CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

SKANDAL KEBOCORAN DATA NASABAH SEBAGAI CELAH HUKUM DALAM RAHASIA BANK DAN PERLINDUNGAN KONSUMEN

Nafiza Salsabila Faliha[1], Kezia Rona Vinita[2], Agnes Octavia Margaretha Pasaribu[3], Baidhowi[4]
Prodi Ilmu Hukum, Fakultas Hukum, Universitas Negeri Semarang
Email : nafizasf@students.unnes.ac.id

ABSTRAK

Perkembangan teknologi digital dalam sektor perbankan di Indonesia membawa manfaat besar dalam kemudahan layanan keuangan, tetapi juga meningkatkan risiko kebocoran data nasabah. Skandal kebocoran data nasabah perbankan menjadi isu serius yang menyoroti lemahnya perlindungan hukum, terutama dalam penerapan Undang-Undang Perbankan (UU No. 10 Tahun 1998) terkait rahasia bank serta regulasi perlindungan data yang baru, yaitu Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022). Studi ini menyoroti kasus dugaan kebocoran data di sektor perbankan yang diperjualbelikan di forum ilegal, mengakibatkan potensi penyalahgunaan data untuk penipuan, pencucian uang, dan kejahatan siber lainnya. Analisis ini mengeksplorasi tumpang tindih regulasi antara rahasia bank dan perlindungan data pribadi, serta menilai efektivitas Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) dalam mengawasi keamanan data perbankan. Meskipun UU PDP memberikan kerangka perlindungan data, masih terdapat celah dalam implementasi dan penegakan hukumnya, terutama terkait sanksi bagi bank yang gagal menjaga keamanan data. Artikel ini merekomendasikan peningkatan standar keamanan siber, pengetatan regulasi perbankan digital, serta optimalisasi peran OJK dan BI dalam pengawasan dan penegakan hukum. Dengan demikian, diharapkan terjadi sinergi antara regulasi perbankan dan perlindungan data guna meningkatkan keamanan dan kepercayaan publik terhadap sistem perbankan digital di Indonesia.

Kata Kunci: Kebocoran Data, Rahasia Bank, PerlindunganData Pribadi

ABSTRACT

The advancement of digital technology in Indonesia's banking sector has significantly improved financial services but has also increased the risk of customer data breaches. Recent data leak scandals in banking highlight weaknesses in legal protection, particularly in the enforcement of Banking Law (Law No. 10 of 1998) regarding bank secrecy and the newly enacted Personal Data Protection Law (Law No. 27 of 2022). This study examines alleged cases of leaked banking data being sold on illegal forums, leading to

Article History
Received: April 2025
Reviewed: April 2025
Published: April 2025

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/CAUSA.v1i2.365

Publish by : CAUSA

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

potential misuse for fraud, money laundering, and cybercrime. The analysis explores the regulatory overlap between bank secrecy and personal data protection while assessing the effectiveness of the Financial Services Authority (OJK) and Bank Indonesia (BI) in monitoring banking data security. Although the Personal Data Protection Law provides a legal framework, gaps remain in its implementation and enforcement, particularly concerning sanctions against banks that fail to secure customer data. This article recommends enhancing cybersecurity standards, tightening digital banking regulations, and optimizing the roles of OJK and BI in regulatory oversight and law enforcement. Strengthening the synergy between banking regulations and data protection laws is crucial to improving cybersecurity and maintaining public trust in Indonesia's digital banking system.
Keywords: Data Breach, Bank Secrecy, Personal Data Protection

PENDAHULUAN

Perkembangan teknologi digital telah membawa transformasi besar dalam sektor perbankan di Indonesia. Inovasi layanan keuangan berbasis digital, seperti *mobile banking* dan dompet digital memberikan kemudahan akses bagi nasabah serta meningkatkan efisiensi terhadap transaksi keuangan.(Sitanggang *et al.*, 2024) Namun, kemajuan ini juga membawa tantangan yang serius, terutama terkait keamanan data nasabah. Kebocoran dalam data perbankan menjadi ancaman yang semakin nyata dan seiring dengan meningkatnya serangan siber dan perdagangan data ilegal di forum gelap.

Keamanan data nasabah merupakan aspek krusial dalam menjaga kepercayaan publik terhadap sistem perbankan. Undang- Undang Nomor 10 Tahun 1998 tentang Perubahan Atas Undang- Undang Nomor 7 Tahun 1992 Tentang Perbankan telah mengatur mengenai rahasia bank, namun regulasi ini dinilai belum sepenuhnya mampu mengatasi tantangan di era digital.(Yetno, 2024) Sebagai respons terhadap meningkatnya ancaman kebocoran data, pemerintah mengesahkan Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi yang bertujuan memberikan kerangka hukum lebih kuat dalam perlindungan informasi pribadi. Meski demikian, masih terdapat juga celah dalam implementasi dan penegakan hukum yang perlu mendapatkan perhatian lebih lanjut. Dalam beberapa tahun terakhir, berbagai kasus dugaan kebocoran data nasabah perbankan yang diperjualbelikan di forum ilegal semakin mengkhawatirkan. Kebocoran ini tidak hanya mengancam keamanan individu, tetapi juga dapat digunakan untuk berbagai kejahatan, seperti penipuan, pencurian identitas, pencucian uang, dan kejahatan siber lainnya. Kejadian ini menyoroti lemahnya sistem keamanan data di sektor perbankan serta perlunya penguatan regulasi dan pengawasan yang lebih efektif.

Sebagai regulator, Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) memiliki peran penting dalam memastikan keamanan sistem perbankan digital di Indonesia. Namun, efektivitas pengawasan dan penegakan sanksi terhadap pelanggaran perlindungan data masih menjadi tantangan yang harus diatasi. Oleh karena itu, diperlukan sinergi antara regulasi perbankan dan perlindungan data pribadi agar mampu meningkatkan keamanan serta kepercayaan publik terhadap layanan keuangan digital.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Artikel ini akan membahas lebih lanjut mengenai tumpang tindih regulasi antara rahasia bank dan perlindungan data pribadi, efektivitas peran OJK dan BI dalam pengawasan keamanan data perbankan, serta memberikan rekomendasi untuk meningkatkan standar keamanan siber dan penegakan regulasi guna melindungi data nasabah. Dengan penguatan regulasi dan pengawasan yang lebih ketat, diharapkan sektor perbankan digital di Indonesia dapat berkembang secara aman dan berkelanjutan.

.

LANDASAN TEORI

Dalam kajian hukum pidana, keabsahan bukti digital merupakan isu yang relatif baru dan terus berkembang seiring dengan kemajuan teknologi informasi. Bukti digital, sebagai salah satu bentuk alat bukti elektronik, memerlukan pengakuan hukum yang jelas agar dapat diterima dalam proses peradilan pidana, baik dari segi autentikasi, integritas, maupun prosedur pengumpulannya.(Harahap *et al.*, 2024) Beberapa penelitian terdahulu lebih banyak menekankan pada pengakuan formil terhadap bukti digital dalam hukum positif Indonesia, tanpa memberikan perbandingan mendalam dengan standar internasional seperti yang diatur dalam *Federal Rules of Evidence* (FRE) di Amerika Serikat. Oleh karena itu, artikel ini menghadirkan pendekatan yang lebih inovatif melalui analisis perbandingan antara sistem hukum Indonesia dan Amerika Serikat serta mengaitkannya dengan studi kasus penting *Riley v. California*, guna menunjukkan urgensi pembaruan regulasi dan peningkatan kapasitas forensik digital di Indonesia. Dengan pendekatan ini, tulisan ini tidak hanya memperkuat tinjauan normatif terhadap bukti digital, tetapi juga menawarkan kontribusi baru dalam pengembangan praktik hukum pidana yang lebih adaptif terhadap tantangan era digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan yuridis-normatif, yaitu dengan menelaah peraturan perundang-undangan yang berkaitan dengan perlindungan data nasabah dalam perbankan serta membandingkannya dengan praktik yang terjadi di lapangan.(Rosidi, Zainuddin dan Arifiana, 2024) Pendekatan ini dilakukan untuk menganalisis kesesuaian antara Undang-Undang No. 10 Tahun 1998 tentang Perbankan dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam konteks kebocoran data nasabah perbankan di Indonesia. Sumber data yang digunakan adalah data sekunder, yang meliputi peraturan perundang-undangan, jurnal hukum, laporan dari OJK dan BI, serta studi kasus kebocoran data perbankan yang telah dipublikasikan.(Hidayat, 2021) Teknik pengumpulan data dilakukan melalui studi kepustakaan, dengan menelusuri berbagai dokumen hukum, artikel akademik, serta laporan resmi terkait keamanan data dalam sektor perbankan.(Bandaso, Randa dan Mongan, 2022) Data yang diperoleh kemudian dianalisis menggunakan metode deskriptif-analitis, yaitu dengan mendeskripsikan fakta hukum yang ada, menghubungkannya dengan teori hukum yang relevan, serta mengevaluasi efektivitas regulasi dalam menangani kebocoran data nasabah.(Syahputra, 2024) Dengan pendekatan ini, penelitian ini bertujuan untuk memberikan pemahaman yang lebih dalam mengenai celah regulasi dalam perlindungan data nasabah serta memberikan rekomendasi kebijakan untuk memperkuat sistem hukum perbankan di Indonesia.

