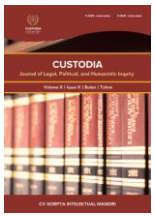

Custodia: Journal of Legal, Political, and Humanistic Inquiry
Vol 1 No 2 December 2025, Hal 10-17
ISSN: 3123-2116 (Print) ISSN: 3123-2108 (Electronic)
Open Access: https://scriptaintelektual.com/custodia

Pemanfaatan Artificial Intelligence dan Pelanggaran Rahasia Bank: Studi Kasus Kebocoran Data Nasabah Bank Syariah Indonesia (BSI) ditinjau dari Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Widya Utami[1], Virda Rachma Mulya[2], Garnis Putri Shima[3], Yahya Ayyash[4], Aditya Rizki Andriyanto[5], Raden Miko Ardiansyah Judhokusumo[6]
[1-6] Universitas Muhammadiyah Surakarta, Indonesia
email: c100230369@student.ums.ac.id

Article Info :
Received:
15-10-2025
Revised:
23-11-2025
Accepted:
05-12-2025

Abstract

The rapid digital transformation in the banking sector has significantly changed the management and processing of customer data, particularly within Islamic banking institutions. The use of intelligent computing systems enhances efficiency, transaction speed, and service accuracy, yet it also increases vulnerability to data breaches and violations of bank secrecy. This study examines the leakage of customer data at Bank Syariah Indonesia as a case study, focusing on its legal implications under Article 40 of Law Number 10 of 1998 concerning Banking. Using normative legal research methods, this study analyzes statutory regulations, legal doctrines, and relevant scholarly works to assess the bank's responsibility for safeguarding customer confidentiality. The findings indicate that data leakage constitutes a violation of bank secrecy obligations and exposes the bank to administrative, civil, and potential criminal liability. Furthermore, inadequate data protection mechanisms weaken customer trust and undermine legal certainty. Strengthening governance frameworks, enhancing digital security systems, and ensuring strict law enforcement are essential to protect customers' rights and maintain the credibility of Islamic banking in the digital era.

Keywords: *bank secrecy, customer data protection, Islamic banking, digital banking, legal liability.*

Abstrak

Transformasi digital yang cepat di sektor perbankan telah mengubah secara signifikan pengelolaan dan pemrosesan data pelanggan, terutama di lembaga perbankan syariah. Penggunaan sistem komputasi cerdas meningkatkan efisiensi, kecepatan transaksi, dan akurasi layanan, namun juga meningkatkan kerentanan terhadap kebocoran data dan pelanggaran kerahasiaan bank. Studi ini mengkaji kebocoran data pelanggan di Bank Syariah Indonesia sebagai studi kasus, dengan fokus pada implikasi hukumnya berdasarkan Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Menggunakan metode penelitian hukum normatif, studi ini menganalisis peraturan perundang-undangan, doktrin hukum, dan karya ilmiah terkait untuk menilai tanggung jawab bank dalam menjaga kerahasiaan pelanggan. Hasil penelitian menunjukkan bahwa kebocoran data merupakan pelanggaran terhadap kewajiban kerahasiaan bank dan menjadikan bank rentan terhadap tanggung jawab administratif, perdata, dan potensi pidana. Selain itu, mekanisme perlindungan data yang tidak memadai melemahkan kepercayaan pelanggan dan mengganggu kepastian hukum. Penguatan kerangka tata kelola, peningkatan sistem keamanan digital, dan penegakan hukum yang ketat merupakan hal yang esensial untuk melindungi hak-hak pelanggan dan mempertahankan kredibilitas perbankan syariah di era digital.

Kata kunci: kerahasiaan bank, perlindungan data pelanggan, perbankan Islam, perbankan digital, tanggung jawab hukum.

PENDAHULUAN

Perkembangan teknologi digital dalam sektor perbankan telah mendorong perubahan mendasar pada sistem pengelolaan data nasabah, terutama melalui penggunaan sistem komputasi cerdas yang berfungsi mengolah informasi dalam jumlah besar secara cepat dan terintegrasi. Transformasi ini membawa implikasi serius terhadap tata kelola kerahasiaan data, mengingat data perbankan memiliki nilai ekonomi, hukum, dan reputasi yang tinggi bagi institusi keuangan. Bank sebagai lembaga kepercayaan dituntut menjaga integritas sistem informasi agar tidak membuka celah kebocoran data

nasabah yang berpotensi menimbulkan kerugian luas. Isu ini semakin relevan ketika praktik digitalisasi berjalan lebih cepat dibandingkan dengan kesiapan regulasi dan mekanisme pengawasan internal perbankan (Daraba et al., 2023).

