng ransomware paling aktif dan berbahaya di dunia, berhasil mengenkripsi sistem internal BSI dan menuntut tebusan dengan batas waktu 72 jam. Mereka juga mengancam akan membocorkan data sensitif yang mereka klaim berhasil dicuri, apabila permintaan tersebut tidak dipenuhi. Ancaman ini menyoroti betapa pentingnya ketahanan siber sebagai bagian dari manajemen risiko digital yang komprehensif.⁶

Serangan terhadap BSI ini mengungkapkan sejumlah kelemahan mendasar dalam sistem pertahanan siber, seperti tidak adanya sistem deteksi dini terhadap aktivitas mencurigakan, lambatnya respons terhadap insiden, serta belum optimalnya mekanisme cadangan sistem dan prosedur pemulihan bencana (disaster recovery). Dampak dari serangan ini tidak hanya terasa pada terganggunya operasional bank, tetapi juga pada menurunnya tingkat kepercayaan publik terhadap keamanan layanan digital perbankan. Kejadian ini menjadi peringatan serius bagi seluruh industri perbankan untuk segera memperkuat postur keamanan digital mereka. Hal ini dapat dilakukan melalui investasi pada infrastruktur teknologi yang lebih andal, penguatan kapasitas sumber daya manusia di bidang keamanan siber, serta penerapan kebijakan keamanan informasi yang sejalan dengan standar dan praktik terbaik internasional.

Namun demikian, lambatnya respons manajemen BSI dan minimnya transparansi informasi kepada publik mencerminkan lemahnya implementasi regulasi dan tata kelola dalam menangani insiden siber. Seperti yang diungkapkan oleh Fitriyani, pengaturan terkait fintech dan keamanan digital di Indonesia masih cenderung bersifat reaktif, belum terbangun secara sistemik dan proaktif.⁷ Hal ini menunjukkan perlunya pembaruan regulasi yang lebih adaptif serta peningkatan peran pengawasan dari otoritas terkait, agar industri perbankan mampu merespons ancaman digital secara cepat, terbuka, dan terkoordinasi. Studi ini, menganalisis aspek yuridis dari perlindungan terhadap kebocoran data nasabah, termasuk efektivitas regulasi, penegakan hukum, serta faktor-faktor penghambat dalam mewujudkan ekosistem perbankan digital yang aman.

Penelitian ini bertujuan untuk mengevaluasi regulasi dan efektivitas implementasi perlindungan data nasabah dalam perbankan digital, menganalisis upaya penegakan hukum terhadap kebocoran data, serta mengidentifikasi hambatan dalam sistem perlindungan data di Indonesia. Secara praktis, hasil kajian ini diharapkan memberikan kontribusi nyata bagi perbaikan kebijakan dan sistem keamanan bank serta peningkatan kesadaran nasabah. Sementara secara teoritis, penelitian ini menambah khazanah keilmuan di bidang hukum siber dan perlindungan data pribadi, serta menjadi dasar pengembangan model penegakan hukum yang lebih adaptif dan responsif terhadap dinamika teknologi informasi di sektor keuangan.

Berdasarkan pendahuluan di atas maka perumusan masalah hukum terdiri dari 3 yaitu:

1. Apakah regulasi dan implementasi perlindungan data nasabah dalam perbankan di era digital saat ini sudah memadai?
2. Bagaimana efektivitas upaya penegakan hukum yang ada dalam menangani kasus kebocoran data nasabah?
3. Apa saja faktor-faktor yang menghambat peningkatan perlindungan data nasabah dalam perbankan digital?

⁵ Yira Dianti, "Serangan Cyber Dan Kebocoran Data Pada Lembaga Keuangan Syariah Pra Dan Pasca Uu No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dan Uu No. 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan," *Fakultas Syariah Dan Hukum UIN Syarif Hidayatullah Jakarta* (2024), [http://repo.iain-tulungagung.ac.id/5510/5/BAB 2.pdf](http://repo.iain-tulungagung.ac.id/5510/5/BAB%20.pdf).

⁶ *Ibid*, hlm 108.