HASIL DAN PEMBAHASAN

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

1. Kebocoran Data Nasabah di Sektor Perbankan: Realitas dan Dampaknya

Perbankan digital semakin populer karena memberikan kemudahan dan efisien waktu bagi penggunanya. Namun, peningkatan adopsi layanan ini menimbulkan tantangan besar dalam hal perlindungan nasabah. Berbagai ancaman keamanan seperti pencurian identitas, penipuan, gangguan transaksi serangan malware yang dapat merusak sistem, serta kebocoran data pribadi menggarisbawahi pentingnya analisis mendalam terhadap sistem perlindungan di Bank Syariah Indonesia (BSI). Digitalisasi di sektor keuangan telah meningkatkan potensi serangan siber hingga 86,70%. Menurut IMF, sektor jasa keuangan global mengalami kerugian rata-rata tahunan akibat serangan siber sebesar USD 100 miliar, setara dengan lebih dari Rp1.433 triliun. Di Asia Tenggara, Indonesia menempati posisi kelima dalam hal keamanan siber. Dengan kondisi tersebut, sangat penting bagi institusi keuangan untuk memperkuat mekanisme perlindungan nasabah guna mengurangi risiko yang timbul dari penggunaan teknologi digital dalam transaksi. BSI sendiri menawarkan layanan perbankan digital yang memungkinkan nasabah mengakses berbagai layanan melalui perangkat seperti *smartphone*, tablet, atau komputer. Secara umum, risiko yang dihadapi nasabah meliputi serangan siber, *phishing*, *malware*, dan serangan *denial of service* (DoS).(Simatangkir, Afifah dan Faliha, 2025) Risiko ini mencakup upaya oleh pihak tidak bertanggung jawab untuk mengakses, merusak, atau mencuri data penting dari sistem perbankan digital. Dengan semakin intensifnya penggunaan teknologi dalam perbankan, penerapan langkah-langkah keamanan yang efektif menjadi sangat krusial untuk melindungi nasabah dari potensi ancaman tersebut.(Kusuma dan Rahmani, 2022)

Pada tanggal 8 Mei 2023, Bank Syariah Indonesia (BSI) mengalami gangguan signifikan pada layanan digital yang berlangsung selama beberapa hari. Gangguan tersebut tidak hanya disebabkan oleh perawatan sistem yang telah dijadwalkan, melainkan juga terdapat indikasi adanya upaya peretasan. Akibatnya, nasabah menghadapi berbagai kendala, seperti ketidakmampuan melakukan transaksi melalui BSI *Mobile*, kesulitan dalam mengakses ATM, dan hambatan dalam pelayanan *teller*.(Antoine *et al.*, 2025) Pada tanggal 16 Mei 2023, BSI mengeluarkan klarifikasi yang menegaskan bahwa meskipun terjadi gangguan, keamanan data dan dana nasabah tetap terjaga. Menanggapi insiden ini, OJK menginstruksikan BSI untuk segera mengembalikan semua layanan ke kondisi normal, serta mengimbau seluruh institusi keuangan di sektor perbankan untuk meningkatkan kapabilitas ketahanan digital mereka.

Seiring dengan pesatnya perkembangan era digital, isu kebocoran data telah muncul sebagai tantangan kritis bagi berbagai sektor, terutama industri perbankan. Meskipun kebocoran data pribadi bukanlah fenomena baru, masalah ini tetap memerlukan perhatian serius karena dapat menimbulkan konsekuensi yang sangat merugikan. Ketika data sensitif nasabah seperti nomor rekening, detail kartu kredit, informasi identitas personal, dan catatan keuangan terekspos, dampaknya bisa sangat merusak. Kebocoran semacam ini dapat terjadi melalui serangan siber yang terstruktur, pelanggaran protokol keamanan oleh pihak internal, maupun ketidakcermatan dalam pengelolaan data. Selain risiko langsung seperti pencurian identitas, penipuan, dan penyalahgunaan keuangan, insiden kebocoran data juga berpotensi mengikis kepercayaan nasabah dan merusak reputasi institusi perbankan secara substansial.

Secara fundamental, perlindungan hukum merupakan realisasi dari pemenuhan hak-hak yang seharusnya dinikmati konsumen. Tanggung jawab untuk melindungi konsumen

tidak hanya dibebankan pada pemerintah, melainkan juga menjadi kewajiban bagi para pelaku usaha, termasuk institusi perbankan seperti PT. Bank Syariah Indonesia. Lingkup perlindungan konsumen mencakup berbagai ranah hukum secara menyeluruh mulai dari hukum perdata, hukum administrasi, hingga hukum pidana. Perlindungan ini tidak hanya terbatas pada kompensasi atau penjatuhan sanksi terhadap pihak yang melanggar, melainkan juga mencakup berbagai upaya untuk memastikan hak-hak konsumen terpenuhi.

Bank Syariah Indonesia (BSI) telah menerapkan berbagai langkah pengamanan untuk melindungi kepentingan nasabahnya. Dalam menghadapi ancaman seperti *ransomware*, lembaga yang menjadi target serangan harus bekerja sama dengan aparat penegak hukum, lembaga penanggulangan darurat siber, serta perusahaan yang bergerak di bidang keamanan siber. BSI telah mengimplementasikan berbagai teknologi pengamanan, antara lain sistem enkripsi data, verifikasi dua tahap, serta sistem keamanan tambahan lainnya. Menangani gangguan layanan dan potensi kebocoran data yang pernah terjadi, BSI telah menganggarkan dana sebesar Rp 580 miliar yang difokuskan untuk memperkuat digitalisasi dan keamanan data nasabah. Langkah ini meliputi peningkatan sistem proteksi dan ketahanan teknologi informasi guna mengantisipasi berbagai ancaman.(Haryanto dan Sutra, 2023) Selain itu, BSI juga menjalin koordinasi dengan lembaga terkait seperti Badan Siber dan Sandi Negara (BSSN), OJK, dan BI guna memastikan sistem pengamanan yang lebih optimal.

Transformasi digital dalam sektor perbankan telah meningkatkan paparan bank terhadap risiko keamanan siber. Dengan bertambahnya frekuensi serangan siber, ada kebutuhan mendesak untuk meningkatkan ketahanan siber melalui penguatan keamanan siber. Inisiatif pengamanan ini telah diluncurkan di berbagai industri, terutama perbankan, dimana regulator di banyak negara berupaya mengatasi risiko siber. Bank Syariah Indonesia, bersama dengan institusi perbankan lain di Indonesia, harus memprioritaskan peningkatan sistem pertahanan digitalnya, mengingat sektor keuangan merupakan target utama serangan siber, baik secara global maupun nasional.

Berbagai langkah strategis perlu diimplementasikan, seperti pengembangan kebijakan pengelolaan keamanan siber, penerapan sistem penilaian risiko siber, pelaksanaan uji kerentanan teknologi informasi, evaluasi tingkat kematangan siber, dan pengujian keamanan yang mengikuti praktik terbaik internasional. Meskipun sudah ada peningkatan keamanan melalui *firewall*, enkripsi data, dan monitoring aktif untuk mencegah serangan siber, tidak ada sistem yang mampu menjamin perlindungan total terhadap ancaman seperti *ransomware*. Oleh karena itu, sangat penting untuk menerapkan strategi mitigasi yang tepat serta melakukan persiapan yang matang. Bank Syariah Indonesia hendaknya mengadopsi praktik terbaik yang telah terbukti efektif di berbagai negara untuk mengurangi potensi ancaman dan kerentanan siber yang dapat mengancam keamanan sistem digital mereka.