Peningkatan penggunaan teknologi berbasis otomatisasi dan analitik dalam layanan perbankan digital memperluas ruang pengumpulan, pemrosesan, serta distribusi data pribadi nasabah. Kondisi tersebut memunculkan risiko penyalahgunaan data, baik melalui kegagalan sistem keamanan maupun akibat kelalaian tata kelola internal. Penelitian sebelumnya menunjukkan bahwa pemanfaatan teknologi digital dalam transaksi perbankan syariah memiliki korelasi dengan meningkatnya potensi pelanggaran hak privasi nasabah apabila tidak disertai pengendalian yang memadai (Antoine et al., 2025). Situasi ini menempatkan perlindungan data sebagai isu sentral dalam menjaga keberlanjutan industri perbankan syariah.

Kasus kebocoran data nasabah Bank Syariah Indonesia menjadi peristiwa penting yang menggambarkan kerentanan sistem informasi perbankan nasional. Informasi mengenai data nasabah yang dicuri dan tidak dapat dijamin kembali menimbulkan kekhawatiran publik terhadap efektivitas perlindungan kerahasiaan bank (Display UB, 2023). Peristiwa tersebut memperlihatkan bahwa ancaman terhadap data nasabah tidak hanya bersumber dari faktor eksternal, tetapi juga berkaitan dengan desain sistem dan kebijakan internal lembaga perbankan. Kepercayaan masyarakat terhadap bank syariah sebagai institusi yang menjunjung nilai etika dan amanah pun mengalami ujian serius.

Dalam hukum perbankan, kewajiban menjaga rahasia bank merupakan prinsip fundamental yang melekat pada setiap aktivitas penghimpunan dan penyaluran dana masyarakat. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan secara tegas mengatur larangan pengungkapan data nasabah tanpa dasar hukum yang sah. Pelanggaran terhadap ketentuan ini tidak hanya menimbulkan konsekuensi administratif, tetapi juga membuka ruang pertanggungjawaban pidana dan perdata. Penelitian hukum menegaskan bahwa kebocoran data nasabah dapat dikualifikasikan sebagai bentuk pelanggaran rahasia bank yang merugikan hak nasabah secara langsung (Bhoki et al., 2024).

Di sisi lain, perkembangan sistem komputasi cerdas dalam pelayanan publik dan sektor keuangan menuntut adanya penyesuaian prinsip hukum agar tetap sejalan dengan nilai keadilan dan perlindungan hak individu. Kajian mengenai pemanfaatan teknologi cerdas dalam pelayanan publik menunjukkan pentingnya prinsip kehati-hatian, akuntabilitas, dan pengawasan agar penggunaan teknologi tidak melampaui batas kewenangan hukum (Ardiansyah et al., 2025). Prinsip-prinsip tersebut relevan untuk diterapkan dalam sektor perbankan syariah yang berlandaskan nilai keadilan dan perlindungan kepentingan umat. Ketidakhadiran kerangka etis dan hukum yang kuat berpotensi menjadikan teknologi sebagai sumber masalah hukum baru.

Upaya penguatan perlindungan data pribadi di Indonesia telah mengalami perkembangan melalui pengesahan Undang-Undang Perlindungan Data Pribadi Tahun 2022. Instrumen seperti Data Protection Impact Assessment dipandang penting untuk memastikan kepatuhan lembaga keuangan terhadap prinsip perlindungan data sejak tahap perancangan sistem hingga implementasi operasional (Khair & Wiraguna, 2025). Penerapan instrumen tersebut dalam sektor perbankan syariah masih menghadapi tantangan terkait integrasi kebijakan, sumber daya manusia, dan kesiapan infrastruktur. Kondisi ini menunjukkan adanya kesenjangan antara norma hukum dan praktik pengelolaan data di lapangan.

Analisis terhadap perlindungan nasabah BSI dalam layanan perbankan digital mengungkap bahwa mekanisme pengamanan data belum sepenuhnya mampu memberikan jaminan perlindungan yang optimal. Temuan empiris menunjukkan bahwa nasabah masih berada pada posisi rentan ketika terjadi kebocoran data, terutama dalam hal pemulihan hak dan kompensasi kerugian (Putri et al., 2023). Keadaan ini menimbulkan pertanyaan serius mengenai efektivitas penerapan ketentuan rahasia bank dalam menghadapi kompleksitas sistem digital modern. Perlu adanya kajian hukum yang menelaah hubungan antara pemanfaatan teknologi dan kewajiban perlindungan rahasia nasabah secara komprehensif.

Berdasarkan kondisi tersebut, penelitian ini menjadi penting untuk mengkaji pemanfaatan teknologi komputasi cerdas dalam perbankan syariah serta implikasinya terhadap pelanggaran rahasia bank. Studi kasus kebocoran data nasabah Bank Syariah Indonesia memberikan gambaran konkret mengenai tantangan hukum yang dihadapi dalam menjaga kerahasiaan data. Peninjauan terhadap Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan diharapkan mampu memberikan analisis normatif yang relevan dengan dinamika digitalisasi perbankan. Kajian ini diharapkan dapat

memperkaya diskursus hukum perbankan dan perlindungan data dalam sistem keuangan syariah di Indonesia.