⁷ and Anderson Tanjaya. Pakpahan, Elvira Fitriyani, Kristina Chandra, "'Urgensi Pengaturan Financial Technology Di Indonesia,'" *Jurnal Darma Agung* 28, no. 3 (2020): 444–56.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan sifat deskriptif-analitik, yang bertujuan untuk menggambarkan serta menganalisis regulasi dan implementasi perlindungan data pribadi nasabah dalam sistem perbankan digital. Data kualitatif sendiri merupakan data yang tidak berbentuk angka, melainkan berupa kata-kata, kalimat, atau gambar.⁸ Sifat deskriptif-analitik dalam penelitian ini memungkinkan peneliti tidak hanya mendeskripsikan fenomena yang ada, tetapi juga menganalisisnya secara kritis dan mendalam.⁹

Metode penelitian yang digunakan adalah yuridis normatif, yaitu suatu metode yang berfokus pada analisis terhadap peraturan perundang-undangan serta norma hukum yang berlaku.¹⁰ Dalam penelitian ini, regulasi yang dianalisis meliputi Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Peraturan Otoritas Jasa Keuangan (POJK) terkait perlindungan data nasabah, serta kebijakan internal bank yang berhubungan dengan keamanan data.

Sumber data dalam penelitian ini dibedakan menjadi dua kategori, yaitu data primer dan data sekunder. Data primer merupakan data yang diperoleh secara langsung dari sumber asli dan otoritatif, seperti dokumen peraturan perundang-undangan, putusan pengadilan, atau dokumen resmi lainnya yang secara langsung berkaitan dengan kasus kebocoran data nasabah. Sementara itu, data sekunder diperoleh secara tidak langsung melalui berbagai sumber literatur yang relevan, seperti buku, jurnal ilmiah, artikel akademik, serta laporan media dan berita yang membahas isu-isu terkait.

Teknik pengumpulan data yang digunakan adalah studi dokumen, yang merupakan metode pengumpulan data dengan memanfaatkan bahan tertulis seperti peraturan perundang-undangan, putusan pengadilan, dan literatur ilmiah.¹¹ Studi dokumen ini memungkinkan peneliti untuk memahami perspektif subjek melalui bahan yang dihasilkan langsung oleh individu atau lembaga yang terkait. Selanjutnya, data yang telah terkumpul dianalisis secara kualitatif menggunakan pendekatan analisis isi, yaitu proses pengelompokan dan pengkodean data naratif untuk menemukan pola dan tema utama. Analisis kualitatif melibatkan pengelompokan aspek-aspek individu dan peristiwa beserta karakteristik yang membedakan mereka, sehingga memungkinkan peneliti mendapatkan pemahaman mendalam terhadap fenomena yang dikaji.

HASIL DAN PEMBAHASAN

Regulasi dan Implementasi Perlindungan Data Nasabah dalam Perbankan Digital

Perlindungan data pribadi nasabah dalam perbankan digital menjadi isu yang penting diatur oleh berbagai regulasi di Indonesia, meskipun belum ada undang-undang khusus untuk perbankan digital. Regulasi utama meliputi:

1. Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan yang menjadi pedoman umum pengelolaan data nasabah (UU Perbankan, 1992).

⁸ Sugiyono, *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R&D* (Bandung: Alfabeta, 2013).

⁹ Elvira Fitriani Pakpahan, Tommy Leonard, and Syahrudin Nasution, "JURIDIC ANALYSIS OF INDEPENDENT COMPANY ESTABLISHMENT POST GOVERNMENT REGULATION NUMBER 8 YEAR 2021," *International Journal of Latin Notary* 1, no. 2 (2021): 150–57, <https://doi.org/10.61968/journal.v1i2.29>.

¹⁰ Soerjono Soekanto and Sri Mamudji, "Penelitian Hukum Normatif Suatu Tinjauan Singkat" (Jakarta: Raja Grafindo Persada, 2010), hlm 13.

¹¹ Haris Herdiansyah, *Metodologi Penelitian Kualitatif Untuk Ilmu-Ilmu Sosial* (Jakarta: Salemba Empat, 2010).

2. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE Revisi) yang menegaskan bahwa penggunaan data pribadi melalui media elektronik harus didasarkan pada persetujuan pemilik data (Rizki et al., 2022).
3. Peraturan Otoritas Jasa Keuangan No. 12/POJK.03/2018 yang mengatur layanan perbankan digital, mewajibkan penggunaan teknologi enkripsi dan mekanisme otentikasi ganda untuk keamanan data (Rizal & Imaniyati).
4. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 sebagai pedoman pengelolaan data pribadi dalam sistem elektronik, termasuk layanan perbankan digital (Kominfo, 2016).¹²

Implementasi perlindungan data meliputi kebijakan keamanan internal bank dengan penggunaan teknologi enkripsi dan otentikasi ganda, serta pengawasan ketat oleh OJK yang berperan sebagai regulator. Nasabah juga dijamin memiliki hak atas keamanan data pribadi, transparansi informasi, pengajuan pengaduan, serta penghapusan atau penarikan persetujuan penggunaan data (Berutu et al., 2024).