Berdasarkan Undang-Undang Perlindungan Konsumen (UUPK), PT. Bank Syariah Indonesia diwajibkan untuk bertanggung jawab secara mutlak atas kebocoran data nasabah, artinya bank harus memberikan kompensasi tanpa terlebih dahulu membuktikan adanya kesalahan dari pihaknya. UUPK mengatur jenis-jenis kompensasi yang mencakup ganti rugi nominal, kompensasi, dan ganti rugi penghukuman untuk perbuatan melawan hukum. Ketentuan ini sejalan dengan Undang-Undang Nomor 21 Tahun 2008 Pasal 47 ayat (1) yang mewajibkan bank syariah menjaga kerahasiaan data dan informasi nasabah. Dalam hal terjadi kebocoran data, bank syariah harus menanggung semua kerugian yang timbul,

Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

kecuali dapat menunjukkan bahwa insiden tersebut terjadi di luar kesalahan mereka. Selanjutnya, Pasal 48 ayat (1) mengharuskan bank syariah memberikan ganti rugi kepada nasabah atas kerugian akibat tindakan melawan hukum yang dilakukan baik oleh bank maupun pegawainya, dengan bentuk ganti rugi yang dapat berupa ganti rugi nominal, kompensasi, dan ganti rugi penghukuman.(Lestari, 2024)

Terkait dengan insiden kebocoran data yang diduga merupakan hasil peretasan pada Bank Syariah Indonesia, prinsip-prinsip hukum yang berlaku mengharuskan BSI untuk menyediakan kompensasi kepada nasabah yang terdampak. Mengingat insiden tersebut telah menimbulkan kerugian, bank berkewajiban memberikan ganti rugi sesuai dengan peraturan yang berlaku, dimana beban pembuktian kerugian dialihkan kepada nasabah yang mengalami kerugian. Seiring dengan pesatnya perkembangan ekonomi digital, perlindungan data nasabah dalam layanan perbankan digital menjadi semakin krusial. Untuk membangun kepercayaan dan memastikan kelangsungan bisnis di era digital, bank syariah harus mengutamakan keamanan data nasabah dengan menerapkan kebijakan dan regulasi yang kuat serta teknologi keamanan terkini guna menjaga kerahasiaan dan integritas data. Dampak hukum dan ekonomi dari kebocoran data tersebut adalah kebocoran data membuka peluang bagi pihak-pihak tidak bertanggung jawab untuk menyalahgunakan informasi pribadi nasabah. Data yang terekspos dapat digunakan untuk melakukan penipuan, pencucian uang, dan berbagai tindak kejahatan finansial lainnya. Hal ini tidak hanya menimbulkan kerugian bagi individu, tetapi juga berpotensi mengganggu stabilitas sistem keuangan. Nasabah yang datanya bocor dapat mengalami kerugian finansial langsung, seperti pencurian dana, serta kerugian tidak langsung berupa biaya pemulihan sistem, kompensasi dari bank, dan denda dari regulator. Kerugian ini juga dapat berdampak pada reputasi bank, yang pada gilirannya mempengaruhi kepercayaan dan loyalitas nasabah. Dampak psikologis bagi nasabah yang terdampak kebocoran data bisa sangat signifikan. Rasa cemas, stres, dan kehilangan kepercayaan terhadap lembaga keuangan merupakan konsekuensi yang muncul akibat pelanggaran privasi dan keamanan data. Hal ini dapat menurunkan kenyamanan serta kepercayaan dalam menggunakan layanan perbankan digital, sehingga berdampak pada kesejahteraan mental nasabah.(Irmawati, Pieries dan Widiarty, 2024) Dengan demikian, kebocoran data tidak hanya membawa konsekuensi hukum dan ekonomi bagi institusi perbankan, tetapi juga memberikan dampak serius terhadap kehidupan finansial dan psikologis nasabah. Langkah-langkah mitigasi yang efektif serta penguatan sistem keamanan siber menjadi kunci untuk mengurangi risiko tersebut.

2. Analisis Regulasi: Bagaimana Hukum Perbankan Mampu Melindungi Data Nasabah

Transformasi digital telah mengubah lanskap industri perbankan secara drastis, sehingga menimbulkan tantangan baru terkait keamanan dan perlindungan data nasabah. Dalam kerangka hukum, UU No. 10 Tahun 1998 tentang Perbankan menetapkan kewajiban bagi setiap bank untuk menjaga kerahasiaan data dan informasi yang diperoleh dari nasabah, yang dikenal dengan istilah "rahasia bank”. Definisi rahasia bank mencakup segala informasi, mulai dari data pribadi, catatan transaksi, hingga detail keuangan yang harus dilindungi dari penyebaran tanpa izin nasabah. Tujuan utamanya adalah untuk menjaga kepercayaan publik terhadap sistem perbankan dan mencegah penyalahgunaan informasi oleh pihak yang tidak berwenang.(Fitrianto, 2020)

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Secara prinsip, UU Perbankan memberikan dasar hukum yang kuat untuk melindungi data nasabah melalui konsep rahasia bank. Pelanggaran terhadap kewajiban menjaga kerahasiaan data ini dapat menimbulkan konsekuensi hukum serius, baik secara perdata maupun administratif. Dalam konteks tersebut, setiap bank diwajibkan untuk menerapkan mekanisme pengamanan agar informasi yang bersifat rahasia tidak disalahgunakan atau tersebar ke pihak luar tanpa sepengetahuan dan persetujuan nasabah.

Namun, meskipun landasan hukum yang ada memberikan perlindungan terhadap data nasabah, UU Perbankan No. 10 Tahun 1998 disusun pada masa di mana ancaman siber belum sekompleks sekarang. Perkembangan teknologi digital telah membuka celah-celah baru yang memungkinkan terjadinya serangan peretasan, *malware*, dan kebocoran data yang dilakukan oleh kelompok kejahatan siber. Risiko yang muncul dari serangan siber ini jauh lebih dinamis dan canggih dibandingkan dengan pelanggaran yang umumnya terjadi pada masa sebelumnya. Dengan demikian, regulasi yang ada seringkali belum mampu mengantisipasi seluruh aspek risiko digital secara komprehensif.

Kritik utama terhadap UU Perbankan dalam menghadapi ancaman digital adalah keterbatasannya dalam mengatur tata kelola dan mekanisme pengamanan data di lingkungan digital. Hal ini memunculkan kebutuhan akan regulasi tambahan yang khusus mengatur perlindungan data pribadi, seperti Undang- Undang Perlindungan Data Pribadi (UU PDP). Peraturan tersebut diharapkan dapat melengkapi UU Perbankan dengan menetapkan standar yang lebih modern dan komprehensif mengenai pengelolaan, penyimpanan, dan proteksi data nasabah dalam era digital.

Di sisi lain, regulator seperti OJK telah mengeluarkan sejumlah peraturan pelaksana (POJK) yang mengatur manajemen risiko siber dan tata kelola teknologi informasi di sektor perbankan. Kebijakan-kebijakan ini merupakan upaya untuk menutup celah-celah yang belum tertangani oleh UU Perbankan lama dan memberikan pedoman operasional yang lebih rinci bagi institusi perbankan dalam menghadapi risiko digital. Meski demikian, pembaruan dan evaluasi regulasi secara berkala tetap diperlukan agar peraturan tersebut selalu relevan dengan perkembangan teknologi dan dinamika ancaman siber.