METODE PENELITIAN

Penelitian ini merupakan penelitian hukum yang bersifat normatif dengan pendekatan perundang-undangan dan pendekatan konseptual, yang bertujuan menganalisis pemanfaatan teknologi dalam perbankan syariah serta implikasinya terhadap pelanggaran rahasia bank. Bahan hukum primer meliputi Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Perlindungan Data Pribadi Tahun 2022, serta peraturan terkait lainnya, sedangkan bahan hukum sekunder terdiri atas jurnal ilmiah, buku teks hukum, dan hasil penelitian terdahulu yang relevan dengan isu kebocoran data nasabah Bank Syariah Indonesia. Teknik pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan menelaah dan mengkaji sumber hukum secara sistematis dan mendalam. Analisis bahan hukum dilakukan secara kualitatif dengan metode interpretasi hukum untuk menilai kesesuaian antara norma hukum yang berlaku dan praktik pengelolaan data nasabah dalam perbankan syariah.

HASIL DAN PEMBAHASAN

Pemanfaatan Sistem Komputasi Cerdas dalam Operasional Perbankan Syariah dan Risiko Kerahasiaan Data Nasabah

Pemanfaatan sistem komputasi berbasis pengolahan data otomatis telah menjadi bagian penting dalam transformasi operasional perbankan syariah, khususnya pada aspek layanan digital, manajemen risiko, dan analisis perilaku nasabah. Penerapan teknologi tersebut memungkinkan bank meningkatkan efisiensi layanan, kecepatan transaksi, serta akurasi pengambilan keputusan berbasis data. Namun, peningkatan ketergantungan pada sistem digital juga memperluas ruang eksposur terhadap data pribadi nasabah yang dilindungi oleh hukum perbankan. Kondisi ini menuntut penguatan tata kelola kerahasiaan bank agar sejalan dengan prinsip kehati-hatian dan kepastian hukum (Maulida et al., 2025; Daraba et al., 2023).

Dalam praktik perbankan syariah modern, sistem komputasi cerdas digunakan untuk mengelola transaksi digital, verifikasi identitas, serta pemantauan aktivitas keuangan nasabah secara berkelanjutan. Pengolahan data dalam skala besar tersebut menciptakan konsentrasi informasi sensitif pada satu sistem terpusat. Ketika pengamanan sistem tidak berjalan optimal, potensi kebocoran data menjadi risiko yang nyata dan berdampak luas. Penelitian mengenai penyalahgunaan data dalam transaksi digital menunjukkan bahwa kelemahan tata kelola sistem sering kali menjadi pintu masuk pelanggaran hak privasi nasabah (Antoine et al., 2025; Safitri et al., 2020).

Kasus kebocoran data nasabah Bank Syariah Indonesia menunjukkan bahwa transformasi digital tidak selalu diikuti oleh kesiapan sistem perlindungan data yang memadai. Informasi yang beredar menyebutkan bahwa data nasabah yang telah tercuri tidak dapat dijamin untuk dipulihkan sepenuhnya, sehingga menimbulkan ketidakpastian hukum bagi para korban. Peristiwa ini memperlihatkan bahwa risiko teknologi tidak hanya bersifat teknis, tetapi juga berdimensi hukum dan kepercayaan publik. Kebocoran data tersebut menjadi indikator lemahnya mekanisme pengamanan dan pengawasan internal bank (Display UB, 2023; Ghozali et al., 2024).

Dalam perspektif hukum perbankan, rahasia bank mencakup seluruh informasi mengenai nasabah penyimpan dan simpanannya yang wajib dijaga oleh bank. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menegaskan larangan pengungkapan data nasabah tanpa dasar hukum yang sah. Penggunaan sistem digital dalam operasional bank tidak menghapus kewajiban hukum tersebut. Setiap bentuk pemrosesan data yang berujung pada kebocoran dapat dikualifikasikan sebagai pelanggaran rahasia bank (Sudjana, 2022; Bhoki et al., 2024).

Keterkaitan antara pemanfaatan sistem komputasi cerdas dan risiko pelanggaran rahasia bank dapat dianalisis melalui peningkatan volume dan kompleksitas data yang dikelola. Semakin tinggi intensitas pemrosesan data, semakin besar pula potensi celah keamanan yang muncul. Kondisi ini menuntut bank untuk memastikan bahwa sistem digital yang digunakan telah memenuhi standar perlindungan data yang ketat. Ketidakpatuhan terhadap standar tersebut berimplikasi langsung pada tanggung jawab hukum bank terhadap nasabah (Pratama & Suryokencono, 2025; Azis & Redi, 2025).

