Indonesian Journal of Law and Justice Volume: 3, Number 3, 2026, *Page*: 1-18

Perlindungan Hukum Nasabah Bank Konvensional dalam Kasus Kejahatan Siber di Era Digital

Nadhia Shafira Rismawati, Charis Alif Aditya Permana*, Nova Kurnia Safitri Tarigan, Aiko Danya Kinaya

Universitas Negeri Semarang

Abstrak: Penelitian ini bertujuan untuk menganalisis pengaturan hukum positif di Indonesia dalam memberikan perlindungan terhadap nasabah bank konvensional dari kejahatan siber di era digital, serta mengkaji bentuk pertanggungjawaban hukum bank dan efektivitas mekanisme penyelesaian sengketa. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan kasus, yang didukung oleh bahan hukum primer berupa peraturan perundang-undangan terkait perbankan, perlindungan konsumen, dan perlindungan data pribadi, serta bahan hukum sekunder berupa literatur ilmiah dan putusan pengadilan, dengan analisis data dilakukan secara kualitatif melalui interpretasi sistematis dan teleologis. Hasil penelitian menunjukkan bahwa transformasi digital dalam sektor perbankan meningkatkan efisiensi layanan sekaligus memperbesar risiko kejahatan siber seperti *phishing*, *malware*, dan pencurian data nasabah. Kerangka regulasi di Indonesia pada dasarnya telah mengatur perlindungan nasabah melalui prinsip kehati-hatian, perlindungan konsumen, dan perlindungan data pribadi, serta membuka ruang pertanggungjawaban bank secara perdata, administratif, dan pidana. Namun demikian, implementasinya masih menghadapi berbagai kendala, antara lain lemahnya sistem keamanan, rendahnya literasi digital masyarakat, serta belum optimalnya efektivitas mekanisme penyelesaian sengketa baik melalui penyelesaian internal bank, LAPS SJK, maupun jalur litigasi. Oleh karena itu, disimpulkan bahwa meskipun regulasi telah cukup komprehensif, diperlukan penguatan implementasi melalui peningkatan keamanan sistem perbankan, pengawasan regulator, serta edukasi kepada nasabah, disertai optimalisasi mekanisme penyelesaian sengketa guna menjamin perlindungan hukum yang efektif dan berkeadilan di era digital.

Kata Kunci: Perlindungan Hukum; Nasabah Bank; Kejahatan Siber; Perbankan; Pertanggungjawaban.

DOI: https://doi.org/10.47134/ijlj.v3i3.5640
*Correspondence: Charis Alif Aditya Permana
Email: charisalif@students.unnes.ac.id

Received: 26-01-2026
Accepted: 26-02-2026
Published: 26-03-2026

Abstract: *This study aims to analyze the positive legal framework in Indonesia regarding the protection of conventional bank customers from cybercrime in the digital age, as well as to examine the forms of legal liability of banks and the effectiveness of dispute resolution mechanisms. The research method employed is a normative legal approach using legislative, conceptual, and case-based methodologies, supported by primary legal sources such as laws and regulations related to banking, consumer protection, and personal data protection, as well as secondary legal sources including academic literature and court rulings, with data analysis conducted qualitatively through systematic and teleological interpretation. The research findings indicate that digital transformation in the banking sector enhances service efficiency while simultaneously increasing the risk of cybercrimes such as phishing, malware, and customer data theft. The regulatory framework in Indonesia fundamentally addresses customer protection through the principles of prudence, consumer protection, and personal data protection, and establishes avenues for holding banks accountable under civil, administrative, and criminal law. However, its implementation still faces various obstacles, including weak security systems, low public digital literacy, and the suboptimal effectiveness of dispute resolution mechanisms—whether through internal bank resolution, the LAPS SJK, or litigation. Therefore, it is concluded that although the regulations are already quite comprehensive, their implementation must be strengthened through improved banking system security, enhanced regulatory oversight, and customer education, along with the optimization of dispute resolution mechanisms to ensure effective and equitable legal protection in the digital age.*