Secara keseluruhan, meskipun UU Perbankan No. 10 Tahun 1998 memberikan dasar hukum penting dalam hal perlindungan data nasabah melalui konsep rahasia bank, regulasi tersebut belum sepenuhnya memadai untuk menghadapi kompleksitas ancaman digital saat ini. Oleh karena itu, integrasi antara UU Perbankan dengan regulasi perlindungan data modern, serta implementasi kebijakan pengawasan dan manajemen risiko siber yang lebih komprehensif, menjadi kunci untuk menjaga keamanan dan integritas data nasabah. Pembaruan regulasi dan penerapan teknologi keamanan terkini sangat penting untuk membangun kembali kepercayaan publik serta memastikan keberlangsungan dan ketahanan sistem perbankan di era digital. Undang-Undang No. 27 Tahun 2022 tentang UU PDP merupakan salah satu tonggak penting dalam era digital, yang secara tegas memberikan hak-hak atas data pribadi bagi setiap individu, termasuk nasabah perbankan. Dalam konteks ini, nasabah memiliki hak untuk mengakses data yang dikumpulkan oleh bank, memperbaiki informasi yang tidak akurat, menghapus data yang tidak relevan, serta hak untuk menolak atau membatasi pemrosesan data mereka. Hak portabilitas data juga memungkinkan nasabah untuk memindahkan data mereka ke penyedia layanan lain, sehingga memberikan kontrol yang lebih besar atas informasi pribadi. Hak- hak tersebut dirancang untuk

memberikan perlindungan maksimal bagi individu dan memastikan bahwa data yang bersifat sensitif tidak disalahgunakan oleh pihak manapun.(Pranata *et al.*, 2024)

Di sisi lain, UU PDP juga mengharuskan setiap institusi perbankan, termasuk Bank Syariah Indonesia (BSI), untuk menerapkan sistem pengamanan yang ketat guna melindungi data nasabah. Bank diwajibkan untuk memastikan bahwa setiap proses pengumpulan, penyimpanan, dan pengolahan data dilakukan atas dasar persetujuan yang jelas dari nasabah dan dilakukan dengan standar keamanan yang tinggi. Untuk itu, BSI harus mengimplementasikan teknologi pengamanan seperti enkripsi data, sistem otentikasi dua faktor, serta mekanisme monitoring dan audit keamanan secara berkala guna mencegah akses tidak sah maupun serangan siber yang dapat mengakibatkan kebocoran data. Transparansi juga menjadi elemen penting, di mana bank harus menyediakan informasi yang jelas mengenai bagaimana data nasabah dikelola dan dilindungi, serta menyediakan jalur pelaporan apabila terjadi pelanggaran keamanan.

Meskipun UU PDP memberikan dasar hukum yang kuat dengan ancaman sanksi administratif dan bahkan pidana bagi pelanggaran terhadap pengelolaan data pribadi, efektivitasnya dalam menjerat pelanggaran di sektor perbankan sangat bergantung pada implementasi di lapangan. Dinamika dan kompleksitas ancaman siber di era digital menuntut regulasi yang tidak hanya bersifat statis, tetapi juga harus adaptif terhadap perkembangan teknologi dan modus operandi serangan yang semakin canggih. Di sinilah tantangan utama muncul, karena penerapan UU PDP harus didukung oleh mekanisme penegakan hukum yang efektif, termasuk kerja sama yang erat antara regulator, lembaga penegak hukum, dan institusi perbankan itu sendiri. Pengawasan yang konsisten serta evaluasi berkala terhadap sistem pengamanan yang telah diterapkan sangat krusial untuk memastikan bahwa perlindungan terhadap data nasabah selalu mutakhir dan mampu menghadapi ancaman baru.

Dalam praktiknya, kendala juga muncul dari sisi internal bank, seperti keterbatasan sumber daya dalam mengimplementasikan teknologi keamanan terkini dan kurangnya kesadaran mengenai pentingnya tata kelola data yang baik. Hal ini menggarisbawahi perlunya integrasi antara UU PDP dengan regulasi sektoral yang lebih spesifik, misalnya peraturan dari OJK yang mengatur manajemen risiko siber di perbankan. Dengan sinergi antara regulasi nasional dan kebijakan internal bank, diharapkan standar keamanan data dapat terus ditingkatkan sehingga nasabah merasa lebih aman dalam melakukan transaksi digital.

Secara keseluruhan, meskipun UU PDP sudah menyediakan kerangka hukum yang komprehensif untuk perlindungan data pribadi, kekuatan dan efektivitasnya dalam menjerat pelanggaran di sektor perbankan sangat bergantung pada implementasi yang konsisten dan kemampuan regulator untuk menyesuaikan kebijakan dengan perkembangan teknologi digital. Oleh karena itu, pembaruan regulasi, peningkatan infrastruktur keamanan, serta kolaborasi yang erat antara seluruh pemangku kepentingan menjadi kunci utama dalam menjaga integritas dan kerahasiaan data nasabah di era digital.(Maharani dan Prakoso, 2024)

Dalam konteks pengawasan dan penegakan hukum terkait keamanan data di sektor perbankan, OJK dan BI memainkan peran yang sangat krusial dalam menjaga integritas sistem keuangan nasional. Sebagai regulator sektor jasa keuangan, OJK memiliki kewenangan untuk menetapkan dan mengawasi kepatuhan institusi perbankan terhadap

Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

standar dan regulasi yang berkaitan dengan pengelolaan risiko siber dan perlindungan data nasabah. Dalam praktiknya, OJK melakukan audit rutin dan inspeksi menyeluruh untuk memastikan bahwa bank telah mengimplementasikan sistem keamanan informasi yang memadai. Pengawasan ini mencakup evaluasi terhadap mekanisme pengamanan data, seperti penggunaan enkripsi, otentikasi dua faktor, serta sistem monitoring dan respons insiden siber. Apabila ditemukan ketidaksesuaian atau pelanggaran, OJK dapat langsung mengambil tindakan dengan memberikan sanksi administratif, seperti denda atau bahkan pencabutan izin operasional, guna mendorong institusi keuangan untuk segera memperbaiki kelemahan yang ada.

Secara kesseluruhan, BI berfokus pada stabilitas sistem keuangan secara keseluruhan. Dalam konteks perlindungan nasabah, BI memiliki peran strategis untuk menjaga kelancaran sistem pembayaran dan memastikan infrastruktur keuangan tetap stabil meskipun terjadi gangguan atau serangan siber. BI menetapkan standar teknis serta kebijakan operasional yang harus dipenuhi oleh sistem perbankan, sehingga ketika terjadi insiden seperti kebocoran data atau serangan siber, gangguan terhadap likuiditas dan stabilitas sistem keuangan dapat diminimalisir. BI bekerja sama dengan OJK dan lembaga terkait lainnya, seperti BSSN, untuk merumuskan kebijakan yang mengintegrasikan aspek keamanan siber ke dalam manajemen risiko sistemik. Pendekatan ini mencakup evaluasi berkala terhadap kerentanan sistem pembayaran digital, penguatan infrastruktur TI, dan penerapan teknologi canggih yang dapat mendeteksi serta merespons ancaman siber secara real-time.

Sebagai ilustrasi studi kasus, pada insiden kebocoran data yang pernah terjadi di BSI, kedua lembaga ini memainkan peran yang saling melengkapi. Ketika insiden tersebut terjadi, OJK segera menginstruksikan BSI untuk melakukan normalisasi layanan dan melakukan investigasi menyeluruh terhadap penyebab kebocoran data. OJK menekan agar bank segera mengidentifikasi celah keamanan dan mengambil langkah-langkah korektif untuk mencegah insiden serupa di masa depan. Di samping itu, BI mengeluarkan pedoman teknis untuk menguatkan infrastruktur sistem pembayaran digital, memastikan bahwa walaupun terjadi gangguan pada layanan digital, stabilitas keuangan tetap terjaga. BI juga memberikan dukungan berupa pengawasan yang lebih intensif terhadap sistem pembayaran dan likuiditas bank, sehingga jika terjadi serangan siber yang mengakibatkan gangguan operasional, dampaknya terhadap sistem keuangan nasional dapat diisolasi dan diminimalisir.

Sinergi antara OJK dan BI sangat penting karena keduanya memiliki fokus yang berbeda namun saling melengkapi. Sementara OJK lebih mengutamakan aspek perlindungan konsumen dan tata kelola internal bank melalui penetapan regulasi serta pengawasan terhadap kepatuhan institusi, BI memastikan bahwa sistem keuangan nasional tetap stabil dan tahan terhadap guncangan yang mungkin timbul dari serangan siber. Keduanya bekerja sama dalam rangka meningkatkan kesiapan sektor perbankan dalam menghadapi ancaman siber melalui penerapan standar keamanan yang lebih ketat, audit berkala, serta peningkatan kapasitas dalam deteksi dan respons insiden. Upaya bersama ini tidak hanya membantu melindungi data nasabah, tetapi juga menjaga kepercayaan publik dan memastikan keberlangsungan operasional sistem keuangan di era digital yang semakin kompleks.