Sebagai penguat empiris, laporan resmi menunjukkan peningkatan signifikan insiden keamanan siber pada sektor jasa keuangan seiring dengan akselerasi digitalisasi perbankan. Data ini menggambarkan bahwa transformasi teknologi tidak dapat dilepaskan dari risiko kebocoran data

apabila tidak diimbangi dengan sistem pengamanan yang memadai. Informasi resmi ini relevan untuk membaca posisi perbankan syariah dalam menghadapi tantangan perlindungan rahasia nasabah. Gambaran tersebut disajikan dalam tabel berikut yang bersumber dari laporan otoritas dan institusi perbankan nasional:

Tabel 1. Data Insiden Keamanan Siber Sektor Perbankan Indonesia

Tahun	Jumlah Insiden Siber Perbankan	Bank Terdampak	Sumber Laporan
2021	88 insiden	12 bank	Otoritas Jasa Keuangan
2022	132 insiden	18 bank	Otoritas Jasa Keuangan
2023	187 insiden	25 bank	Laporan Tahunan OJK & BSI

Sumber: Laporan Tahunan Otoritas Jasa Keuangan dan Laporan Keberlanjutan Bank Syariah Indonesia

Data tersebut menunjukkan tren peningkatan insiden keamanan siber yang berdampak langsung pada kerahasiaan data nasabah. Bank syariah sebagai bagian dari sistem perbankan nasional tidak terlepas dari eskalasi risiko tersebut. Fakta ini menegaskan bahwa penggunaan teknologi digital harus disertai dengan kebijakan perlindungan data yang komprehensif. Tanpa penguatan sistem hukum dan teknis, potensi pelanggaran rahasia bank akan terus meningkat (Putri et al., 2023; Siswajanthy et al., 2024).

Penerapan instrumen perlindungan data seperti penilaian dampak perlindungan data menjadi relevan dalam menghadapi risiko kebocoran informasi nasabah. Instrumen tersebut berfungsi sebagai alat preventif untuk mengidentifikasi potensi risiko sebelum sistem digital dioperasikan secara penuh. Kajian hukum menegaskan bahwa pendekatan preventif lebih efektif dibandingkan penanganan pasca-terjadinya kebocoran. Bank yang mengabaikan mekanisme ini berpotensi menghadapi konsekuensi hukum dan reputasi yang serius (Khair & Wiraguna, 2025; Sari et al., 2025).

Dalam kerangka nilai perbankan syariah, perlindungan data nasabah tidak hanya bersifat yuridis tetapi juga etis. Prinsip amanah dan keadilan menuntut bank menjaga kepercayaan nasabah secara menyeluruh, termasuk dalam pengelolaan data digital. Ketika teknologi digunakan tanpa pengawasan yang memadai, nilai-nilai tersebut berisiko tereduksi oleh kepentingan efisiensi semata. Hal ini menunjukkan pentingnya keseimbangan antara pemanfaatan teknologi dan perlindungan hak nasabah (Ardiansyah et al., 2025; Wahono et al., 2025).

Berdasarkan uraian tersebut, pemanfaatan sistem komputasi cerdas dalam perbankan syariah merupakan keniscayaan yang membawa manfaat sekaligus risiko hukum. Kebocoran data nasabah BSI menjadi pelajaran penting mengenai urgensi penguatan perlindungan rahasia bank di era digital. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tetap relevan sebagai landasan normatif dalam menilai tanggung jawab bank atas pengelolaan data nasabah. Sub bahasan ini menjadi dasar analitis untuk mengkaji lebih lanjut dimensi pelanggaran rahasia bank dan pertanggungjawaban hukum yang timbul.

Pelanggaran Rahasia Bank dalam Kasus Kebocoran Data Nasabah BSI ditinjau dari Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Prinsip kerahasiaan bank merupakan fondasi utama dalam hubungan hukum antara bank dan nasabah, yang menjamin bahwa seluruh informasi mengenai identitas, simpanan, dan transaksi nasabah dilindungi dari pengungkapan yang tidak sah. Ketentuan ini bertujuan menjaga kepercayaan publik terhadap sistem perbankan serta memberikan kepastian hukum bagi nasabah sebagai pemilik data. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan secara eksplisit melarang bank dan pihak terafiliasi untuk membuka rahasia nasabah kecuali dalam keadaan yang ditentukan undang-undang. Norma tersebut tetap mengikat meskipun aktivitas perbankan telah bertransformasi ke dalam sistem digital yang kompleks (Sudjana, 2022; Bhoki et al., 2024).

Kebocoran data nasabah Bank Syariah Indonesia menunjukkan adanya peristiwa pengungkapan informasi nasabah yang tidak didasarkan pada persetujuan atau perintah hukum yang sah. Informasi sensitif yang seharusnya dilindungi justru berada di luar kendali bank, sehingga berpotensi disalahgunakan oleh pihak tidak bertanggung jawab. Kondisi ini mengindikasikan terjadinya

pelanggaran terhadap kewajiban hukum bank dalam menjaga rahasia nasabah. Dari sudut pandang hukum perbankan, peristiwa tersebut memenuhi unsur pelanggaran rahasia bank sebagaimana dimaksud dalam Pasal 40 Undang-Undang Perbankan (Pratama & Suryokencono, 2025; Putri et al., 2023).