Namun, perlindungan data pribadi menghadapi tantangan besar berupa ancaman keamanan siber yang terus berkembang. Oleh karena itu, bank harus terus memperbarui sistem keamanan dan berkolaborasi dengan berbagai pihak, termasuk OJK dan nasabah, untuk mengelola risiko ini secara efektif.¹³ Pelanggaran data dapat berakibat pada sanksi hukum dan tuntutan ganti rugi, serta risiko kerugian finansial bagi kreditur, terutama pada transaksi fintech dan P2P lending yang rentan terhadap risiko gagal bayar.¹⁴ Selain itu, legalitas badan hukum juga berperan penting dalam membangun kepercayaan masyarakat terhadap bank sebagai pengelola data pribadi. Masyarakat cenderung lebih yakin untuk menyerahkan data pribadinya kepada institusi yang memiliki status hukum yang jelas serta berada di bawah pengawasan otoritas yang berwenang.

Efektivitas Penegakan Hukum dalam Menangani Kasus Kebocoran Data Nasabah

Dalam era digital saat ini, perlindungan data nasabah menjadi aspek yang harus diprioritaskan oleh setiap lembaga perbankan. Perkembangan teknologi informasi telah membawa perubahan signifikan dalam operasional perbankan, termasuk dalam hal pengumpulan, penyimpanan, dan pemrosesan data pribadi nasabah secara elektronik. Oleh karena itu, kebutuhan akan sistem perlindungan data yang andal menjadi semakin mendesak.¹⁵

Namun, di tengah kompleksitas sistem digital, risiko kebocoran data masih menjadi ancaman serius. Dalam konteks ini, efektivitas penegakan hukum menjadi kunci penting dalam memberikan perlindungan nyata bagi nasabah sekaligus menjaga stabilitas dan kepercayaan publik terhadap sistem perbankan nasional. Penegakan hukum yang tegas terhadap pelaku kebocoran data, baik dari pihak internal maupun eksternal, mencerminkan keseriusan negara dalam menindak segala bentuk pelanggaran privasi.¹⁶

¹² Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," *Jatiswara* 34, no. 3 (2019): 239–49, <https://doi.org/10.29303/jtsw.v34i3.218>.

¹³ Muhazzab Alief Faizal et al., "ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH: IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI," *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam* 5, no. 2 (2023): 87–100, <https://doi.org/10.47435/asy-syarikah.v5i2.2022>.

¹⁴ Tim Publikasi Hukumonline, "Debitur Gagal Bayar, Dapatkah Fintech P2P Lending Bertanggung Jawab?," *Hukum Online*, 2024, <https://www.hukumonline.com/berita/a/debitur-gagal-bayar--dapatkah-fintech-p2p-lending-bertanggung-jawab-lt66f517173f2ec?page=2>.

¹⁵ Anisa kautsar, "Urgensi Keamanan Data Nasabah Perbankan Dan Profesi Terkait Bidang Ini," *future skills by pijar foundation*, 2024, <https://futureskills.id/blog/keamanan-data-nasabah-perbankan/>.

¹⁶ Ibid, Anisa Kautsar

a. Kronologi Kasus Bank Bsi

Salah satu contoh kasus konkret pada kebocoran data adalah kasus bank syariah Indonesia (BSI), pada 8 Mei 2023, layanan mobile banking dan ATM milik Bank Syariah Indonesia (BSI) mengalami gangguan yang berlangsung selama hampir sepekan. Awalnya, pihak BSI menyampaikan bahwa gangguan ini disebabkan oleh pemeliharaan sistem. Namun, pada 14 Mei 2023, terungkap bahwa gangguan tersebut disebabkan oleh serangan ransomware dari kelompok hacker LockBit. Para pelaku menyandera sistem perbankan dan menuntut uang tebusan dalam waktu 72 jam, disertai ancaman untuk membocorkan data nasabah jika permintaan mereka tidak dipenuhi. Meskipun demikian, pihak BSI tidak secara terbuka mengakui serangan ini, dan tetap menyatakan gangguan disebabkan oleh maintenance. Belakangan diketahui bahwa data nasabah, termasuk informasi rekening, identitas pribadi, dan transaksi keuangan, berhasil diretas.