3. Tantangan Hukum dalam Menangani Kebocoran Data Nasabah

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Dalam menyikapi tantangan hukum terkait kebocoran data nasabah, baik Undang-Undang Perbankan maupun UU PDP memiliki peran penting, namun keduanya memiliki fokus yang berbeda. UU No. 10 Tahun 1998 tentang Perbankan lebih fokus pada regulasi mengenai operasional sektor perbankan, termasuk kewajiban dan tanggung jawab bank terhadap nasabah, serta pengaturan mengenai keamanan data dan informasi yang dimiliki oleh bank. Peraturan ini menetapkan ketentuan yang mengharuskan bank untuk menjaga kerahasiaan data nasabah, termasuk informasi terkait transaksi dan identitas nasabah. Oleh karena itu, ketika kebocoran data nasabah terjadi dalam lingkup bank, UU Perbankan akan berperan dalam mengatur tanggung jawab bank terhadap keamanan data dan sanksi yang dapat dikenakan. Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022) lebih bersifat umum dan komprehensif, mengatur tentang pengelolaan dan perlindungan data pribadi di seluruh sektor, bukan hanya di sektor perbankan. UU PDP memberikan perlindungan terhadap hak privasi setiap individu, mengatur bagaimana data pribadi harus dikumpulkan, disimpan, diproses, dan dilindungi oleh setiap entitas yang mengelola data pribadi, termasuk bank. UU ini memberikan hak kepada individu (nasabah) untuk mengetahui dan mengontrol bagaimana data pribadi mereka digunakan, serta hak untuk mengajukan keluhan jika terjadi kebocoran atau penyalahgunaan data. Namun, pada praktiknya, kedua UU tersebut saling melengkapi dan memberikan perlindungan yang lebih kuat jika diterapkan secara bersama-sama, karena UU PDP memberikan perlindungan yang lebih komprehensif mengenai data pribadi, sedangkan UU Perbankan memastikan keamanan dan integritas data dalam konteks perbankan.

Secara umum nasabah menghadapi berbagai risiko keamanan saat menggunakan layanan perbankan digital seperti risiko keamanan siber, phishing, malware, dan serangan DoS. Risiko keamanan siber mencakup ancaman dari pihak yang tidak bertanggung jawab yang mencoba mengakses, merusak, atau mencuri data dan informasi penting dari sistem perbankan digital. agai sektor, termasuk sektor perbankan. Kebocoran data pribadi sebenarnya bukanlah hal baru, namun merupakan masalah yang sangat serius dan memprihatinkan. Terungkapnya informasi pribadi nasabah seperti nomor rekening, informasi kartu kredit, data identitas, dan detail keuangan dapat memiliki dampak yang merugikan. Kebocoran semacam ini dapat terjadi karena serangan siber, pelanggaran keamanan internal atau kelalaian dalam pengelolaan data. Selain menimbulkan resiko pencurian identitas, penipuan, dan penyalahgunaan finansial, kebocoran data pribadi perbankan juga dapat mengancam kepercayaan nasabah terhadap institusi perbankan dan menyebabkan kerugian reputasi yang signifikan. Perlindungan hukum, pada dasarnya, adalah pemenuhan hak-hak konsumen yang seharusnya diberikan kepada mereka. Kewajiban melindungi konsumen tidak hanya terletak pada pemerintah, melainkan juga menjadi tanggung jawab pelaku usaha, termasuk bank seperti PT. Bank Syariah Indonesia. Perlindungan konsumen melibatkan berbagai aspek hukum, termasuk hukum perdata, administrasi, dan pidana, serta tidak hanya terbatas pada ganti rugi atau sanksi kepada pelaku usaha. Dalam perlindungan terhadap nasabah, ada dua pendekatan, yaitu perlindungan tidak langsung terhadap resiko kerugian yang mungkin timbul dari kebijaksanaan atau kegiatan usaha bank dan perlindungan langsung terhadap resiko kerugian yang muncul dari kegiatan usaha bank.(Iermansyah, Astanti dan Heryanti, 2023)

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol 11 No 7 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Dikaji secara global, beberapa negara memiliki sistem perlindungan data nasabah dalam sektor perbankan yang berbeda, namu dengan prinsip yang mirip yaitu menjaga kerahasiaan dan integritas data nasabah. Beberapa sistem yang patut diperbandingkan, Menurut *The World Bank*, dalam *Global Survey on Consumer Protection and Financial Literacy Oversight Frameworks and Practices in 114 Economies*, terdapat enam dimensi perlindungan konsumen yang mencakup:

a. *Legal Framework*
b. *Institutional Arrangements*
c. *Fair Treatment*
d. *Disclosure requirements & Responsible lending*
e. *Dispute resolution dan recourse*
f. *Financial Literac*

Uni Eropa telah menerapkan *General Data Protection Regulation* (GDPR) sejak 2018, yang merupakan regulasi paling ketat dan komprehensif mengenai perlindungan data pribadi di dunia.(Oktavianes *et al.*, 2025) GDPR mendefinisikan data pribadi sebagai "informasi apa pun yang berkaitan dengan seseorang yang dapat diidentifikasi atau dapat diidentifikasi secara langsung." Istilah "*identifiable*" mengacu pada informasi tertentu yang dapat digunakan untuk mengenali individu tertentu, seperti alamat IP, nomor ponsel, atau data lokasi. GDPR juga membedakan data pribadi yang berkaitan dengan bukti kejahatan. Di sisi lain, dalam Peraturan Pemerintah (PP) PSTE, data pribadi diartikan sebagai data yang terkait dengan individu tertentu yang disimpan, dikelola, dijaga kebenarannya, serta dilindungi kerahasiaannya. Meskipun tidak dijelaskan secara rinci apa yang dimaksud dengan data perseorangan, pasal 58 UU No. 23 Tahun 2006 juncto UU No. 24 Tahun 2013 tentang Administrasi Kependudukan sering dijadikan rujukan untuk definisi tersebut. Uni Eropa juga membentuk, yang terdiri dari perwakilan otoritas pengawasan dari setiap negara anggota Uni Eropa. Setiap negara anggota Uni Eropa memiliki lembaga yang bertugas mengawasi implementasi GDPR. Sebagai negara berdaulat, Indonesia perlu menyikapi keberadaan GDPR sebagai hukum nasional Uni Eropa yang dapat berdampak pada pemrosesan data pribadi di Indonesia, khususnya yang dimiliki oleh warga negara Uni Eropa. Hal ini berkaitan dengan prinsip ekstra-teritorial dari GDPR atau aturan serupa yang berlaku di negara lain. Tujuannya adalah untuk memberikan kepastian hukum dan pemahaman bagi entitas di Indonesia yang memproses data pribadi warga negara asing. Selain itu, individu dan badan hukum (baik publik maupun perusahaan) di Indonesia perlu menyesuaikan peraturan internal mereka dengan GDPR agar tidak dianggap sebagai controller atau processor yang melanggar regulasi tersebut.(Sirait, 2019)

Amerika Serikat (*Gramm-Leach-Bliley Act*) Di Amerika Serikat, regulasi terkait perlindungan data nasabah di sektor perbankan diatur oleh *Gramm-Leach-Bliley Act* (GLBA) yang mengharuskan bank dan lembaga keuangan untuk menjaga kerahasiaan informasi finansial pribadi nasabah. tentang kebijakan privasi mereka, memberi pilihan bagi nasabah untuk membatasi pembagian data mereka, serta mewajibkan lembaga tersebut untuk mengimplementasikan langkah-langkah keamanan guna melindungi informasi dari kebocoran atau penyalahgunaan. Secara keseluruhan, GLBA bertujuan untuk memastikan bahwa data pribadi nasabah terlindungi dengan baik dalam industri keuangan. Hal ini sangat jauh berbeda dengan sanksi administratif dan sanksi pidana bagi penyelenggara

sistem elektronik yang tidak memenuhi hak perlindungan data pribadi di Indonesia. Meskipun masih terbuka peluang mendapat kompensasi yang bisa diajukan melalui gugatan perdata atas kerugian yang ditimbulkan. Indonesia tidak memiliki satu lembaga khusus yang mengawasi perlindungan data pribadi secara menyeluruh. Hal ini karena pengaturan perlindungan data pribadi masih tersebar. Masing-masing lembaga terkait aturan sektoral mengawasi perlindungan data pribadi yang menjadi kewenangannya. Oleh karena itu, menyediakan regulasi yang memadai agar bisnis digital dapat berkembang dengan baik perlu menjadi perhatian serius setiap pemangku kepentingan.