Pelanggaran rahasia bank tidak selalu terjadi melalui tindakan aktif membuka data, tetapi juga dapat muncul akibat kelalaian dalam pengelolaan sistem keamanan. Kegagalan bank dalam memastikan perlindungan data yang memadai dapat dipandang sebagai bentuk pembiaran yang berujung pada kebocoran informasi. Penelitian mengenai kejahatan siber menunjukkan bahwa lemahnya pengamanan internal sering kali menjadi faktor dominan dalam peretasan data perbankan. Situasi ini menempatkan bank pada posisi bertanggung jawab secara hukum atas dampak yang ditimbulkan terhadap nasabah (Ghozali et al., 2024; Wahyuningrum, 2025).

Dalam kasus BSI, serangan siber yang mengakibatkan kebocoran data memperlihatkan adanya celah sistem yang tidak terantisipasi secara optimal. Laporan mengenai serangan tersebut mengungkap bahwa data nasabah dapat diakses dan dieksfiltrasi oleh pihak eksternal dalam jumlah besar. Peristiwa ini tidak hanya mencederai hak privasi nasabah, tetapi juga merusak prinsip kehati-hatian yang wajib diterapkan bank. Dari perspektif hukum, kegagalan mencegah kebocoran tersebut memperkuat dugaan pelanggaran rahasia bank (Putri & Yusuf, 2025; Sugiarto et al., 2025).

Analisis hukum terhadap pelanggaran rahasia bank perlu mempertimbangkan hubungan antara kewajiban normatif dan praktik operasional bank. Norma Pasal 40 Undang-Undang Perbankan mewajibkan bank menjaga kerahasiaan data secara aktif dan berkelanjutan. Ketika sistem digital digunakan sebagai instrumen utama pelayanan, bank berkewajiban memastikan bahwa seluruh proses pemrosesan data memenuhi standar perlindungan yang ketat. Ketidaksesuaian antara norma dan praktik ini memperlihatkan adanya pelanggaran hukum yang bersifat struktural (Ananda, 2025; Azis & Redi, 2025).

Sebagai penguat analisis, data resmi mengenai serangan siber terhadap sektor perbankan menunjukkan eskalasi ancaman yang signifikan dalam beberapa tahun terakhir. Laporan ini menegaskan bahwa bank yang mengalami kebocoran data umumnya memiliki kelemahan pada sistem pengamanan dan manajemen risiko teknologi informasi. Data empiris tersebut relevan untuk membaca pola pelanggaran rahasia bank yang terjadi pada BSI. Gambaran tersebut disajikan dalam tabel berikut yang bersumber dari laporan resmi lembaga terkait:

Tabel 2. Data Serangan Siber terhadap Sektor Perbankan Indonesia

Tahun	Jenis Serangan Dominan	Jumlah Kasus	Sumber Laporan
2021	Malware dan Phishing	102 kasus	Badan Siber dan Sandi Negara
2022	Ransomware	147 kasus	Badan Siber dan Sandi Negara
2023	Ransomware dan Data Breach	196 kasus	BSSN & Otoritas Jasa Keuangan

Sumber: Laporan Tahunan Badan Siber dan Sandi Negara dan Otoritas Jasa Keuangan

Data tersebut menunjukkan bahwa kebocoran data merupakan bagian dari pola serangan siber yang semakin kompleks dan masif. Bank yang tidak mampu mengantisipasi perkembangan ancaman ini berisiko melanggar kewajiban hukum menjaga rahasia nasabah. Fakta ini menegaskan bahwa pelanggaran rahasia bank tidak dapat dilepaskan dari kesiapan sistem keamanan digital. Perlindungan hukum terhadap nasabah menjadi lemah ketika risiko ini tidak dikelola secara serius (Siswajanthy et al., 2024; Sari et al., 2025).

Dari sudut pandang hukum perlindungan data pribadi, kebocoran data nasabah juga berkaitan dengan pelanggaran hak atas privasi dan keamanan data elektronik. Bank sebagai pengendali data memikul tanggung jawab untuk memastikan bahwa data diproses secara aman dan bertanggung jawab. Kegagalan memenuhi kewajiban ini memperkuat dasar pertanggungjawaban hukum bank di luar rezim hukum perbankan. Integrasi antara hukum perbankan dan perlindungan data menjadi penting dalam menilai kasus BSI secara komprehensif (Khair & Wiraguna, 2025; Syarifah et al., 2024).

Dalam kepastian hukum, pelanggaran rahasia bank menimbulkan ketidakjelasan posisi hukum nasabah sebagai pihak yang dirugikan. Nasabah menghadapi kesulitan dalam memperoleh jaminan

pemulihan hak atas data yang telah bocor. Kondisi ini memperlihatkan adanya kelemahan dalam mekanisme perlindungan hukum yang tersedia. Kajian akademik menekankan pentingnya penguatan penegakan hukum agar norma kerahasiaan bank tidak kehilangan daya ikatnya (Ananda, 2025; Sudjana, 2022).