Keywords: *Legal Protection; Bank Customers; Cybercrime; Banking; Liability.*

Pendahuluan

Revolusi industri 4.0 telah mendorong transformasi digital yang masif di berbagai sektor, termasuk industri perbankan. Perbankan konvensional di Indonesia merespons perkembangan ini dengan menghadirkan layanan berbasis teknologi seperti *mobile banking*, *internet banking*, dan berbagai *e-channel* lainnya. Inovasi ini bertujuan memberikan kemudahan, kecepatan, serta efisiensi bagi nasabah dalam melakukan transaksi keuangan kapan saja dan di mana saja (Chairunnisa et al., 2024). Namun, pesatnya digitalisasi layanan perbankan berbanding lurus dengan peningkatan risiko kejahatan siber yang semakin kompleks. Berdasarkan laporan Otoritas Jasa Keuangan Tahun 2023, tercatat lebih dari 11.000 kasus penipuan digital di sektor perbankan dengan kerugian mencapai ratusan miliar rupiah (Asmaru Amru, 2025). Modus kejahatan seperti *phishing*, *skimming*, *malware*, rekayasa sosial, hingga pembobolan data menjadi ancaman nyata yang tidak hanya merugikan secara finansial tetapi juga menggerus kepercayaan nasabah terhadap sistem perbankan. Kejahatan siber ini memanfaatkan celah keamanan sistem elektronik dan kerentanan pengguna, menjadikannya tantangan serius dalam lanskap keamanan siber nasional. Dalam hubungan hukum antara nasabah dan bank, nasabah secara struktural menempati posisi yang lebih lemah. Nasabah adalah konsumen yang hanya dapat menerima atau menolak produk dan layanan yang telah ditetapkan oleh bank sebagai pelaku usaha jasa keuangan (Chairunnisa et al., 2024). Ketergantungan nasabah pada sistem elektronik bank dan keterbatasan pemahaman terhadap teknologi informasi sering kali membuat mereka menjadi pihak paling rentan menjadi korban kejahatan siber. Kerugian yang dialami nasabah tidak hanya bersifat materiil, seperti hilangnya dana di rekening, tetapi juga immateriil, seperti kebocoran data pribadi yang dapat disalahgunakan untuk tindak kejahatan lainnya (Utomo et al., 2024). Posisi yang tidak seimbang ini menegaskan perlunya campur tangan negara melalui hukum untuk memberikan perlindungan yang memadai bagi nasabah sebagai konsumen pengguna jasa perbankan digital. Sebagaimana dikemukakan dalam teori hukum pembangunan Mochtar Kusumaatmadja, hukum berfungsi sebagai sarana pembaruan masyarakat dan melindungi kelompok rentan untuk mencapai ketertiban dan kepastian hukum (Chairunnisa et al., 2024).

Prinsip kehati-hatian yang menjadi fondasi operasional perbankan mewajibkan bank untuk senantiasa menjalankan usahanya secara hati-hati dalam rangka melindungi dana masyarakat yang dipercayakan kepadanya (Keliat, 2024). Prinsip ini diperkuat dengan kewajiban bank memberikan perlindungan konsumen, yang menuntut bank tidak hanya bertanggung jawab atas keamanan dana nasabah, tetapi juga atas kerahasiaan dan keamanan data pribadi nasabah. Berdasarkan Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, bank sebagai penyelenggara sistem elektronik wajib menyelenggarakan sistem secara andal dan aman serta bertanggung jawab atas pengoperasiannya (Chairunnisa et al., 2024). Tanggung jawab ini mencakup upaya preventif melalui penguatan sistem keamanan siber, serta upaya represif melalui penanganan dan penyelesaian pengaduan nasabah ketika terjadi insiden kejahatan siber. Dalam praktiknya, bank wajib menerapkan tata kelola teknologi informasi yang baik dan

menjaga ketahanan siber sesuai Peraturan OJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi (Chairunnisa et al., 2024).