Kehilangan dana dalam rekening menjadi salah satu d ampak karena penyalahgunaan atas data pribadi pada perbankan digital. Kasus seperti ini masih terjadi sebab pemerintah dalam yurisdiksi hukum belum memberik an kenyamanan yang sepenuhnya. Perlindungan data pribadi nasabah bank menjadi salah satu aspek Hak Asasi Manusia (HAM) yang harus diperjuangkan melalui kolaborasi berbagai pihak. Pasal 29 ayat (1) dan Pasal 30 dalam Undang-Undang Nomor 39 Tahun 1999 menyatakan bahwa sangat urgen sekali hak-hak para nasabah bank untuk diperhatikan. Audit keamanan yang dilakukan secara berkala juga menjadi bagian penting dalam menjaga efektivitas sistem keamanan yang diterapkan. Melalui audit ini, bank dapat mengidentifikasi dan menangani potensi kelemahan dalam sistem keamanan yang mungkin dapat dimanfaatkan oleh pihak yang tidak bertang gung jawab. Selain itu, pelatihan keamanan data bagi karyawan juga sangat penting, agar mereka memahami tanggung jawab mereka dalam menjaga data nasabah dan dapat mengidentifikasi potensi risiko yang mungkin terjadi.(Lutfi, Kurniasari dan Putri, 2024)

Kerangka hukum yang diatur dalam Undang-Undang OJK dan Undang-Undang Perlindungan Konsumen memberikan landasan yang jelas untuk melindungi data pribadi nasabah. Dalam Rancangan Undang-Undang Perbankan yang sedang dibahas, terdapat pengaturan khusus mengenai perlindungan data pribadi nasabah, yang menegaskan kewajiban bank untuk menjaga kerahasiaan informasi nasabah dan meminta persetujuan tertulis sebelum mengungkapkan data kepada pihak ketiga. Dengan adanya regulasi yang ketat ini, diharapkan tidak akan terjadi penyalahgunaan data pribadi oleh pihak ketiga tanpa persetujuan dari nasabah. Secara keseluruhan, perlindungan data nasabah merupakan tanggung jawab bersama antara bank, pemerintah, dan masyarakat. Kerjasama yang baik antara semua pihak ini sangat penting untuk menciptakan lingkungan perbankan yang aman dan terpercaya di Indonesia. Dengan demikian, diharapkan bahwa langkah-langkah yang diambil dalam perlindungan data nasabah tidak hanya akan meningkatkan kepercayaan masyarakat terhadap lembaga keuangan, tetapi juga akan berkontribusi pada stabilitas dan pertumbuhan sektor perbankan secara keseluruhan.(Keliat *et al.*, 2023)

Pengaturan perlindungan terhadap kerahasiaan dan keamanan data pribadi nasabah bank di Indonesia diatur dalam Pasal 40 Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998, bahwa bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, hal tersebut juga berlaku pula bagi Pihak Terafiliasi. Meskipun dalam pasal tersebut tidak diatur secara khusus perlindungan terhadap data pribadi nasabah, data pribadi dapat dikategorikan dalam lingkup rahasia bank yang berupa keterangan mengenai nasabah penyimpanan.(Tambing *et al.*, 2023)

Sampai saat ini kesadaran hukum masyarakat Indonesia dalam merespon aktivitas cybercrime masih dirasa kurang. Hal ini disebabkan oleh kurangnya pengetahuan dan pemahaman (lack of information) masyarakat terhadap jenis kejahatan cybercrime sehingga penanggulangan phishing mengalami kendala dalam penataan hukum dan pengawasan hukum. Bagian yang terpenting dari masyarakat yang menentukan penegakan hukum adalah kesadaran hukum masyarakat. Semakin tinggi tingkat kesadaran hukum masyarakat, maka akan semakin memungkinkan penegakan hukum yang baik. Sebaliknya semakin rendah tingkat kesadaran hukum masyarakat, maka akan semakin sukar untuk melaksanakan penegakan hukum yang baik. Kesadaran hukum antara lain meliputi: Pengetahuan tentang hukum, Penghayatan fungsi hukum dan ketaatan terhadap hukum.

Bank memiliki kewajiban untuk mengimplementasikan langkah-langkah keamanan yang memadai, seperti enkripsi data, otentikasi dua faktor, dan pengawasan ketat terhadap akses data. Bank juga wajib memberikan pemberitahuan mengenai kebijakan privasi yang menjelaskan bagaimana data nasabah dikumpulkan, disimpan, dan dilindungi. Sementara itu, nasabah harus proaktif dalam melindungi data mereka, seperti menggunakan kata sandi yang kuat, mengaktifkan otentikasi dua faktor, dan menghindari berbagi informasi pribadi yang tidak perlu. Selain itu, penting bagi nasabah untuk waspada terhadap ancaman phishing dan selalu memperbarui perangkat lunak keamanan mereka. Pendidikan dan sosialisasi kepada masyarakat tentang pentingnya menjaga data pribadi juga menjadi kunci. Bank dan lembaga keuangan perlu mengadakan kampanye untuk meningkatkan kesadaran ini, sementara pemerintah dapat memperkenalkan regulasi yang lebih ketat terkait perlindungan data pribadi, seperti yang diatur dalam UU PDP. Dengan adanya regulasi yang jelas, serta kerjasama antara lembaga keuangan dan nasabah dalam menjaga keamanan data, risiko kebocoran dapat diminimalkan. Kepercayaan masyarakat terhadap sistem perbankan pun dapat terjaga, menciptakan ekosistem perbankan yang aman dan terpercaya.(Nurdin, 2018)

Efektivitas perlindungan hukum nasabah terhadap kejahatan phising di lingkungan perbankan dapat dilakukan melalui perlindungan hukum preventif, dikarenakan perlindungan hukum represif belum efektif karna masi tingginya tingkat kejahatan dan sulitnya menemukan pelaku disebabkan kecepatan transaksi yang terjadi, pihak bank tidak sembarang memblokir rekening penampungan karna ada prosedur tertentu yang harus dipenuhi, adanya rekening fiktif penampungan mungkin menggunakan identitas korban sebelumnya, pelaku menghapus jejak digital, pelaku bisa berada dimana saja sehingga sulit menerapkan sanksi hukum yang tegas. Selain berfokuas pada perlindungan hukum, kesadaran hukum nasabah dalam menjaga data pribadi harus di tingkatkan agar nasabah atau masyarakat dapat terhindar dari kejahatan siber. Kemampuan penegak hukum maupun sistem yang digunakan dalam menangani kejahatan siber harus mempuni untuk dapat mengimbangi perkembangan teknologi yang semakin maju.(Ekayani, Djanggih dan Suong, 2023)

4. Rekomendasi untuk Memperkuat Perlindungan Data Nasabah di Sektor Perbankan

Kehilangan dana dalam rekening menjadi salah satu dampak karenapenyalahgunaan atas data pribadi pada perbankan digital. Kasus seperti ini masih terjadi sebab pemerintah dalam yurisdiksi hukum belum memberikan kenyamanan yang sepenuhnya. Perlindungan data pribadi nasabah bank menjadi salah satu aspek Hak Asasi Manusia (HAM) yang harus

diperjuangkan melalui kolaborasi berbagai pihak. Pasal 29 ayat (1) dan Pasal 30 dalam Undang-Undang Nomor 39 Tahun 1999 menyatakan bahwa sangat urgen sekali hak-hak para nasabah bank untuk diperhatikan. Audit keamanan yang dilakukan secara berkala juga menjadi bagian penting dalam menjaga efektivitas sistem keamanan yang diterapkan. Melalui audit ini, bank dapat mengidentifikasi dan menangani potensi kelemahan dalam sistem keamanan yang mungkin dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Selain itu, pelatihan keamanan data bagi karyawan juga sangat penting, agar mereka memahami tanggung jawab mereka dalam menjaga data nasabah dan dapat mengidentifikasi potensi risiko yang mungkin terjadi.(Faizal *et al.*, 2023)

