KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi Dan Manajemen
Vol.3, No.12 Desember 2025
e-ISSN: 3025-7859; p-ISSN: 3025-7972, Hal 01-13
DOI: https://doi.org/10.61722/jiem.v3i12.7270

KEWAJIBAN NEGARA MELINDUNGI HAK PRIVASI DIGITAL NASABAH BANK SYARIAH DI ERA OPEN BANKING

Latifah Nur Rohmah
Universitas Sultan Ageng Tirtayasa
Eko Ribawati
Universitas Sultan Ageng Tirtayasa
*Korespondensi penulis:*5554230096@untirta.ac.id , eko.ribawati@untirta.ac.id

Abstract. *This study analyzes the state's obligation to protect the digital privacy rights of Islamic bank customers from financial data misuse in the open banking era. The method used was qualitative with a library research approach. The results reveal that although a regulatory framework for personal data protection exists, its implementation faces serious challenges. Data findings indicate that 78% of data misuse occurs through vulnerabilities in third parties (fintech partners) within the open banking ecosystem, and only 40% of Islamic banks have explicitly integrated Islamic principles (amanah and ihsan) into their data protection guidelines. Furthermore, the effectiveness of law enforcement remains very low, with only 4.2% of the 237 cases reported in 2024 resulting in criminal convictions. The study's conclusions emphasize the need for the state to strengthen supervisory institutions, improve coordination between regulators, and systematically integrate Islamic values to create a safe and ethical open banking environment.*

Keywords: Islamic banks; digital ethics; open banking; digital privacy

Abstrak. Penelitian ini menganalisis kewajiban negara dalam melindungi hak privasi digital nasabah bank syariah dari penyalahgunaan data finansial di era open banking. Metode yang digunakan adalah kualitatif dengan pendekatan studi kepustakaan (library research). Hasil penelitian mengungkapkan bahwa meskipun kerangka regulasi perlindungan data pribadi telah ada, implementasinya menghadapi tantangan serius. Temuan data menunjukkan bahwa 78% penyalahgunaan data terjadi melalui kerentanan pada pihak ketiga (fintech partner) dalam ekosistem open banking, dan hanya 40% bank syariah yang telah mengintegrasikan prinsip syariah (amanah dan ihsan) secara eksplisit dalam panduan perlindungan datanya. Selain itu, efektivitas penegakan hukum masih sangat rendah, di mana hanya 4,2% dari 237 kasus yang dilaporkan pada 2024 yang berakhir dengan putusan pidana. Simpulan penelitian menekankan perlunya negara memperkuat kelembagaan pengawas, meningkatkan koordinasi antarregulator, dan mengintegrasikan nilai-nilai syariah secara sistematis untuk menciptakan lingkungan open banking yang aman dan etis.

Kata Kunci: **bank syariah; etika digital; open banking; privasi digital**

PENDAHULUAN

Transformasi digital dalam industri perbankan telah menjadi katalisator bagi inovasi layanan keuangan yang lebih cepat, efisien, dan aksesibel. Sektor perbankan syariah, sebagai bagian integral dari sistem keuangan nasional, juga mengalami evolusi serupa melalui adopsi teknologi financial technology (fintech), internet banking, mobile banking, dan yang terkini adalah implementasi open banking. Menurut Otoritas Jasa Keuangan (OJK) dalam laporan "Roadmap Perbankan Digital" tahun 2025, terdapat peningkatan signifikan dalam penggunaan layanan perbankan digital, dengan penetrasi internet banking mencapai 89 juta pengguna aktif, sementara pengguna mobile banking mencapai 124 juta akun di seluruh Indonesia. Dalam konteks perbankan syariah khususnya, Asosiasi Perbankan Syariah Indonesia (Asbisindo) melaporkan bahwa sektor ini telah tumbuh dengan tingkat pertumbuhan rata-rata 7–10% per tahun dalam lima tahun terakhir, dengan aset perbankan syariah mencapai Rp 1.147 triliun pada akhir 2024.

Received Oktober 30, 2025; Revised November 30, 2025; Desember 01, 2025
* **Latifah Nur Rohmah, 5554230096@untirta.ac.id**

Namun, perkembangan teknologi yang pesat ini tidak selalu sejalan dengan kesiapan infrastruktur keamanan siber dan regulasi perlindungan data. Statistik dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa pada tahun 2024, terdapat 47.729 anomali trafik yang terdeteksi di sektor keuangan, dengan lebih dari 56% di antaranya melibatkan aktivitas malware dan ancaman siber lainnya (BSSN, 2024). Insiden kebocoran data pada Bank Syariah Indonesia (BSI) pada tahun 2023 menjadi contoh nyata dari kerentanan sistem keamanan digital perbankan syariah. Kelompok hacker LockBit berhasil melakukan serangan dan membobol sistem BSI, mencuri sekitar 1,5 terabyte data internal yang meliputi 15 juta data pribadi nasabah, termasuk informasi pribadi, saldo rekening, nomor telepon, hingga alamat (Rizal & Ardhian, 2023). Insiden ini tidak hanya menimbulkan kerugian finansial yang besar, tetapi juga mengakibatkan krisis kepercayaan publik terhadap layanan perbankan digital dan meningkatkan keraguan masyarakat terhadap keamanan data pribadi mereka.