Menyadari urgensi perlindungan nasabah di era digital, pemerintah bersama regulator telah menerbitkan berbagai instrumen hukum. Otoritas Jasa Keuangan sebagai lembaga pengawas sektor jasa keuangan mengeluarkan POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan yang mewajibkan bank bertanggung jawab atas kerugian nasabah yang disebabkan oleh kesalahan bank (Keliat, 2024). Bank Indonesia sebagai bank sentral juga memiliki kewenangan dalam mengatur sistem pembayaran yang aman. Lembaga Penjamin Simpanan turut berperan memberikan rasa aman dengan menjamin simpanan nasabah, meskipun jaminan ini tidak mencakup kerugian akibat kejahatan siber yang bersifat non-kegagalan bank (Utomo et al. 2024). Selain itu, POJK Nomor 12/POJK.03/2021 tentang Bank Umum mengatur secara khusus mengenai bank digital, termasuk kewajiban memiliki model bisnis dengan teknologi yang inovatif dan aman serta menjalankan perlindungan terhadap data nasabah (Keliat, 2024)atkan perkembangan teknologi informasi dan sistem digital dalam layanan keuangan.

Secara lebih spesifik, perlindungan hukum terhadap nasabah bank konvensional di era digital diatur dalam beberapa undang-undang utama. Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Jasa Keuangan mengatur kewajiban bank menjaga rahasia bank dan memberikan sanksi berat atas pelanggarannya, termasuk pidana penjara hingga 4 tahun dan denda miliaran rupiah (Chairunnisa et al., 2024). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya menjadi payung hukum utama untuk menjerat pelaku kejahatan siber seperti *phishing* dan *hacking* dengan ancaman pidana penjara hingga 10 tahun dan denda hingga Rp10 miliar (Asmaru Amru, 2025). Sementara itu, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi memperkuat kerangka hukum perlindungan data pribadi nasabah dan memberikan hak untuk menuntut ganti rugi atas kebocoran data. Keberadaan regulasi ini menunjukkan keseriusan negara menciptakan ekosistem perbankan digital yang aman dan memberikan kepastian hukum bagi nasabah. Namun, implementasi di lapangan masih menghadapi tantangan, seperti tumpang tindih norma, keterbatasan kapasitas forensik digital aparat penegak hukum, serta kelemahan sistem elektronik perbankan yang masih dapat dieksploitasi (Asmaru Amru, 2025). Studi menunjukkan bahwa 68% nasabah korban penipuan digital tidak puas dengan penanganan hukum yang diterima (Asmaru Amru, 2025). Oleh karena itu, penelitian mengenai perlindungan hukum terhadap nasabah bank konvensional di era digital menjadi sangat penting untuk memastikan hak-hak nasabah terakomodasi secara optimal dan penegakan hukum dapat berjalan efektif.

Berdasarkan latar belakang yang telah diuraikan, penelitian ini mengajukan rumusan masalah yang akan dikaji secara komprehensif, yaitu bagaimana pengaturan hukum positif Indonesia dalam memberikan perlindungan kepada nasabah bank konvensional terhadap kejahatan siber di era digital, serta bagaimana bentuk

pertanggungjawaban hukum bank konvensional dan efektivitas mekanisme penyelesaian sengketa dalam melindungi nasabah korban kejahatan siber.