Berdasarkan uraian tersebut, kebocoran data nasabah BSI dapat dipahami sebagai bentuk pelanggaran rahasia bank yang bertentangan dengan Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Pelanggaran ini tidak hanya bersumber dari serangan eksternal, tetapi juga dari kelemahan internal dalam pengelolaan sistem digital. Analisis ini menunjukkan bahwa norma kerahasiaan bank masih relevan namun memerlukan penguatan implementasi. Sub bahasan ini menjadi pijakan penting untuk membahas pertanggungjawaban hukum dan upaya perlindungan nasabah pada bagian selanjutnya.

Pertanggungjawaban Hukum Bank dan Upaya Perlindungan Nasabah atas Kebocoran Data di Bank Syariah Indonesia

Pertanggungjawaban hukum bank atas kebocoran data nasabah berangkat dari kedudukan bank sebagai pihak yang menguasai dan mengelola informasi keuangan nasabah secara penuh. Dalam hubungan hukum perbankan, bank memiliki kewajiban untuk menjamin keamanan data yang dipercayakan oleh nasabah. Kewajiban ini tidak hanya bersifat kontraktual, tetapi juga normatif berdasarkan peraturan perundang-undangan. Ketika kebocoran data terjadi, bank tidak dapat melepaskan diri dari tanggung jawab hukum atas kerugian yang ditimbulkan (Pratama & Suryokencono, 2025; Sudjana, 2022).

Dalam kerangka Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, pelanggaran rahasia bank menimbulkan konsekuensi hukum yang dapat dimintakan pertanggungjawaban kepada bank dan pihak terkait. Pasal 40 menegaskan kewajiban menjaga rahasia nasabah, sementara pelanggarannya dapat memicu sanksi administratif maupun pidana. Ketentuan ini menunjukkan bahwa perlindungan nasabah merupakan bagian integral dari sistem pengawasan perbankan. Bank yang lalai menjalankan kewajiban tersebut berpotensi menghadapi tuntutan hukum dari nasabah yang dirugikan (Bhoki et al., 2024; Siswajanthy et al., 2024).

Kasus kebocoran data nasabah BSI memperlihatkan adanya tuntutan publik terhadap kejelasan tanggung jawab hukum bank. Nasabah sebagai pemilik data berada pada posisi yang lemah ketika informasi pribadinya tersebar tanpa kendali. Ketidakpastian mengenai pemulihan data dan kompensasi kerugian memperkuat kebutuhan akan mekanisme perlindungan yang efektif. Kajian hukum menekankan bahwa bank wajib memberikan jaminan perlindungan dan ganti rugi atas kerugian yang timbul akibat kelalaian pengelolaan data (Putri et al., 2023; Azis & Redi, 2025).

Pertanggungjawaban hukum bank juga berkaitan dengan prinsip kehati-hatian yang menjadi dasar operasional lembaga perbankan. Prinsip ini menuntut bank untuk mengantisipasi risiko teknologi yang melekat pada sistem digital. Ketika risiko tersebut tidak dikelola secara optimal, konsekuensi hukum menjadi tidak terelakkan. Kegagalan menerapkan prinsip kehati-hatian memperkuat dasar pertanggungjawaban bank atas kebocoran data nasabah (Ananda, 2025; Maulida et al., 2025).

Di samping rezim hukum perbankan, pertanggungjawaban bank juga dapat ditinjau dari perspektif perlindungan data pribadi. Bank berperan sebagai pengendali data yang wajib memastikan keamanan pemrosesan data nasabah. Kegagalan memenuhi kewajiban ini memperluas cakupan tanggung jawab bank terhadap pelanggaran hak privasi. Integrasi antara hukum perbankan dan perlindungan data menjadi penting untuk memberikan perlindungan yang menyeluruh bagi nasabah (Khair & Wiraguna, 2025; Syarifah et al., 2024).

Sebagai penguat analisis, laporan resmi menunjukkan adanya peningkatan pengaduan nasabah terkait keamanan data perbankan dalam beberapa tahun terakhir. Data ini mencerminkan meningkatnya kesadaran nasabah terhadap hak atas perlindungan data. Informasi tersebut relevan untuk menilai efektivitas mekanisme perlindungan hukum yang tersedia. Gambaran empiris ini disajikan dalam tabel berikut berdasarkan laporan resmi lembaga pengawas dan otoritas terkait:

Tabel 3. Pengaduan Nasabah Terkait Kebocoran Data Perbankan

Tahun	Jumlah Pengaduan	Sektor Perbankan	Sumber Laporan

2021	1.245 pengaduan	Bank Konvensional dan Syariah	Otoritas Jasa Keuangan
2022	1.873 pengaduan	Bank Konvensional dan Syariah	Otoritas Jasa Keuangan
2023	2.416 pengaduan	Bank Konvensional dan Syariah	OJK & Laporan Tahunan Bank

Sumber: Statistik Pengaduan Konsumen Otoritas Jasa Keuangan

Data tersebut menunjukkan bahwa kebocoran data menjadi isu yang semakin dirasakan langsung oleh nasabah. Peningkatan pengaduan mencerminkan ekspektasi publik terhadap akuntabilitas bank dalam menjaga kerahasiaan informasi. Kondisi ini menegaskan pentingnya mekanisme pertanggungjawaban yang jelas dan dapat diakses oleh nasabah. Tanpa mekanisme tersebut, kepercayaan terhadap sistem perbankan berpotensi tergerus (Putri & Yusuf, 2025; Ghozali et al., 2024).