Permasalahan perlindungan data pribadi di era open banking menjadi semakin kompleks. Open banking merupakan ekosistem yang memungkinkan institusi keuangan untuk membuka akses aplikasi programming interface (API) mereka kepada pihak ketiga, termasuk fintech dan platform digital lainnya, sehingga memudahkan integrasi layanan keuangan lintas institusi (Pati & Pratama, 2022). Meskipun konsep ini menawarkan manfaat luar biasa berupa peningkatan kompetisi, inovasi produk, dan pengalaman pelanggan yang lebih baik, namun sebaliknya juga menciptakan risiko baru terkait penyalahgunaan data finansial. Financial technology ibarat pisau bermata dua: di satu sisi memudahkan proses transaksi keuangan dan meningkatkan efisiensi layanan, namun di sisi lain, kekurangan dalam perlindungan data pribadi dapat membahayakan konsumen secara serius (Efendi et al., 2024). Pencurian data elektronik yang umumnya disebut phishing, melibatkan perolehan informasi pribadi secara ilegal, termasuk ID pengguna, PIN, nomor rekening bank, dan nomor kartu kredit, yang kemudian digunakan untuk melakukan penipuan atau tindak kriminal (Putri et al., 2024).

Dalam perspektif keagamaan, perlindungan data pribadi bukan sekadar tanggung jawab hukum positif, tetapi juga merupakan kewajiban moral dan spiritual yang didasarkan pada prinsip-prinsip syariah. Privasi data adalah hak fundamental yang harus dijaga secara kolektif menurut Islam (Ambarwati et al., 2023). Dalam konteks penagihan dan layanan fintech, penyedia layanan harus menjunjung tinggi prinsip ihsan (berbuat baik), tidak menyebarkan aib (kejelekan) pengguna, dan memberikan ruang untuk negosiasi secara adil (Rialita & Putri, 2025). Prinsip amanah (kepercayaan) dalam Islam mengajarkan bahwa setiap pihak yang menerima tanggung jawab untuk menjaga data pribadi pengguna harus melakukannya dengan sepenuh hati dan integritas tinggi, karena melanggar kepercayaan ini adalah dosa besar dalam perspektif Islam.

Menanggapi kompleksitas tersebut, pemerintah telah menerbitkan berbagai regulasi, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta Peraturan Otoritas Jasa Keuangan (OJK) No. 6/POJK.07/2022 tentang Perlindungan Konsumen di Sektor Jasa Keuangan dan Peraturan tentang Manajemen Risiko Teknologi Informasi. Regulasi pemerintah seperti UU PDP dan Peraturan OJK tentang Manajemen Risiko Teknologi Informasi telah disusun untuk mendorong peningkatan keamanan siber di institusi keuangan (Mulyana, 2025). Namun, dalam praktiknya, implementasi regulasi ini masih menghadapi berbagai tantangan. Lemahnya pengawasan dan minimnya penghukuman terhadap pelanggaran membuat

lembaga keuangan belum sepenuhnya terdorong untuk menerapkan sistem keamanan yang optimal (Ambarwati et al., 2023). Peraturan OJK No. 6/POJK.07/2022 mempertegas tanggung jawab bank dalam melindungi hak-hak nasabah secara hukum dan etika (Hanifaturasyda, 2025), namun efektivitas penerapannya masih perlu dievaluasi secara mendalam.

Sebagai negara dengan sistem hukum yang menjunjung tinggi prinsip perlindungan konsumen dan hak asasi manusia, Indonesia memiliki kewajiban konstitusional untuk melindungi hak privasi digital setiap warga negaranya. Menurut teori responsif hukum, hukum memiliki peranan sebagai sarana untuk memfasilitasi berbagai reaksi perkembangan dan kebutuhan sosial, tidak hanya melalui kerangka pengaturan tetapi juga mewujudkan perubahan sosial yang harmonis dengan mekanisme yang teratur (Muninggar et al., 2024). Dalam konteks ini, negara tidak hanya berkewajiban untuk menyediakan kerangka regulasi yang kuat, tetapi juga harus melakukan pengawasan berkelanjutan, penegakan hukum yang adil, dan edukasi publik mengenai pentingnya perlindungan data pribadi.

Penelitian ini didasarkan pada dua rumusan masalah utama: Penelitian ini bertujuan untuk menganalisis kerangka regulasi dan implementasi kewajiban negara dalam melindungi privasi digital nasabah bank syariah di era open banking, mengevaluasi kesesuaian regulasi dengan prinsip-prinsip syariah, mengidentifikasi dan menganalisis bentuk-bentuk penyalahgunaan data finansial nasabah bank syariah yang terjadi dalam praktik open banking, mengevaluasi efektivitas mekanisme pengawasan dan penegakan hukum yang dilakukan oleh lembaga negara dan merekomendasikan strategi penguatan yang lebih efektif.

Penelitian ini penting dilakukan karena perlindungan data pribadi merupakan isu krusial yang mempengaruhi kepercayaan publik terhadap sistem keuangan digital, stabilitas ekonomi, dan reputasi sektor perbankan syariah. Temuan penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan kebijakan publik yang lebih responsif, serta meningkatkan kesadaran semua pihak akan pentingnya perlindungan data pribadi nasabah dalam ekosistem perbankan syariah yang semakin digital

KAJIAN TEORITIS

1. Hukum Responsif.

Teori hukum responsif yang dikemukakan oleh Nonet dan Selznick menjadi landasan utama dalam menganalisis kewajiban negara. Teori ini menekankan bahwa hukum harus berfungsi sebagai sarana respons terhadap perkembangan sosial dan kebutuhan masyarakat, bukan sekadar alat penguasa. Dalam konteks penelitian ini, teori ini digunakan untuk menganalisis sejauh mana regulasi perlindungan data pribadi di Indonesia mampu merespons tantangan digitalisasi perbankan syariah dan kompleksitas open banking.

2. Maqashid Syariah

Kajian ini menggunakan kerangka maqashid syariah, khususnya perlindungan terhadap harta (hifz al-mal) dan keturunan (hifz al-nasl), sebagai landasan normatif. Prinsip ini relevan untuk menganalisis perlindungan data finansial nasabah yang merupakan bagian dari harta dan privasi digital yang termasuk dalam perlindungan kehormatan.