Peristiwa ini menimbulkan kekhawatiran besar, karena BSI tidak memberikan notifikasi resmi kepada nasabah seperti yang diamanatkan dalam Pasal 46 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Hal ini menunjukkan kelalaian BSI sebagai Pengendali Data Pribadi dalam memenuhi kewajiban hukum atas insiden kebocoran data. Pakar keamanan siber Alfons Tanujaya menegaskan bahwa gangguan layanan lebih dari empat jam menandakan kemungkinan besar adanya gangguan serius pada sistem inti, yang diperkuat oleh indikasi serangan siber.

Hingga saat ini, mekanisme pertanggungjawaban BSI masih belum jelas, meskipun sempat disebutkan bahwa bank akan mempertimbangkan ganti rugi bagi nasabah. Namun, lembaga pelaksana UU PDP, yaitu Lembaga Perlindungan Data Pribadi, belum terbentuk, sehingga penegakan hukum belum optimal.¹⁷ Kasus BSI menunjukkan bahwa tanpa sistem keamanan siber yang andal dan penegakan hukum yang tegas, kepercayaan publik terhadap institusi perbankan dapat terkikis. Regulasi seperti UU PDP di Indonesia dan GDPR di Eropa menjadi instrumen penting dalam memberikan kerangka hukum untuk melindungi data pribadi dan menuntut pertanggungjawaban atas pelanggaran.

b. Upaya dan Penegakan Hukum Perlindungan Data Nasabah

Regulasi perlindungan data nasabah bank di Indonesia didasarkan pada Undang-Undang Republik Indonesia Nomor 7 Tahun 1992 tentang Perbankan, yang mengatur kewajiban menjaga kerahasiaan data nasabah sesuai dengan prinsip rahasia bank. Selain ketentuan perundang-undangan, bank juga menetapkan kebijakan internal berupa Manual Produk, Standar Prosedur, dan Petunjuk Teknis guna memastikan bahwa seluruh pegawai memahami serta mematuhi prinsip perlindungan data secara konsisten. Dalam hal terjadi kebocoran data, pelaku termasuk pegawai bank dapat dikenai sanksi berdasarkan Pasal 47 UU Perbankan, sementara tanggung jawab hukum juga dapat dibebankan kepada direksi dan pemegang saham sebagai representasi korporasi.¹⁸

Penanganan atas insiden kebocoran data mengharuskan bank melakukan investigasi internal serta bekerja sama dengan aparat penegak hukum untuk mengungkap penyebab dan menentukan langkah hukum yang sesuai. Bank Indonesia turut berperan dalam menjaga stabilitas sistem keuangan melalui penyediaan mekanisme mediasi perbankan

¹⁷ Agdelia Meiva Azarine, "Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah," LK2FHUI, 2023, <https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/>.

¹⁸ Hakam Ahmad, Sri Anggraini, and Gesang Iswahyudi, "Perlindungan Hukum Terhadap Keamanan Rahasia Bank Dalam Menjaga Kepentingan Nasabah Perbankan," *AL-MANHAIJ: Jurnal Hukum Dan Pranata Sosial Islam* 4, no. 2 (2022): 337–50, <https://doi.org/10.37680/almanhaj.v4i2.1800>.

untuk menyelesaikan sengketa antara bank dan nasabah.¹⁹ Kepatuhan terhadap UU Perbankan, peraturan Otoritas Jasa Keuangan (OJK), serta kebijakan dari Kementerian Komunikasi dan Informatika (Kemenkominfo) menjadi landasan utama dalam menjamin perlindungan data yang efektif.

Penegakan hukum terhadap pelanggaran data pribadi melibatkan sejumlah lembaga, antara lain OJK sebagai pengawas kepatuhan regulasi perlindungan data nasabah, Kemenkominfo yang mengatur pelaksanaan UU ITE dan UU Perlindungan Data Pribadi serta menjatuhkan sanksi administratif, Kepolisian dan Kejaksaan yang menangani aspek pidana melalui investigasi dan proses peradilan, serta Badan Siber dan Sandi Negara (BSSN) yang mengawasi aspek keamanan siber serta memberikan rekomendasi teknis terhadap penanganan insiden kebocoran data.²⁰ Penegakan hukum ini dilakukan melalui investigasi rutin maupun insidental oleh OJK dan Kemenkominfo, serta melalui mekanisme pelaporan dan pengaduan dari nasabah, yang dapat berujung pada sanksi administratif maupun pidana sesuai dengan hasil investigasi.²¹