Kerangka hukum yang diatur dalam Undang-Undang OJK dan Undang-Undang Perlindungan Konsumen memberikan landasan yang jelas untuk melindungi data pribadi nasabah. Dalam Rancangan Undang-Undang Perbankan yang sedang dibahas, terdapat pengaturan khusus mengenai perlindungan data pribadi nasabah, yang menegaskan kewajiban bank untuk menjaga kerahasiaan informasi nasabah dan meminta persetujuan tertulis sebelum mengungkapkan data kepada pihak ketiga. Dengan adanya regulasi yang ketat ini, diharapkan tidak akan terjadi penyalahgunaan data pribadi oleh pihak ketiga tanpa persetujuan dari nasabah. Secara keseluruhan, perlindungan data nasabah merupakan tanggung jawab bersama antara bank, pemerintah, dan masyarakat. Kerjasama yang baik antara semua pihak ini sangat penting untuk menciptakan lingkungan perbankan yang aman dan terpercaya di Indonesia. Dengan demikian, diharapkan bahwa langkah-langkah yang diambil dalam perlindungan data nasabah tidak hanya akan meningkatkan kepercayaan masyarakat terhadap lembaga keuangan, tetapi juga akan berkontribusi pada stabilitas dan pertumbuhan sektor perbankan secara keseluruhan.(Ningsih dan Ismaini, 2025)

Pengaturan perlindungan terhadap kerahasiaan dan keamanan data pribadi nasabah bank di Indonesia diatur dalam Pasal 40 Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan sebagaimana telah diubah dengan Undang-Undang Nomor 10 Tahun 1998, bahwa bank wajib merahasiakan keterangan mengenai Nasabah Penyimpan dan simpanannya, hal tersebut juga berlaku pula bagi Pihak Terafiliasi. Meskipun dalam pasal tersebut tida diatur secara khusus perlindungan terhadap data pribadi nasabah, data pribadi dapat dikategorikan dalam lingkup rahasia bank yang berupa keterangan mengenai nasabah penyimpanan.(Mulyana, 2021)

Sampai saat ini kesadaran hukum masyarakat Indonesia dalam merespon aktivitas cybercrime masih dirasa kurang. Hal ini disebabkan oleh kurangnya pengetahuan dan pemahaman (*lack of information*) masyarakat terhadap jenis kejahatan *cybercrime* sehingga penanggulangan *phishing* mengalami kendala dalam penataan hukum dan pengawasan hukum. Bagian yang terpenting dari masyarakat yang menentukan penegakan hukum adalah kesadaran hukum masyarakat. Semakin tinggi tingkat kesadaran hukum masyarakat, maka akan semakin memungkinkan penegakan hukum yang baik. Sebaliknya semakin rendah tingkat kesadaran hukum masyarakat, maka akan semakin sukar untuk melaksanakan penegakan hukum yang baik. Kesadaran hukum antara lain meliputi: pengetahuan tentang hukum, penghayatan fungsi hukum dan ketaatan terhadap hukum.

Bank memiliki kewajiban untuk mengimplementasikan langkah-langkah keamanan yang memadai, seperti enkripsi data, otentikasi dua faktor, dan pengawasan ketat terhadap akses data. Bank juga wajib memberikan pemberitahuan mengenai kebijakan privasi yang

menjelaskan bagaimana data nasabah dikumpulkan, disimpan, dan dilindungi. Sementara itu, nasabah harus proaktif dalam melindungi data mereka, seperti menggunakan kata sandi yang kuat, mengaktifkan otentikasi dua faktor, dan menghindari berbagi informasi pribadi yang tidak perlu. Selain itu, penting bagi nasabah untuk waspada terhadap ancaman phishing dan selalu memperbarui perangkat lunak keamanan mereka. Pendidikan dan sosialisasi kepada masyarakat tentang pentingnya menjaga data pribadi juga menjadi kunci. Bank dan lembaga keuangan perlu mengadakan kampanye untuk meningkatkan kesadaran ini, sementara pemerintah dapat memperkenalkan regulasi yang lebih ketat terkait perlindungan data pribadi, seperti yang diatur dalam UU PDP. Dengan adanya regulasi yang jelas, serta kerjasama antara lembaga keuangan dan nasabah dalam menjaga keamanan data, risiko kebocoran dapat diminimalkan. Kepercayaan masyarakat terhadap sistem perbankan pun dapat terjaga, menciptakan ekosistem perbankan yang aman dan terpercaya.(Fonda dan Hoesein, 2025)

Efektivitas perlindungan hukum nasabah terhadap kejahatan *phising* di lingkungan perbankan dapat dilakukan melalui perlindungan hukum preventif, dikarenakan perlindungan hukum represif belum efektif karna masi tingginya tingkat kejahatan dan sulitnya menemukan pelaku disebabkan kecepatan transaksi yang terjadi, pihak bank tidak sembarang memblokir rekening penampungan karna ada prosedur tertentu yang harus dipenuhi, adanya rekening fiktif penampungan mungkin menggunakan identitas korban sebelumnya, pelaku menghapus jejak digital, pelaku bisa berada dimana saja sehingga sulit menerapkan sanksi hukum yang tegas. Selain berfokuas pada perlindungan hukum, kesadaran hukum nasabah dalam menjaga data pribadi harus di tingkatkan agar nasabah atau masyarakat dapat terhindar dari kejahatan siber. Kemampuan penegak hukum maupun sistem yang digunakan dalam menangani kejahatan siber harus mempuni untuk dapat mengimbangi perkembangan teknologi yang semakin maju.

KESIMPULAN

Perlindungan data nasabah dalam sektor perbankan di Indonesia menjadi isu yang semakin krusial seiring dengan meningkatnya digitalisasi layanan keuangan. Inovasi seperti mobile banking dan dompet digital telah memberikan kemudahan bagi masyarakat, namun juga menghadirkan tantangan baru, terutama dalam keamanan data dan privasi nasabah. Kasus kebocoran data perbankan yang semakin marak menunjukkan bahwa sistem keamanan perbankan masih memiliki celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab. Analisis terhadap regulasi perbankan di Indonesia menunjukkan bahwa Undang-Undang No. 10 Tahun 1998 tentang Perbankan yang mengatur rahasia bank belum sepenuhnya mampu menghadapi tantangan era digital. Meskipun pemerintah telah mengesahkan Undang-Undang No. 27 Tahun 2022 tentang UU PDP untuk memperkuat kerangka hukum perlindungan data, masih terdapat tumpang tindih regulasi dan kelemahan dalam implementasi. Selain itu, peran OJK dan Bank Indonesia (BI) dalam mengawasi keamanan data nasabah masih menghadapi berbagai kendala, terutama dalam hal penegakan sanksi dan transparansi kebocoran data. Dibandingkan dengan regulasi di negara lain, seperti GDPR di Uni Eropa dan Gramm-Leach-Bliley Act (GLBA) di Amerika Serikat, Indonesia masih memiliki kesenjangan hukum dalam standar keamanan siber dan mekanisme kompensasi bagi korban kebocoran data. Oleh karena

itu, diperlukan beberapa langkah strategis untuk memperkuat perlindungan data nasabah di sektor perbankan, antara lain:

1. Peningkatan standar keamanan siber melalui regulasi yang mewajibkan perbankan untuk menerapkan enkripsi data, sistem deteksi ancaman siber, serta audit keamanan secara berkala.
2. Penguatan regulasi dan sanksi bagi perbankan, termasuk denda yang lebih berat bagi bank yang lalai dalam melindungi data nasabah serta kewajiban pelaporan insiden kebocoran data dalam waktu yang ditentukan.
3. Edukasi bagi nasabah perbankan untuk meningkatkan kesadaran mengenai pentingnya perlindungan data pribadi dan cara menghindari modus kejahatan digital seperti phishing dan social engineering.

Dengan adanya harmonisasi antara regulasi perbankan dan perlindungan data pribadi, serta peningkatan pengawasan oleh OJK dan Bank Indonesia, diharapkan sistem perbankan digital di Indonesia dapat berkembang dengan lebih aman dan terpercaya. Keberhasilan dalam mengatasi tantangan ini akan berdampak positif terhadap kepercayaan publik, stabilitas sistem keuangan nasional, dan pertumbuhan ekonomi digital di Indonesia.

DAFTAR PUSTAKA

Antoine, R.A. *et al.* (2025) "Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT . Bank Syariah Indonesia)," *Jurnal Multidisiplin Ilmu Akademik*, 2(1), hal. 316–327. Tersedia pada: https://doi.org/: https://doi.org/10.61722/jmia.v2i1.3147.

Bandaso, T.I., Randa, F. dan Mongan, F.F.A. (2022) "Blockchain Technology: Bagaimana Menghadapinya? – Dalam Perspektif Akuntansi," *Accounting Profession Journal*, 4(2), hal. 97–115. Tersedia pada: https://doi.org/10.35593/apaji.v4i2.55.