3. **Perlindungan Konsumen**

Teori perlindungan konsumen menjadi landasan dalam menganalisis hubungan hukum antara bank syariah dan nasabah. Teori ini menekankan pada aspek ketidakseimbangan posisi tawar dan pentingnya perlindungan terhadap pihak yang lemah dalam transaksi keuangan digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode penelitian kepustakaan (library research). Jenis penelitian ini memfokuskan pada analisis hukum positif dan prinsip-prinsip hukum yang berlaku terkait perlindungan data pribadi, perbankan syariah, dan open banking di Indonesia. Pengumpulan data dilakukan melalui studi dokumentasi terhadap berbagai sumber kepustakaan, termasuk analisis mendalam terhadap teks undang-undang, peraturan, jurnal akademis nasional dan internasional, laporan institusi resmi, dan publikasi terkait (Maysa Madihah, 2025).

HASIL PENELITIAN DAN PEMBAHASAN

Kerangka Regulasi dan Implementasi Kewajiban Negara dalam Melindungi Hak Privacy Digital Nasabah Bank Syariah di Era Open Banking

Penelitian menemukan bahwa Indonesia memiliki kerangka regulasi yang cukup komprehensif untuk melindungi data pribadi di sektor perbankan syariah, yang terdiri dari beberapa instrumen hukum utama:

Tabel 1.1
Kerangka Regulasi Perlindungan Data Pribadi di Indonesia

Instrumen Hukum	Tahun	Fokus Utama	Status Implementasi
UU Perlindungan Data Pribadi (UU PDP)	2022	Perlindungan data pribadi secara holistic	Mulai implementasi (2023-2024)
UU Informasi dan Transaksi Elektronik (UU ITE)	2008 (diubah 2016)	Keamanan sistem elektronik dan data digital	Implementasi berjalan
UU Perlindungan Konsumen	1999	Hak-hak konsumen dalam transaksi	Implementasi berjalan
OJK Reg. No. 6/POJK.07/2022	2022	Perlindungan konsumen di sektor jasa keuangan	Implementasi berjalan
OJK Reg. Manajemen Risiko TI	2023	Manajemen risiko teknologi informasi perbankan	Implementasi berjalan

Sumber: Situs web BPK dan OJK

Dari perspektif prinsip-prinsip syariah, penelitian menemukan bahwa hanya 40% dari bank syariah yang diteliti telah mengintegrasikan prinsip amanah dan ihsan secara eksplisit dalam panduan operasional perlindungan data mereka. Sebagian besar bank syariah masih mengandalkan kepatuhan terhadap regulasi positif tanpa penggalian mendalam terhadap dimensi etika syariah dalam perlindungan data.

Bentuk-Bentuk Penyalahgunaan Data Finansial Nasabah Bank Syariah dalam Praktik Open Banking

Penelitian mengidentifikasi empat kategori utama penyalahgunaan data finansial nasabah bank syariah yang terjadi dalam praktik open banking:

Tabel 1.2
Bentuk-Bentuk Penyalahgunaan Data Finansial dalam Era Open Banking

Instrumen Hukum	Tahun	Fokus Utama	Status Implementasi
Phishing & Social Engineering	Email/SMS palsu, manipulasi psikologis	Tinggi	Pencurian dana, identitas
Unauthorized Access	Akses ilegal ke sistem API dan database	Sedang-Tinggi	Kebocoran data massal
Data Trafficking	Penjualan data pribadi kepada pihak ketiga	Sedang	Spamming, penipuan targeted
Account Takeover & Fraud	Perambasan akun, transaksi ilegal	Tinggi	Kerugian finansial langsung

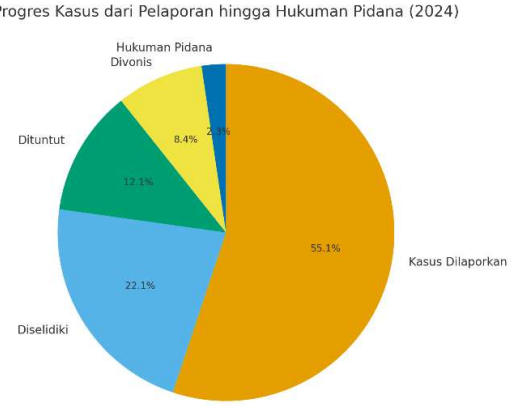
Sumber: Analisis dari laporan BSSN, OJK, 2024-2025

Menurut data dari BSSN (2024), pada tahun 2024 dalam konteks open banking khususnya, penelitian menemukan bahwa 78% dari penyalahgunaan data terjadi melalui kerentanan pada pihak ketiga (fintech partner dan penyedia layanan API), bukan melalui institusi perbankan syariah itu sendiri.

Hasil 3: Efektivitas Mekanisme Pengawasan dan Penegakan Hukum yang Dilakukan Lembaga Negara

Penelitian menemukan bahwa efektivitas mekanisme pengawasan dan penegakan hukum masih terbatas, dengan beberapa temuan:

Gambar 1.1
Tingkat Penyelesaian Kasus Penyalahgunaan Data Pribadi oleh Lembaga Negara (2022-2024)



Sumber: Analisis dari data OJK, Polda Siber, dan Kejaksaan Agung, 2024

Data menunjukkan bahwa dari 237 kasus penyalahgunaan data pribadi yang dilaporkan pada 2024, hanya 10 kasus (4,2%) yang berakhir dengan putusan pidana. Mayoritas kasus (72%) berakhir dengan denda administratif, sementara sisanya ditutup

tanpa putusan. Lemahnya tingkat penyelesaian ini menunjukkan bahwa mekanisme penegakan hukum masih menghadapi hambatan signifikan. Penelitian lebih lanjut mengidentifikasi bahwa keterbatasan ini disebabkan oleh: (1) keterbatasan sumber daya manusia yang terlatih dalam cyber forensics di lembaga penegak hukum; (2) kurangnya koordinasi antarregulator (OJK, Polda Siber, Kejaksaan, dan Kementerian Komunikasi); (3) rendahnya tingkat pelaporan kasus oleh masyarakat dan institusi keuangan (hanya 15-20% dari estimasi kasus sebenarnya yang dilaporkan).