Penegakan hukum terhadap pelanggaran perlindungan data nasabah, seperti yang terjadi pada kasus kebocoran data Bank Syariah Indonesia (BSI), mencerminkan pentingnya efektivitas regulasi dan koordinasi antar-lembaga dalam menangani insiden keamanan siber di sektor perbankan. Salah satu kekuatan penegakan hukum di Indonesia terletak pada keberadaan landasan hukum yang cukup kuat, seperti Undang-Undang OJK No. 21 Tahun 2011 yang memberikan kewenangan kepada OJK untuk melakukan pengawasan serta tindakan preventif dan represif terhadap praktik yang merugikan nasabah.²² Selain itu, bank digital juga diwajibkan menerapkan perlindungan konsumen secara menyeluruh, termasuk menyediakan mekanisme pengaduan yang dapat diakses 24 jam.

Namun demikian, kasus BSI juga memperlihatkan beberapa kelemahan nyata, di antaranya belum adanya pengaturan yang spesifik mengenai perlindungan nasabah bank digital dalam Undang-Undang Perlindungan Konsumen, sehingga menciptakan celah hukum. Ditambah lagi, rendahnya literasi hukum dan kompleksitas prosedur pengaduan membuat banyak nasabah mengalami kesulitan dalam menuntut haknya, seperti terlihat pada lambatnya informasi resmi yang diberikan BSI kepada publik terkait serangan ransomware. Dalam beberapa kasus, penyelenggara layanan perbankan juga menunjukkan kecenderungan lebih fokus pada kepentingan bisnis ketimbang perlindungan konsumen, yang menyebabkan transparansi terhadap insiden data menjadi terbatas.²³

Padahal, penegakan hukum idealnya tidak hanya sebatas pemberian sanksi, melainkan juga mencakup kompensasi terhadap kerugian nasabah, pemulihan reputasi bank, serta upaya preventif melalui sanksi administratif dan pidana.²⁴ Efektivitas penegakan hukum dalam kasus kebocoran data seperti pada BSI sangat ditentukan oleh

¹⁹ Amelia Kandisa Luh Putu Vera Astri Pujyanti, "PENYELESAIAN SENGKETA PERBANKAN MELALUI MEDIASI PERBANKAN," 2014, 223–31.

²⁰ Silvi Salavi Sauqina, Siti Ainun Zahriya, and Yulia Nur Afifah, "Gudang Jurnal Multidisiplin Ilmu Manajemen Bank Sentral Dan Aplikasinya Di Indonesia" 2 (2024): 632–36.

²¹ Aditia Syapriallah, "Penegakan Hukum Administrasi Lingkungan Melalui Instrumen Pengawasan," *Bina Hukum Lingkungan* 1, no. 1 (2016): 99–113, <https://doi.org/10.24970/jbhl.v1n1.8>.

²² Venia Utami Keliat et al., "ANALISIS UPAYA DAN PERAN PERLINDUNGAN HUKUM TERHADAP KASUS PERETASAN DATA BANK SYARIAH INDONESIA," *Ilmu Hukum Prima (IHP)* 6, no. 2 (2023): 182–90, <https://doi.org/10.34012/jihp.v6i2.4251>.

²³ JUMRAH. S, "PERLINDUNGAN HUKUM KONSUMEN TERHADAP PENGGUNAAN INTERNET BANKING DI BANK SYARIAH INDONESIA (BSI) CABANG PAREPARE," *Pare-Pare* 15, no. 1 (2024): 37–48.

²⁴ Bambang Purwogandi, "Padahal, Penegakan Hukum Idealnya Tidak Hanya Sebatas Pemberian Sanksi, Melainkan Juga Mencakup Kompensasi Terhadap Kerugian Nasabah, Pemulihan Reputasi Bank, Serta Upaya Preventif Melalui Sanksi Administratif Dan Pidana" (2022).

kepatuhan bank terhadap regulasi yang berlaku, serta kemampuan lembaga pengawas dan penegak hukum dalam melakukan investigasi secara menyeluruh. Untuk itu, dibutuhkan peningkatan kesadaran hukum di kalangan nasabah dan pelaku industri, serta sinergi antar lembaga terkait guna memperkuat sistem perlindungan data nasabah di era digital.