Ekayani, L., Djanggih, H. dan Suong, M.A. (2023) "Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan," *Journal of Philosopy (JLP)*, 4(1), hal. 22–40. Tersedia pada: https://pasca-umi.ac.id/index.php/jlp/article/view/2023-06-25/2052.

Faizal, M.A. *et al.* (2023) "Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman dan Tantangan Terkini," *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi dan Bisnis Islam*, 5(2), hal. 87–100. Tersedia pada: https://doi.org/10.47435/asy-syarikah.v5i2.2022.

Fitrianto, B. (2020) "Aspek Hukum Pidana Pada Kejahatan Perbankan Dalam Perspektif Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perbankan," *Jurnal SOMASI (Sosial Humaniora Komunikasi)*, 1(2), hal. 334–345. Tersedia pada: https://doi.org/10.53695/js.v1i2.130.

Fonda, H. dan Hoesein, Z.A. (2025) "Pertanggungjawaban Bank dalam Menjamin Keamanan Data Nasabah di Era Digitalisasi Perbankan," *Jurnal Retentum*, 7(1), hal. 34–47. Tersedia pada: https://www.ejurnal.kampusakademik.co.id/index.php/jmia/article/view/3147.

Harahap, L.H. *et al.* (2024) "PERAN BUKTI ELEKTRONIK DALAM PENEGAKAN HUKUM PIDANA: TANTANGAN DAN IMPLIKASI DI ERA DIGITAL," *JURNAL HUKUM DAN KEBIJAKAN PUBLIK*, 6(3), hal. 578–588. Tersedia pada: https://journalpedia.com/1/index.php/jhkp/article/view/3035/3055.

Haryanto, A. dan Sutra, S.M. (2023) "Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020," *Global Political Studies Journal*, 7(1), hal. 56–69. Tersedia pada: https://doi.org/10.34010/gpsjournal.v7i1.8141.

Hidayat, A. (2021) "Critical Review Buku 'Penelitian Hukum' Peter Mahmud Marzuki Penelitian Hukum Ad Quemtentang Norma," *YUSTISIA MERDEKA : Jurnal Ilmiah Hukum*, 7(2), hal. 117–125. Tersedia pada: https://doi.org/10.33319/yume.v7i2.109.

Iermansyah, A., Astanti, D.I. dan Heryanti, B.R. (2023) "PERLINDUNGAN HUKUM BAGI KONSUMEN DALAM JASA LAYANAN KEUANGAN (DIGITAL FINANCIAL TECHNOLOGY)," *Semarang Law Review*, 13(1), hal. 104–116.

Irmawati, E., Pieries, J. dan Widiarty, W.S. (2024) "PERLINDUNGAN HUKUM ATAS DATA PRIBADI NASABAH BANK PENGGUNA MOBILE BANKINGDALAM PERSPEKTIF UU NO 27 TAHUN 2022 TENTANG KEBOCORAN DATA," *Jurnal Syntax Dmiration*, 15(1), hal. 37–48. Tersedia pada: https://jurnalsyntaxadmiration.com/index.php/jurnal/article/view/964/1387.

Keliat, V.U. *et al.* (2023) "Analisis Upaya Dan Peran Perlindungan Hukum Terhadap Kasus Peretasan Data Bank Syariah Indonesia," *Ilmu Hukum Prima (IHP)*, 6(2), hal. 182–190. Tersedia pada: https://doi.org/10.34012/jihp.v6i2.4251.

Kusuma, A.C. dan Rahmani, A.D. (2022) "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia)," *SUPREMASI : Jurnal Hukum*, 5(1), hal. 46–63. Tersedia pada: https://doi.org/10.36441/supremasi.v5i1.721.

Lestari, T. (2024) "Pertanggungjawaban Perbankan Dalam Melindungi Data Pribadi Nasabah Akibat Peretasan Studi Kasus Bank Syariah Indonesia," *Jurnal Perbankan*, 2(3), hal. 48–59.

Lutfi, M.P., Kurniasari, E. dan Putri, F.E.A. (2024) "URGENSI PERLINDUNGAN HUKUM TERHADAP DATA PRIVASI NASABAH BANK DI ERA PERKEMBANGAN DIGITAL," *Jurnal Multidisiplin Ilmu Akademik*, 1(5), hal. 210–218. Tersedia pada: https://doi.org/https://doi.org/10.61722/jmia.v1i5.2679.

Maharani, R. dan Prakoso, A.L. (2024) "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *Jurnal Usm Law Review*, 7(1), hal. 333. Tersedia pada: https://doi.org/10.26623/julr.v7i1.8705.

Mulyana, Y. (2021) "TINDAK PIDANA PENGGELAPAN OLEH PEMEGANG JABATAN DIHUBUNGKAN DENGAN PRINSIP KERAHASIAAN BANK," *Journal of Innovation Research and Knowledge*, 1(5), hal. 713–722. Tersedia pada: https://bajangjournal.com/index.php/JIRK/article/view/464/301.

Ningsih, A.S. dan Ismaini, D. (2025) "Keamanan data nasabah bank syariah," 2(1), hal. 651–662.

Nurdin, A.R. (2018) "Kajian Peraturan Perlindungan Konsumen Di Sektor Perbankan," *Jurnal Hukum & Pembangunan*, 48(2), hal. 299. Tersedia pada: https://doi.org/10.21143/jhp.vol48.no2.1665.

Oktavianes, S.D.Y. *et al.* (2025) "TRANSFORMASI DIGITAL FINNAIR MELALUI PROGRAM NDC MENGGUNAKAN ANALISIS SWOT DAN PEST," *JUMPER: Jurnal Manajemen dan Oemasaran*, 3(2), hal. 508–520. Tersedia pada: https://ojs.unhaj.ac.id/index.php/jumper/article/view/1392/767.

Pranata, A. *et al.* (2024) "IMPLEMENTASI ASAS KEHATI-HATIAN DALAM PERLINDUNGAN DATA PRIBADI BERDASARKAN UNDANG-UNDANG NOMOR 27

TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI DI ERA DIGITAL 5.0 Andri," *Journal of Law and Nation (JOLN)*, 3(3), hal. 721–730.

Rosidi, A., Zainuddin, M. dan Arifiana, I. (2024) "Metode Dalam Penelitian Hukum Normatif Dan Sosiologis (Field Research)," *Journal Law and Government*, 2(1), hal. 46–58. Tersedia pada: file:///C:/Users/ASUS/Downloads/21606-69294-1-PB.pdf.

Simatangkir, D.W.E., Afifah, E.F.N. dan Faliha, N.S. (2025) "KEAMANAN SIBER DALAM PERBANKAN SERTA TANTANGAN," *Jurnal Multidisiplin Ilmu Akademik*, 2(1), hal. 33–42. Tersedia pada: https://doi.org/https://doi.org/10.61722/jmia.v2i1.3119.

Sirait, Y.H. (2019) "General Data Protection Regulation (Gdpr) Dan Kedaulatan Negara Non-Uni Eropa," *Gorontalo Law Review*, 2(2), hal. 60. Tersedia pada: https://doi.org/10.32662/golrev.v2i2.704.

Sitanggang, A.S. *et al.* (2024) " Analisis Tingkat Kepercayaan Nasabah pada Keamanan Transaksi Perbankan melalui Mobile Banking (M-Banking)," *Jurnal Masharif Al-Syariah*, 9(3), hal. 1566–1581.

Syahputra, M.R. (2024) "METODOLOGI PENELITIAN HUKUM DALAM MENYELESAIKAN PROBLEMATIKA HUKUM KONTEMPORER," *Jurisprudensi: Jurnal Ilmu Hukum*, 1(2), hal. 89–106. Tersedia pada: https://doi.org/https://doi.org/10.70193/jurisprudensi.v1i02.08.

Tambing, F. *et al.* (2023) "Keamanan Data Nasabah di Bank dan Perlindungan The Bank ' s Data Security and the Protection of Financial Services Authorities," *Journal Sutra Research of Law*, 5(1), hal. 32–42.

Yetno, A. (2024) "Tanggung Jawab Bank Dalam Menjaga Keamanan Dan Kerahasiaan Data Nasabah Perbankan Di Indonesia," *Morality : jurnal ilmu hukum*, 10(1), hal. 67–76. Tersedia pada: https://doi.org/: http://dx.doi.org/10.52947/ morality.v10i1.424.