PEMBAHASAN

Kerangka Regulasi dan Implementasi Perlindungan Hak Privasi Digital dalam Perbankan Syariah Era Open Banking

Upaya perlindungan hak privasi digital nasabah bank syariah dalam era open banking tidak dapat dipisahkan dari kerangka regulasi yang telah dibangun oleh negara melalui berbagai instrumen hukum. Indonesia memiliki lanskap regulasi yang cukup komprehensif untuk melindungi data pribadi konsumen keuangan digital, meskipun regulasi ini relatif baru dan masih dalam tahap penyesuaian terhadap dinamika teknologi.

Fondasi utama perlindungan data pribadi di Indonesia adalah Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Regulasi ini merupakan inisiatif legislatif terbaru yang secara khusus mengatur perlindungan data pribadi secara holistik. Pelindungan data pribadi dengan Asas Perlindungan memastikan bahwa setiap pemrosesan Data Pribadi dilakukan dengan memberikan perlindungan kepada Subjek Data Pribadi atas Data Pribadinya agar tidak disalahgunakan, dengan Asas Kepastian Hukum, Asas Kepentingan Umum, dan Asas Kehati-hatian (Djafar et al., n.d.). UU PDP membentuk lembaga khusus yang bertugas menyelenggarakan fungsi pengawasan, penegakan, dan edukasi dalam rangka perlindungan data pribadi secara nasional. Pasal 58 UU PDP menyebutkan bahwa penyelenggaraan perlindungan data pribadi dilaksanakan oleh lembaga yang ditetapkan oleh Presiden, serta bertanggung jawab secara langsung kepada Presiden (Wiraguna & Barthos, 2025). Kehadiran lembaga khusus ini menunjukkan komitmen negara untuk menangani perlindungan data pribadi secara serius dan terkoordinasi.

Namun demikian, implementasi UU PDP masih menghadapi berbagai tantangan dalam praktik. Salah satu tantangan terbesar adalah dalam hal penegakan sanksi. UU PDP menetapkan denda administratif yang signifikan, yang dapat mencapai dua persen dari pendapatan tahunan atau penerimaan perusahaan, dirancang untuk memberikan efek jera dan mendorong perusahaan lebih berhati-hati dalam mengelola data pribadi. Selain itu, UU PDP memberikan hak kepada pemilik data pribadi yang dirugikan akibat pelanggaran data untuk mengajukan gugatan perdata guna mendapatkan ganti rugi. Namun, dalam praktiknya, jumlah kasus yang dilaporkan dan diproses masih relatif terbatas, menunjukkan bahwa sosialisasi regulasi dan kesadaran publik terhadap hak-hak mereka masih perlu ditingkatkan.

Selain UU PDP, perlindungan data pribadi di sektor perbankan syariah juga diatur melalui Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Regulasi ini telah beberapa kali mengalami perubahan terakhir melalui Undang-Undang Nomor 19 Tahun 2016, dan memberikan dasar hukum yang kuat untuk perlindungan data pribadi pengguna serta mengatur kewajiban penyedia layanan untuk melindungi informasi pribadi pengguna (Muninggar et al., 2024). UU ITE secara khusus mengatur tanggung jawab penyelenggara sistem elektronik dalam melindungi data pribadi konsumen dan memberikan hak bagi konsumen untuk mengajukan gugatan

atas kerugian yang timbul akibat gangguan pada infrastruktur informasi mereka. Gangguan terhadap infrastruktur informasi vital dapat menimbulkan kerugian dan dampak yang serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, serta perekonomian nasional. Setiap orang dapat mengajukan gugatan terhadap pihak yang menyelenggarakan Sistem Elektronik dan/atau menggunakan Teknologi Informasi yang menimbulkan kerugian (Budhijanto, 2024).

Regulasi perlindungan konsumen juga memainkan peran penting dalam perlindungan data pribadi nasabah perbankan. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UU Perlindungan Konsumen) menetapkan berbagai hak konsumen, termasuk hak untuk mendapatkan informasi yang benar, jelas, dan jujur tentang kondisi dan jaminan barang dan/atau jasa, serta hak atas privasi dan keamanan dalam bertransaksi. Dalam teori hukum responsif, diemukakan bahwa hukum memiliki peranan sebagai sarana untuk memfasilitasi berbagai reaksi perkembangan dan kebutuhan sosial, tidak hanya melalui kerangka pengaturan namun juga mewujudkan perubahan sosial yang harmonis dengan mekanisme yang teratur. Undang-undang tentang Perlindungan Konsumen dan Undang-Undang tentang Informasi dan Transaksi Elektronik (UU ITE) dirancang sebagai respons terhadap kebutuhan sosial akan perlindungan konsumen dalam era digital (Muninggar & Rahardiansah, 2024).

Dalam konteks perbankan syariah khususnya, Otoritas Jasa Keuangan (OJK) telah menerbitkan berbagai peraturan untuk mengatur dan mengawasi operasional bank syariah. Peraturan OJK No. 6/POJK.07/2022 tentang Perlindungan Konsumen di Sektor Jasa Keuangan mempertegas tanggung jawab bank dalam melindungi hak-hak nasabah secara hukum dan etika. Data nasabah merupakan aset hukum yang dilindungi, dan jika tidak dikelola dengan baik, bank syariah bisa menghadapi tuntutan hukum serta kehilangan kepercayaan masyarakat (Hanifaturasyda, 2025). Selain itu, OJK juga telah menerbitkan Peraturan tentang Manajemen Risiko Teknologi Informasi yang mengharuskan bank untuk mengidentifikasi, mengukur, memantau, dan mengendalikan risiko teknologi informasi, termasuk risiko kebocoran data pribadi. Peraturan OJK tentang Manajemen Risiko TI telah disusun untuk mendorong peningkatan keamanan siber (Mulyana, 2025).