Faktor-Faktor yang Menghambat Peningkatan Perlindungan Data Nasabah

Perlindungan data pribadi nasabah yang efektif membutuhkan regulasi yang lebih rinci serta pembentukan lembaga pengawas yang memiliki kewenangan dan independensi yang kuat untuk menangani isu penyalahgunaan data secara serius (Adawiyah et al., 2022). Beberapa faktor utama yang menjadi penghambat peningkatan perlindungan data nasabah dapat diuraikan sebagai berikut:²⁵

1. Ketidakcukupan Regulasi yang Detail Regulasi yang ada saat ini kurang memuat ketentuan yang rinci terkait perlindungan data pribadi nasabah, seperti batas waktu penyimpanan data oleh pelaku usaha yang belum jelas dan spesifik.
2. Lemahnya Sanksi yang Diberlakukan Sanksi yang dikenakan terhadap pelanggaran perlindungan data pribadi cenderung ringan sehingga kurang memberikan efek jera bagi pelaku usaha yang melanggar aturan.
3. Belum terbentuknya badan pengawas yang khusus dan efektif dalam mengawasi penggunaan data pribadi nasabah membuka peluang bagi pelaku usaha untuk melakukan penyalahgunaan data tanpa pengawasan yang memadai.
4. Kesadaran hukum yang rendah baik di kalangan masyarakat maupun pelaku usaha menyebabkan hak-hak konsumen atas perlindungan data pribadi kurang dipahami dan dijalankan, sehingga memudahkan terjadinya pelanggaran.
5. Koordinasi yang tidak optimal antara pemerintah, Bank Indonesia, pelaku usaha, dan aparat penegak hukum menghambat penegakan hukum yang efektif terhadap pelanggaran perlindungan data.
6. Kurangnya upaya edukasi kepada masyarakat mengenai pentingnya perlindungan data pribadi dan hak-hak konsumen membuat masyarakat menjadi lebih rentan terhadap pelanggaran.
7. Perkembangan Teknologi yang Pesat Kemajuan teknologi yang sangat cepat sering kali melampaui kemampuan regulasi dan pengawasan yang ada, sehingga menciptakan celah bagi pelaku usaha untuk menggunakan data nasabah secara tidak etis atau ilegal.

Secara keseluruhan, faktor-faktor penghambat perlindungan data nasabah di Indonesia mencakup kurangnya detail regulasi, lemahnya sanksi, belum efektifnya badan pengawas, rendahnya kesadaran hukum, koordinasi yang kurang, minimnya edukasi publik, serta perkembangan teknologi yang cepat. Untuk mengatasi permasalahan ini, diperlukan revisi regulasi yang lebih spesifik dan komprehensif, penguatan sanksi hukum, peningkatan kapabilitas badan pengawas, peningkatan kesadaran hukum masyarakat dan pelaku usaha, perbaikan koordinasi antar lembaga terkait, serta pelaksanaan kampanye edukasi publik yang intensif. Pemahaman yang mendalam terhadap faktor-faktor ini akan menjadi dasar dalam merumuskan langkah strategis yang efektif guna meningkatkan perlindungan data pribadi nasabah di Indonesia.²⁶

²⁵ Kaisar Akbar Wibowo et al., "Perlunya Undang-Undang Perlindungan Data Pribadi Yang Komprehensif Guna Menyongsong Digitalisasi Yang Kian Masif," *Al-Hakam Islamic Law & Contemporary Issues* 2, no. 1 (2021): 29–39, <https://ejournal2.undip.ac.id/index.php/ilj/article/view/15101>.

²⁶ Zulkarnain Saleh, Weny Almoravid Dunga, and Sri Nanang Meiske Kamba, "Faktor Penghambat Perlindungan Hak Privasi Nasabah Akibat Kebocoran Data Pribadi Pada Aplikasi Pinjaman Online Dalam Perspektif Hukum Perdata," *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 1 (2023): 26–50, <https://doi.org/10.55606/jhps.v3i1.3156>.

KESIMPULAN

Penelitian ini menyoroti urgensi penguatan perlindungan data pribadi nasabah dalam ekosistem perbankan digital Indonesia, yang menghadapi tantangan signifikan akibat maraknya ancaman keamanan siber serta lemahnya implementasi regulasi yang ada. Berdasarkan analisis yuridis terhadap berbagai peraturan, termasuk UU ITE, UU PDP, dan POJK terkait, ditemukan bahwa meskipun kerangka hukum perlindungan data sudah tersedia, penerapannya di tingkat operasional masih belum optimal. Hal ini terlihat dari kasus kebocoran data Bank Syariah Indonesia (BSI) yang mencerminkan lemahnya deteksi dini, respons terhadap insiden, dan transparansi publik, serta belum efektifnya penegakan hukum yang menimbulkan keraguan terhadap komitmen perlindungan hak nasabah.