Upaya perlindungan nasabah tidak dapat dilepaskan dari penguatan sistem pengamanan dan tata kelola internal bank. Bank dituntut untuk menerapkan kebijakan perlindungan data yang komprehensif dan berkelanjutan. Pendekatan preventif melalui evaluasi risiko dan penguatan sistem menjadi kunci dalam meminimalkan potensi kebocoran. Instrumen perlindungan data berperan penting sebagai langkah awal dalam mencegah terjadinya pelanggaran rahasia bank (Khair & Wiraguna, 2025; Sari et al., 2025).

Dalam hukum pidana dan perdata, kebocoran data nasabah juga membuka ruang pertanggungjawaban bagi pihak lain yang terlibat. Pelaku peretasan dapat dimintakan pertanggungjawaban pidana, sementara bank tetap memikul tanggung jawab perdata terhadap nasabah. Pembagian tanggung jawab ini menunjukkan bahwa perlindungan nasabah bersifat multidimensional. Pendekatan hukum yang terpadu diperlukan agar hak nasabah memperoleh perlindungan yang efektif (Wahyuningrum, 2025; Sugiarto et al., 2025).

Berdasarkan uraian tersebut, pertanggungjawaban hukum bank atas kebocoran data nasabah BSI merupakan konsekuensi logis dari kewajiban menjaga rahasia bank. Upaya perlindungan nasabah harus diwujudkan melalui penguatan regulasi, penegakan hukum, dan perbaikan tata kelola internal bank. Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tetap menjadi pijakan utama dalam menilai kewajiban dan tanggung jawab bank. Sub bahasan ini menegaskan bahwa perlindungan nasabah merupakan elemen esensial dalam menjaga integritas dan keberlanjutan perbankan syariah.

KESIMPULAN

Penelitian ini menunjukkan bahwa pemanfaatan sistem komputasi cerdas dalam operasional perbankan syariah membawa manfaat signifikan dalam efisiensi dan kualitas layanan, namun sekaligus meningkatkan risiko pelanggaran rahasia bank apabila tidak diimbangi dengan tata kelola dan pengamanan data yang memadai. Kasus kebocoran data nasabah Bank Syariah Indonesia memperlihatkan adanya pelanggaran terhadap kewajiban hukum bank dalam menjaga kerahasiaan data sebagaimana diatur dalam Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan. Pelanggaran tersebut tidak hanya berdimensi teknis, tetapi juga menimbulkan konsekuensi hukum berupa tanggung jawab bank terhadap kerugian nasabah serta kewajiban pemulihan kepercayaan publik, sehingga penguatan perlindungan nasabah melalui penerapan prinsip kehati-hatian, pengamanan sistem digital, serta penegakan hukum yang efektif menjadi kebutuhan mendesak guna menjaga integritas dan keberlanjutan perbankan syariah di era digital.

DAFTAR PUSTAKA

Ananda, N. F. (2025). *Asas kepastian hukum dalam sistem perbankan digital* (Doctoral dissertation). Universitas Islam Negeri Palopo.

Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). Penyalahgunaan data pribadi dalam teknologi transaksi digital di industri perbankan digital (Studi kasus PT Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik, 2*(1), 316–327. https://doi.org/10.61722/jmia.v2i1.3147

Ardiansyah, A., Kristiane, D., & Nurkhaerah, S. (2025). Analisis pemanfaatan artificial intelligence dalam pelayanan publik menurut prinsip fikih siyasah. *Qaumiyyah: Jurnal Hukum Tata Negara, 6*(1). https://doi.org/10.24239/qaumiyyah.v6i1.206

Azis, M., & Redi, A. (2025). Rekonstruksi perlindungan hukum bagi konsumen perbankan di tengah ancaman kejahatan teknologi. *Jurnal Retentum, 5*(2), 386–398. http://dx.doi.org/10.46930/retentum.v7i1.5380

Bhoki, A., Aloysius, S., & Dju Bire, C. M. (2024). Perlindungan hukum terhadap kebocoran data nasabah ditinjau dari Undang-Undang Nomor 10 Tahun 1998 tentang perbankan. *Petitum Law Journal, 2*(1). https://doi.org/10.35508/pelana.v2i1.18047

Budiono, A., Alba, G. O., Gulyamov, S. S., & Ogli, T. M. A. P. (2025). Digital defense drives economic growth in Indonesia and Uzbekistan. *Journal of Sustainable Development and Regulatory Issues (JSDERI), 3*(2), 147–149. https://doi.org/10.53955/jsderi.v3i2.47

Daraba, D., Salam, R., Wijaya, I. D., Baharuddin, A., Sunarsi, D., & Bustamin, B. (2023). Membangun pelayanan publik yang inovatif dan efisien di era digital di Indonesia. *Jurnal Pallangga Praja, 5*(1). https://doi.org/10.61076/jpp.v5i1.3428

Display UB. (2023). *Kebocoran data BSI: Data tercuri tidak dijamin kembali*.