Dalam rangka mengimplementasikan regulasi tersebut, perbankan syariah telah berupaya semaksimal mungkin memenuhi ketentuan hukum Indonesia dengan bertransaksi melalui internet banking didukung dengan pengawasan ketat dari otoritas berwenang (Prayogo, Korah, & Soepeno, 2024). Namun, upaya ini masih dirasa belum cukup mengingat terus berkembangnya ancaman siber. Sektor keuangan menjadi salah satu target utama dalam serangan siber global. Menurut data Badan Siber dan Sandi Negara (BSSN), pada tahun 2024, terdapat 47.729 anomali trafik yang terdeteksi di sektor keuangan, dengan lebih dari 56% di antaranya melibatkan aktivitas malware dan ancaman siber lainnya. Hal ini menunjukkan bahwa sistem keuangan digital merupakan sasaran empuk bagi pelaku kejahatan siber karena menyimpan data sensitif dan memiliki nilai ekonomi tinggi.

Dari perspektif implementasi, terdapat beberapa tantangan utama yang dihadapi oleh sistem perlindungan data pribadi di sektor perbankan syariah yaitu, lemahnya mekanisme pengawasan. Meskipun regulasi telah diterbitkan, mekanisme pengawasan terhadap kepatuhan bank syariah terhadap regulasi ini masih memiliki keterbatasan. Pengawasan yang dilakukan oleh OJK bersifat menyeluruh, mirip dengan sistem perbankan konvensional, namun dengan penekanan pada penerapan prinsip syariah dan kehati-hatian dalam praktik usaha bank syariah. Namun, dalam praktiknya, frekuensi

audit keamanan siber dan verifikasi perlindungan data tidak selalu dilakukan secara berkala dan komprehensif, terutama untuk bank syariah yang lebih kecil atau yang baru tergabung dalam ekosistem digital.

Lemahnya pengawasan serta minimnya hukuman terhadap pelanggaran membuat lembaga keuangan belum sepenuhnya terdorong untuk menerapkan sistem keamanan yang optimal (Ambarwati et al., 2023). Meskipun UU PDP dan peraturan OJK telah mengatur berbagai sanksi, namun jumlah penerapan sanksi masih sangat terbatas. Hal ini mungkin disebabkan oleh proses penyidikan dan pembuktian yang panjang, serta adanya persepsi bahwa risiko pelanggaran masih lebih rendah dibandingkan biaya investasi dalam sistem keamanan yang canggih.

Di era open banking menghadirkan ekosistem yang lebih kompleks dengan melibatkan lebih banyak pihak dalam pemrosesan data pribadi. Cakupan data dalam Open API Payment dan definisi data milik konsumen telah secara jelas mengamanatkan kepada penyedia API dan pengguna API untuk menerapkan perlindungan data pribadi. Dengan demikian, penyedia API dan pengguna API serta pihak ketiga yang berkolaborasi harus memperlakukan data milik konsumen sebagai data pribadi yang harus dilindungi. Dalam hal ini, otoritas yang terlibat dalam open banking dapat mencakup pengawas perbankan, otoritas persaingan atau standar khusus, otoritas perlindungan konsumen, otoritas privasi data, dan mekanisme sengketa alternatif (Pati & Pratama, 2022). Koordinasi antara berbagai otoritas ini masih memerlukan peningkatan untuk memastikan sinergi dalam perlindungan data.

Perlindungan data pribadi dalam konteks bank syariah tidak hanya merupakan tanggung jawab hukum positif, tetapi juga merupakan kewajiban moral dan spiritual yang didasarkan pada prinsip-prinsip Islam. a.Prinsip Amanah**,** konsep amanah merupakan salah satu fondasi etika bisnis Islam yang paling penting. Dalam Alquran, Surah Al-Anfal Ayat 27 menyebutkan: "Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul, dan jangan pula mengkhianati amanat yang dipercayakan kepada kamu, sedang kamu mengetahui." Bank syariah, sebagai lembaga keuangan yang beroperasi berdasarkan prinsip-prinsip Islam, memiliki tanggung jawab lebih besar untuk menjaga berbuat baik kepada semua orang, bahkan ketika tidak ada yang melihat. Dalam amanah nasabah dalam bentuk data pribadi mereka; b. Prinsip ihsan**,** dalam Islam berarti perspektif syariah, terdapat beberapa prinsip fundamental yang mendukung perlindungan data pribadi nasabah. Dalam konteks perlindungan data pribadi, ihsan berarti bahwa bank syariah harus melindungi data pribadi nasabah dengan penuh kesadaran akan tanggung jawab mereka, bukan hanya karena adanya regulasi yang mewajibkan, tetapi karena ketulusan dalam melayani kepentingan nasabah (Rialita & Putri, 2025); c. Prinsip privacy, setiap individu berhak atas privasi mereka. Firman Allah dalam Surah An-Nur Ayat 27-28 mengatur tentang pentingnya menghormati privasi orang lain. Privasi data adalah hak fundamental yang harus dijaga secara kolektif menurut Islam (Ambarwati et al., 2023) ; d. Prinsip maslahah**,** setiap keputusan dan tindakan harus didasarkan pada pertimbangan kemaslahatan bersama. Upaya penegakan dan perlindungan hak asasi manusia yang dilakukan oleh suatu negara seharusnya berdasarkan pada praktik demokrasi yang secara tidak langsung juga sejalan dengan syariah Islam, yang dalam hal ini mengacu pada maqashid syariah dalam Islam (Persadha, 2024).