Temuan utama dari penelitian ini menegaskan bahwa efektivitas perlindungan data sangat bergantung pada tiga aspek utama: kualitas dan kejelasan regulasi, efektivitas lembaga penegak hukum, dan kesiapan institusi perbankan dalam mengimplementasikan sistem keamanan digital yang adaptif. Lemahnya sanksi, belum terbentuknya lembaga pengawas yang independen, serta rendahnya kesadaran hukum masyarakat dan pelaku industri merupakan faktor penghambat signifikan yang harus segera diatasi melalui reformasi regulasi dan peningkatan kapasitas kelembagaan.

Secara teoretis, penelitian ini memberikan kontribusi terhadap pengembangan literatur di bidang hukum siber dan perlindungan data pribadi, khususnya dalam konteks industri keuangan digital. Penelitian ini juga mempertegas perlunya pendekatan integratif yang menggabungkan aspek hukum, teknologi, dan tata kelola dalam membangun sistem perlindungan data yang berkelanjutan.

Secara praktis, temuan ini mendorong bank untuk tidak hanya mematuhi regulasi, tetapi juga secara proaktif membangun budaya keamanan siber dan memperkuat koordinasi dengan otoritas terkait. Bagi pembuat kebijakan, penelitian ini menggarisbawahi pentingnya pembentukan lembaga pengawas independen, penyusunan regulasi yang lebih detail dan adaptif, serta penguatan mekanisme sanksi dan kompensasi bagi korban kebocoran data.

DAFTAR PUSTAKA

- Ahmad, Hakam, Sri Anggraini, and Gesang Iswahyudi. "Perlindungan Hukum Terhadap Keamanan Rahasia Bank Dalam Menjaga Kepentingan Nasabah Perbankan." *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 4, no. 2 (2022): 337–50. <https://doi.org/10.37680/almanhaj.v4i2.1800>.
- anisa kautsar. "Urgensi Keamanan Data Nasabah Perbankan Dan Profesi Terkait Bidang Ini." future skills by pijar foundation, 2024. <https://futureskills.id/blog/keamanan-data-nasabah-perbankan/>.
- Azarine, Agdelia Meiva. "Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah." *LK2FHUI*, 2023. <https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/>.
- Dian Ediana Rae. "TATA KELOLA KECERDASAN ARTIFISIAL PERBANKAN INDONESIA." Otoritas Jasa Keuangan, 2025. [https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Tata Kelola Kecerdasan Artifisial Perbankan Indonesia.pdf](https://www.ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/Perbankan/Documents/Tata%20Kelola%20Kecerdasan%20Artifisial%20Perbankan%20Indonesia.pdf).
- Dianti, Yira. "Serangan Cyber Dan Kebocoran Data Pada Lembaga Keuangan Syariah Pra Dan Pasca Uu No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi Dan Uu No. 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan." *Fakultas Syariah Dan Hukum UIN Syarif Hidayatullah Jakarta*, 2024. [http://repo.iain-tulungagung.ac.id/5510/5/BAB 2.pdf](http://repo.iain-tulungagung.ac.id/5510/5/BAB%202.pdf).
- Faizal, Muhazzab Alief, Zelyn Faizatul, Binti Nur Asiyah, and Rokhmat Subagyo. "ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH:

- IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI.” *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam* 5, no. 2 (2023): 87–100. <https://doi.org/10.47435/asy-syarikah.v5i2.2022>.
- Herdiansyah, Haris. *Metodologi Penelitian Kualitatif Untuk Ilmu-Ilmu Sosial*. Jakarta: Salemba Empat, 2010.
- JUMRAH. S. “PERLINDUNGAN HUKUM KONSUMEN TERHADAP PENGGUNAAN INTERNET BANKING DI BANK SYARIAH INDONESIA (BSI) CABANG PAREPARE.” *Pare-Pare* 15, no. 1 (2024): 37–48.
- Keliat, Venia Utami, Andini Pratiwi Siregar, Suhaila Zulkifli, and Iin Purba. “ANALISIS UPAYA DAN PERAN PERLINDUNGAN HUKUM TERHADAP KASUS PERETASAN DATA BANK SYARIAH INDONESIA.” *Ilmu Hukum Prima (IHP)* 6, no. 2 (2023): 182–90. <https://doi.org/10.34012/jihp.v6i2.4251>.
- Lubis, Naswa Salsabila, and Muhammad Irwan Padli Nasution. “Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat.” *KOHESI: Jurnal Multidisplin Saintek* 1, no. 12 (2023): 41–50. <https://ejournal.warunayama.org/index.php/koehesi/article/view/1311>.
- Luh Putu Vera Astri Pujiyanti, Amelia Kandisa. “PENYELESAIAN SENGKETA PERBANKAN MELALUI MEDIASI PERBANKAN,” 2014, 223–31.
- Ngamal, Yohanes, and Maximus Ali Perajaka. “PENERAPAN MODEL MANAJEMEN RISIKO TEKNOLOGI DIGITAL DI LEMBAGA PERBANKAN BERKACA PADA CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN INDONESIA.” *JURNAL MANAJEMEN RISIKO* 2, no. 2 (2021): 59–74. <https://doi.org/10.33541/mr.v2iiv.4099>.
- Pakpahan, Elvira Fitriyani, Kristina Chandra, and Anderson Tanjaya. “Urgensi Pengaturan Financial Technology Di Indonesia.” *Jurnal Darma Agung* 28, no. 3 (2020): 444–56.
- Pakpahan, Elvira Fitriani, Tommy Leonard, and Syahrudin Nasution. “JURIDIC ANALYSIS OF INDEPENDENT COMPANY ESTABLISHMENT POST GOVERNMENT REGULATION NUMBER 8 YEAR 2021.” *International Journal of Latin Notary* 1, no. 2 (2021): 150–57. <https://doi.org/10.61968/journal.v1i2.29>.
- Priscyllia, Fanny. “Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum.” *Jatiswara* 34, no. 3 (2019): 239–49. <https://doi.org/10.29303/jtsw.v34i3.218>.
- Purwogandi, Bambang. “Padahal, Penegakan Hukum Idealnya Tidak Hanya Sebatas Pemberian Sanksi, Melainkan Juga Mencakup Kompensasi Terhadap Kerugian Nasabah, Pemulihan Reputasi Bank, Serta Upaya Preventif Melalui Sanksi Administratif Dan Pidana,” 2022.
- Ra’syiah Rabah, Aluf, and Kharista Dewi Antisha Shakeab. “Problematika Regulasi Lembaga Penjamin Simpanan Dalam Program Penjaminan Simpanan Nasabah Bank Digital.” *Jurnal Lex Renaissance* 8, no. 1 (2023): 129–46. <https://doi.org/10.20885/jlr.vol8.iss1.art8>.
- Sauqina, Silvi Salavi, Siti Ainun Zahriya, and Yulia Nur Afifah. “Gudang Jurnal Multidisiplin Ilmu Manajemen Bank Sentral Dan Aplikasinya Di Indonesia” 2 (2024): 632–36.
- Soekanto, Soerjono, and Sri Mamudji. “Penelitian Hukum Normatif Suatu Tinjauan Singkat,” hlm 13. Jakarta: Raja Grafindo Persada, 2010.
- Sugiyono. *Metode Penelitian Pendidikan Pendekatan Kuantitatif, Kualitatif Dan R&D*. Bandung: Alfabeta, 2013.
- Aditia Syapriillah. “Penegakan Hukum Administrasi Lingkungan Melalui Instrumen Pengawasan.” *Bina Hukum Lingkungan* 1, no. 1 (2016): 99–113. <https://doi.org/10.24970/jbhl.v1n1.8>.
- Tim Publikasi Hukumonline. “Debitur Gagal Bayar, Dapatkah Fintech P2P Lending Bertanggung Jawab?” Hukum Online, 2024. <https://www.hukumonline.com/berita/a/de>

bitur-gagal-bayar--dapatkah-fintech-p2p-lending-bertanggung-jawab-
lt66f517173f2ec?page=2.

- Wibowo, Kaisar Akbar, Akrimna Binuril Fahmi, Brenda Aurora Taradwipa, and Entori Mardiansyah. "Perlunya Undang-Undang Perlindungan Data Pribadi Yang Komprehensif Guna Menyongsong Digitalisasi Yang Kian Masif." *Al-Hakam Islamic Law & Contemporary Issues* 2, no. 1 (2021): 29–39. <https://ejournal2.undip.ac.id/index.php/ilj/article/view/15101>.
- Zulkarnain Saleh, Weny Almoravid Dungga, and Sri Nanang Meiske Kamba. "Faktor Penghambat Perlindungan Hak Privasi Nasabah Akibat Kebocoran Data Pribadi Pada Aplikasi Pinjaman Online Dalam Perspektif Hukum Perdata." *Jurnal Hukum, Politik Dan Ilmu Sosial* 3, no. 1 (2023): 26–50. <https://doi.org/10.55606/jhps.v3i1.3156>.