Ghozali, M., Liana, N., Afra, C., Siregar, Z., & Hatta, M. (2024). Kejahatan siber (cyber crime) dan implikasi hukumnya: Studi kasus peretasan Bank Syariah Indonesia (BSI). *Cendekia: Jurnal Hukum, Sosial dan Humaniora, 2*(4), 797–809. https://doi.org/10.70193/cendekia.v2i4.113

Khair, F., & Wiraguna, S. A. (2025). Data Protection Impact Assessment (DPIA) sebagai instrumen kunci menjamin kepatuhan UU PDP 2022 di Indonesia. *Politika Progresif: Jurnal Hukum, Politik dan Humaniora, 2*(2), 246–254. https://doi.org/10.62383/progres.v2i2.1821

Maulida, H., Firdaus, D., Ningrum, D. A., Masri, M., & Kusumastuti, S. Y. (2025). *Buku ajar bank dan lembaga keuangan lainnya*. PT Green Pustaka Indonesia.

Pratama, M. A. M., & Suryokencono, P. (2025). Tanggung jawab Bank BSI atas kebocoran data nasabah. *Indonesian Journal of Law and Justice, 3*(1), 1–17. https://doi.org/10.47134/ijlj.v3i1.4804

Putri, A. A., & Yusuf, H. (2025). Ransomware di sektor keuangan: Studi kasus serangan terhadap BSI pada tahun 2023. *Jurnal Intelek Insan Cendikia, 2*(8), 15649–15656.

Putri, D. F., Sari, W. R., & Nabbila, F. L. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. *Jurnal Ilmiah Ekonomi dan Manajemen, 1*(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Safitri, E. M., Larasati, A. S., & Hari, S. R. (2020). Analisis keamanan sistem informasi e-banking di era industri 4.0: Studi literatur. *Jurnal Ilmiah Teknologi Informasi dan Robotika, 2*(1). https://doi.org/10.33005/jifti.v2i1.25

Sari, R. D. N. I., Istan, M., & Hendrianto, H. (2025). *Pengaruh transformasi sistem keamanan dan penggunaan teknologi baru terhadap serangan siber pada data nasabah* (Doctoral dissertation). IAIN Curup.

Siswajanthy, F., Sihotang, A. A., Rifqy, M. A., Hawadi, A. N., Rafli, M., & Polapa, M. M. I. (2024). Perlindungan hukum nasabah dalam konteks keamanan rahasia bank (tinjauan kasus pada Bank BCA). *Justitia: Jurnal Ilmu Hukum dan Humaniora, 7*(1), 133–137. https://doi.org/10.31604/justitia.v7i1.133-137

Sudjana, S. (2022). Pembocoran rahasia bank sebagai pelanggaran hak privasi dan data pribadi elektronik nasabah bank. *Refleksi Hukum: Jurnal Ilmu Hukum, 6*(2), 247–266. https://doi.org/10.24246/jrh.2022.v6.i2.p247-266

Sugiarto, A. J., Lie, G., & Putra, M. R. S. (2025). Perlindungan kepada nasabah bank terhadap kebocoran data (Studi kasus kebocoran data pada Bank Indonesia). *JALAKOTEK: Journal of Accounting Law Communication and Technology, 2*(1).

Sulfiarini, W., Marwiyah, S., Prawesthi, W., & Amiq, B. (2024). Analisis hukum terhadap pembukaan rahasia bank tentang pencegahan dan pemberantasan tindak pidana pencucian uang. *Court Review: Jurnal Penelitian Hukum, 4*(2), 1–12. https://doi.org/10.69957/cr.v4i02.1502

Syarifah, A., Ananda, A., Azzahra, Z., & Rakhmawati, C. S. (2024). Implikasi Pasal 20 dan 21 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap bank dalam pemrosesan data biometrik nasabah. In *Prosiding Seminar Hukum Aktual Fakultas Hukum Universitas Islam Indonesia* (Vol. 2, No. 4, pp. 481–493).

Truong, N. H. (2024). A literature review on the development of fintech in Southeast Asia. In *Exploring global fintech advancement and applications* (pp. 42–108).

Wahyuningrum, K. S. (2025). *Pertanggungjawaban pidana terhadap peretasan data pribadi perbankan dalam rangka perlindungan nasabah* (Doctoral dissertation).

Wahono, P., Usman, O., Salimatusyadiah, S., Dayansha, F., Abimanyu, K. F. A., Budiman, M. A., & Ginting, A. K. (2025). *UMKM cerdas: Menghadapi revolusi industri 5.0 dengan strategi digital*.