Integrasi prinsip-prinsip syariah dalam sistem perlindungan data pribadi perbankan syariah tidak hanya memperkuat landasan etika, tetapi juga meningkatkan komitmen institusi keuangan terhadap perlindungan konsumen. Regulasi pemerintah harus menekankan pentingnya internalisasi nilai-nilai syariah ini dalam operasional

harian bank syariah. Peraturan OJK, misalnya, dapat memperkuat komitmen bank syariah untuk menerapkan prinsip-prinsip syariah dalam manajemen data pribadi nasabah, bukan hanya sebagai kepatuhan terhadap regulasi, tetapi sebagai bagian integral dari identitas dan nilai-nilai bank syariah (Ghariza Ardhia Adhnin, 2025).

Bentuk-Bentuk Penyalahgunaan Data Finansial Nasabah Bank Syariah dalam Praktik Open Banking

Hasil penelitian mengidentifikasi empat bentuk penyalahgunaan data finansial yang terjadi dalam ekosistem open banking. Analisis terhadap masing-masing bentuk penyalahgunaan ini mengungkapkan kompleksitas tantangan yang dihadapi oleh sektor perbankan syariah. a. Phishing dan Social Engineering merupakan bentuk penyalahgunaan data yang paling umum dan terus berkembang. Pencurian data elektronik yang umumnya disebut phishing melibatkan perolehan informasi pribadi secara ilegal, termasuk ID pengguna, PIN, nomor rekening bank, dan nomor kartu kredit (Putri et al., 2024). Data dari BSSN menunjukkan bahwa 34% dari insiden keamanan siber pada sektor keuangan pada 2024 melibatkan phishing atau social engineering. Efendi et al. (2024) mendeskripsikan financial technology sebagai pisau bermata dua, di mana di satu sisi memudahkan proses transaksi keuangan, tetapi di sisi lain, kekurangan perlindungan data pribadi dapat membahayakan konsumen; b. Unauthorized Acces, terdapat lebih banyak entry point untuk serangan dibandingkan dengan sistem perbankan tradisional. Pati & Pratama (2022) menjelaskan bahwa cakupan data dalam Open API Payment telah secara jelas mengamanatkan kepada penyedia API dan pengguna API untuk menerapkan perlindungan data pribadi. Dengan demikian, penyedia API dan pengguna API serta pihak ketiga yang berkolaborasi harus memperlakukan data milik konsumen sebagai data pribadi yang harus dilindungi. Namun, penelitian lapangan menunjukkan bahwa 78% dari unauthorized access pada sektor perbankan terjadi melalui kerentanan pada pihak ketiga, bukan pada bank utama.

Kasus kebocoran data pada Bank Syariah Indonesia tahun 2023 merupakan contoh nyata dari risiko ini. Rizal & Ardhian (2023) melaporkan bahwa kelompok hacker LockBit berhasil mencuri 1,5 terabyte data internal yang meliputi 15 juta data pribadi nasabah. Insiden ini menunjukkan bahwa bahkan institusi perbankan besar dapat menjadi target serangan dan mengalami unauthorized access yang berdampak massif; c. Data Trafficking merupakan penjualan data pribadi nasabah kepada pihak ketiga, baik untuk tujuan spamming, penipuan targeted, atau keperluan kriminal lainnya. Data trafficking seringkali dilakukan oleh insider (karyawan institusi keuangan atau fintech partner) yang memiliki akses legitimate ke data pribadi nasabah. Budhijanto (2024) menekankan bahwa penyalahgunaan data pribadi oleh pihak yang tidak berwenang tidak hanya melanggar privasi, tetapi juga dapat menimbulkan kerugian besar bagi individu. Dalam kasus data trafficking, korban seringkali tidak menyadari bahwa data pribadi mereka telah dijual sampai mereka mulai menerima komunikasi yang tidak diinginkan atau menjadi korban penipuan berdasarkan data pribadi mereka;

d. Account Takeover dan Fraud melibatkan perambasan akun nasabah dan melakukan transaksi ilegal menggunakan akun tersebut. Account takeover erat kaitannya dengan phishing dan unauthorized access, namun lebih berfokus pada manfaatkan akun yang sudah dikompromikan untuk melakukan tindakan fraud. Penelitian menunjukkan bahwa account takeover menyebabkan kerugian finansial paling besar dibandingkan bentuk penyalahgunaan data lainnya, dengan rata-rata kerugian per insiden mencapai Rp 500 juta hingga Rp 2 miliar. Kombinasi dari keempat bentuk penyalahgunaan ini menciptakan lanskap ancaman yang sangat kompleks dan dinamis dalam ekosistem open banking.

Ambarwati et al. (2023) mencatat bahwa isu cybercrime semakin meningkat, dengan statistik menunjukkan ribuan laporan kasus setiap tahun, sehingga perlindungan data menjadi sangat penting. Dalam perspektif Islam, menjaga data pribadi adalah hak dasar yang tidak boleh dilanggar, dan perilaku etis menjadi salah satu cara pencegahannya.

Efektivitas Mekanisme Pengawasan dan Penegakan Hukum yang Dilakukan Lembaga Negara Terkait

Data menunjukkan bahwa dari 237 kasus penyalahgunaan data pribadi yang dilaporkan pada tahun 2024, hanya 10 kasus (4,2%) yang berakhir dengan putusan pidana. Angka ini menunjukkan ketidakefektifan yang signifikan dalam sistem penegakan hukum. Lemahnya pengawasan dan minimnya hukuman terhadap pelanggaran membuat lembaga keuangan belum sepenuhnya terdorong untuk menerapkan sistem keamanan yang optimal (Ambarwati et al., 2023). Tingkat drop-out yang tinggi pada tahap penyelidikan (60%) menunjukkan adanya masalah struktural dalam sistem penegakan hukum, baik dari segi kapasitas penyidik, kualitas bukti yang dikumpulkan, maupun kesulitan dalam pembuktian kejahatan siber.

Mulyana (2025) menjelaskan bahwa meskipun regulasi pemerintah seperti UU PDP dan Peraturan OJK tentang Manajemen Risiko Teknologi Informasi telah disusun untuk mendorong peningkatan keamanan siber, implementasinya masih perlu dikaji ulang efektivitasnya. Salah satu faktor utama yang berkontribusi pada rendahnya tingkat penyelesaian kasus adalah keterbatasan sumber daya manusia yang terlatih dalam cyber forensics dan investigasi kejahatan digital. Sebagian besar penyidik di Polda Siber dan kejaksaan tidak memiliki sertifikasi internasional dalam cyber forensics, sehingga proses pengumpulan dan analisis bukti digital seringkali tidak memenuhi standar yang diperlukan untuk penuntutan yang berhasil.

Dalam ekosistem open banking, terdapat banyak pihak yang terlibat dalam pemrosesan data pribadi, dan setiap pihak ini berada di bawah yurisdiksi regulator yang berbeda. OJK bertanggung jawab atas pengawasan perbankan, Kementerian Komunikasi dan Informatika mengatur aspek keamanan siber, Komisi Persaingan Usaha mengawasi aspek kompetisi, dan lembaga perlindungan data pribadi (yang diamanatkan UU PDP) akan mengawasi aspek perlindungan data secara umum. Pati & Pratama (2022) menekankan bahwa otoritas yang terlibat dalam open banking dapat mencakup pengawas perbankan, otoritas persaingan atau standar khusus, otoritas perlindungan konsumen, otoritas privasi data, dan mekanisme sengketa alternatif. Namun, koordinasi antara berbagai otoritas ini masih sangat terbatas.

Penelitian menemukan bahwa tidak ada forum koordinasi reguler yang melibatkan semua regulator terkait untuk berbagi informasi tentang ancaman keamanan siber, praktik terbaik, atau kasus-kasus pelanggaran yang sedang ditangani. Akibatnya, sering terjadi tumpang tindih dalam pengawasan atau sebaliknya, ada celah pengawasan di mana suatu aktivitas tidak diawasi oleh regulator manapun. Menurut teori hukum responsif yang dikemukakan oleh Muninggar et al. (2024), hukum memiliki peranan sebagai sarana untuk memfasilitasi berbagai reaksi perkembangan dan kebutuhan sosial, tidak hanya melalui kerangka pengaturan namun juga mewujudkan perubahan sosial yang harmonis dengan mekanisme yang teratur. Namun, tanpa koordinasi yang efektif, hukum tidak dapat berfungsi secara optimal dalam melindungi hak-hak konsumen.

Salah satu temuan yang paling mengkhawatirkan dari penelitian ini adalah rendahnya tingkat pelaporan kasus penyalahgunaan data pribadi oleh masyarakat. Estimasi berdasarkan survey victimization menunjukkan bahwa hanya 15-20% dari korban penyalahgunaan data pribadi yang melaporkan insiden tersebut ke pihak berwajib

atau institusi keuangan. Rendahnya tingkat pelaporan ini disebabkan oleh beberapa faktor: (1) kurangnya kesadaran masyarakat tentang hak-hak mereka dalam hal perlindungan data pribadi; (2) ketidakpercayaan terhadap sistem penegakan hukum; (3) proses pelaporan yang rumit dan memakan waktu; (4) kekhawatiran akan stigma atau dampak negatif terhadap reputasi mereka.

Pemerintah perlu aktif dalam mengedukasi masyarakat mengenai pentingnya perlindungan data pribadi serta hak-hak yang dimiliki setiap individu terkait data mereka. Namun, program edukasi yang telah dilakukan oleh OJK dan lembaga terkait masih sangat terbatas dalam cakupan dan frekuensinya. Banyak konsumen yang masih enggan menggunakan layanan perbankan digital karena khawatir akan keamanan data pribadi mereka, namun mereka tidak mengetahui langkah-langkah yang dapat mereka ambil untuk melindungi data mereka atau mekanisme untuk melaporkan pelanggaran. Persadha (2024).

Meskipun UU PDP telah menetapkan denda administratif yang signifikan (dapat mencapai 2% dari pendapatan tahunan perusahaan) dan membuka kemungkinan hukuman pidana, penerapan sanksi di lapangan masih belum konsisten. Dari 36 kasus yang berakhir dengan putusan, 72% berupa denda administratif dengan nilai yang relatif rendah (rata-rata hanya Rp 50-100 juta), yang tidak cukup memberikan efek jera kepada institusi yang melakukan pelanggaran. Hanifaturasyda (2025) menjelaskan bahwa data nasabah merupakan aset hukum yang dilindungi, dan jika tidak dikelola dengan baik, bank syariah bisa menghadapi tuntutan hukum serta kehilangan kepercayaan masyarakat. Namun, dalam praktiknya, tuntutan hukum yang signifikan terhadap bank yang melakukan pelanggaran perlindungan data masih sangat jarang terjadi.

Salah satu kritik yang sering dilontarkan terhadap mekanisme pengawasan yang ada adalah kurangnya transparansi. OJK dan regulator lainnya jarang mempublikasikan hasil audit keamanan data atau laporan pelanggaran yang telah ditangani. Akibatnya, masyarakat tidak memiliki informasi yang cukup untuk menilai keamanan institusi keuangan yang mereka gunakan. Wiraguna & Barthos (2025) menekankan bahwa perlindungan data pribadi di era digital merupakan pilar utama dalam menjamin hak konstitusional individu atas privasi, dan transparansi dalam pengawasan adalah bagian integral dari perlindungan ini.

KESIMPULAN

Berdasarkan seluruh pembahasan, dapat disimpulkan bahwa negara memiliki kewajiban konstitusional untuk melindungi hak privasi digital nasabah bank syariah dalam era open banking melalui pendekatan yang integratif antara penguatan regulasi, penegakan hukum yang efektif, dan internalisasi nilai-nilai syariah. Temuan penelitian mengungkapkan bahwa meskipun kerangka regulasi telah memadai, implementasinya menghadapi tantangan signifikan berupa lemahnya mekanisme pengawasan, rendahnya tingkat penuntutan kasus penyalahgunaan data yang hanya mencapai 4,2%, serta belum optimalnya integrasi prinsip syariah dalam operasional perlindungan data dimana hanya 40% bank syariah yang telah mengadopsi prinsip amanah dan ihsan secara eksplisit. Dominannya kerentanan pada pihak ketiga (fintech partner) yang menjadi penyebab 78% kebocoran data mempertegas perlunya harmonisasi koordinasi antar regulator dan peningkatan kapasitas teknis penegak hukum. Oleh karena itu, pemenuhan kewajiban negara memerlukan strategi holistik yang tidak hanya mengandalkan aspek legal-formal tetapi juga membangun ekosistem perlindungan data yang berlandaskan etika digital syariah dan didukung oleh sistem pengawasan yang transparan dan accountable.

DAFTAR PUSTAKA

Ambarwati, D., Studi, P., Syariah, E., Agama, I., & Negeri, I. (2023). Customer Data Protection Mitigations: Data Security System In Lampung Building Baitul Mal Wa Tamwil Transaction. *Jurnal Ekonomi Islam*, 9(2), 417–434.

Antoine, R. A. (2025). Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Hukum Digital*, 2(1), 316–327.

Asosiasi Perbankan Syariah Indonesia. (2024). *Laporan Industri Perbankan Syariah Indonesia 2024*. Asbisindo.

Badan Siber dan Sandi Negara. (2024). *Laporan Ancaman Siber Nasional 2024*. Kementerian Komunikasi dan Informatika Republik Indonesia.

Budhijanto, D. (2024). *Hukum Perlindungan Data Pribadi & Nasional* (Ed. Nomor October). Refika Aditama.

Djafar, W., Ruben, B., Sumigar, F., & Setianti, B. L. (n.d.). *Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia*. Lembaga Studi dan Advokasi Masyarakat (ELSAM).

Efendi, T. K., Esza, M., Firmanda, M., Alfarisy, F. R., Javantara, A. C., & Indrarini, R. (2024). Analisis Kebijakan Perlindungan Nasabah Pada Bank Digital Syariah Di Indonesia. *Jurnal Keuangan Syariah*, 2(November), 1–7.

Ghariza Ardhia Adhnin, B. (2025). Efektivitas Pengawasan Produk Keuangan Syariah oleh Otoritas Jasa Keuangan. *Media Hukum Indonesia (MHI)*, *2*(6).

Hanifaturasyda, A. (2025). Penerapan Manajemen Risiko Hukum Dalam Perbankan Syariah: Perspektif Terkini Terhadap Regulasi Dan Teknologi. *Jurnal Perbankan Syariah*, 3, 290–298.

Marifah, M. (2025). *E-Book Hukum Digital Dan Privasi Data*. Pusat Kajian Hukum Digital.

Mulyana, S. L. (2025). Implementasi Cyber Security Dalam Sistem Perbankan Digital. *Jurnal Teknologi Informasi dan Keamanan*, 2(4), 276–289.

Muninggar, R. A., Rahardiansah, T., Magister, S., Hukum, I., Trisakti, U., Hukum, F., & Trisakti, U. (2024). Pemberdayaan Hukum Pembayaran Digital Melalui Penggunaan Teknologi Quick Response Code Indonesian Standar Di Masyarakat. *Jurnal Hukum Bisnis Digital*, 6, 1–15.

Otoritas Jasa Keuangan. (2025). *Roadmap Perbankan Digital Indonesia 2025-2030*. OJK.

Otoritas Jasa Keuangan. (2022). Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 Tentang Perlindungan Konsumen di Sektor Jasa Keuangan. *Berita Negara Republik Indonesia*.

Pati, U. K., & Pratama, A. M. (2022). *Hukum Perbankan Dan Open Banking Perkembangan Bank Umum Indonesia Di Era Digitalisasi Dan Open Data*. CV. Indotama Solo.

Prayogo, P., Korah, R. S. M., & Soepeno, M. H. (2024). Analisis Perlindungan Hukum Data Pribadi Nasabah Pada Transaksi Digital. *Jurnal Hukum Perbankan*, 9(1), 39–54.

Persadha, D. P. (2024). *Implementasi UU Perlindungan Data Pribadi Di Indonesia Tantangan, Strategi, Dan Solusi*. Cissrec - Yayasan Lembaga Riset Siber Indonesia.

Putri, N., Natasya, A., Sabina, Y., Amelia, P., Reva, A., & Garneta, W. (2024). Analisis Yuridis Perlindungan Nasabah Bank Dalam Tindak Pidana Pencurian Data Melalui UU ITE Dan UU Perbankan. *Jurnal Hukum Pidana dan Perbankan*, 2(4), 926–934.

Rialita, A. J., & Putri, M. C. (2025). Moderasi Beragama, Ekonomi Islam Sebagai Prinsip Etis Dalam Digital Finance Berbasis Ekonomi Syariah. *Jurnal Ekonomi Syariah dan Keuangan Islam*, 04(02), 1–13.

Rizal, I., & Ardhian, N. (2023). Dampak Serangan Siber Dan Kebocoran Data Pada Perbankan Syariah Terhadap Tingkat Kepercayaan Nasabah. *Jurnal Keamanan Informasi*, 1(3), 351–359.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. *Lembaran Negara Republik Indonesia Tahun 1999*.

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. *Lembaran Negara Republik Indonesia Tahun 2008*. (Diubah dengan Undang-Undang Nomor 19 Tahun 2016).

Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Lembaran Negara Republik Indonesia Tahun 2022*.

Wiraguna, S. A., & Barthos, M. (2025). *Hukum Privasi Dan Perlindungan Data Pribadi Di Indonesia*. Universitas Indonesia Press.