Metode Penelitian

Jenis Penelitian

Penelitian ini menggunakan jenis penelitian yuridis normatif yang berfokus pada kajian terhadap norma-norma hukum positif yang mengatur perlindungan nasabah bank konvensional dari kejahatan siber. Penelitian hukum normatif merupakan penelitian yang dilakukan dengan cara meneliti bahan pustaka atau data sekunder belaka, serta mengkaji aspek-aspek internal dari hukum positif. Pendekatan yang digunakan dalam penelitian ini meliputi tiga pendekatan utama. Pertama, pendekatan perundang-undangan (statute approach) dilakukan dengan menelaah berbagai peraturan perundang-undangan yang relevan, seperti Undang-Undang Perbankan, Undang-Undang Informasi dan Transaksi Elektonik, Undang-Undang Perlindungan Data Pribadi, serta peraturan turunan dari Otoritas Jasa Keuangan. Pendekatan perundang-undangan ini sangat penting digunakan dalam menganalisis suatu permasalahan hukum, karena penyelesaian isu hukum harus didasari dengan argumentasi yang membangun dan dengan pijakan aturan atau hukum positifnya (Zainuddin & Karina, 2023). Kedua, pendekatan konseptual (conceptual approach) digunakan untuk menganalisis konsep-konsep hukum seperti perlindungan konsumen, prinsip kehati-hatian, dan tanggung jawab bank dalam perspektif teori keadilan (Wiraguna, 2024). Ketiga, pendekatan kasus (case approach) diterapkan dengan mengkaji putusan-putusan pengadilan yang berkaitan dengan sengketa perbankan digital, guna memahami implementasi norma hukum dalam praktik peradilan. Kombinasi ketiga pendekatan ini diharapkan mampu memberikan pemahaman yang komprehensif mengenai perlindungan hukum nasabah di era digital.

Bahan Hukum

Sumber bahan hukum dalam penelitian ini dikategorikan menjadi bahan hukum primer dan bahan hukum sekunder, sesuai dengan karakteristik penelitian hukum normatif yang bertumpu pada data sekunder (Rizkia & Fardiansyah, 2023). Bahan hukum primer terdiri atas peraturan perundang-undangan yang menjadi landasan utama pengaturan perlindungan nasabah bank yaitu, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Jasa Keuangan, serta Peraturan Otoritas Jasa Keuangan (POJK) yang relevan seperti POJK Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan dan POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi (Sari, Fardiansyah & Tamza, 2025). Bahan hukum sekunder mencakup literatur hukum perbankan, jurnal ilmiah nasional terakreditasi yang membahas kejahatan siber dan perlindungan nasabah, serta putusan-putusan pengadilan terkait sengketa perbankan

digital (Ariningsih, Pamungkas & Lestari, t.t.). Bahan hukum tersier seperti kamus hukum dan ensiklopedia juga digunakan sebagai pelengkap untuk memperjelas istilah-istilah teknis (Benuf & Azhar, 2020). Pengumpulan bahan hukum dilakukan melalui studi kepustakaan dengan menelusuri peraturan perundang-undangan, jurnal ilmiah, buku, dan dokumen hukum lainnya (Sari, Fardiansyah & Tamza, 2025).

Teknik Analisis

Teknik analisis data dalam penelitian ini dilakukan secara kualitatif dengan menggunakan metode interpretasi sistematis dan teleologis. Dalam penelitian hukum normatif, analisis data dilakukan dengan menggunakan logika berpikir deduktif, dimana norma hukum positif, yurisprudensi, dan doktrin ditempatkan sebagai premis mayor, sementara data sekunder yang terkumpul ditempatkan sebagai premis minor untuk kemudian ditarik suatu kesimpulan (Benuf & Azhar, 2020). Interpretasi sistematis digunakan untuk memahami keterkaitan antar pasal dalam satu peraturan maupun antar peraturan yang berbeda, sehingga diperoleh pemahaman yang utuh mengenai struktur norma perlindungan nasabah (Wiraguna, 2024). Interpretasi teleologis diterapkan untuk menggali tujuan dan nilai filosofis di balik pembentukan suatu regulasi, khususnya dalam kaitannya dengan upaya mewujudkan keadilan substantif bagi nasabah sebagai konsumen jasa keuangan (Zainuddin & Karina, 2023). Selanjutnya, dilakukan analisis terhadap sinkronisasi vertikal dan horizontal antara peraturan perundang-undangan. Sinkronisasi vertikal mengkaji kesesuaian antara peraturan di tingkat undang-undang dengan peraturan pelaksana di bawahnya, seperti POJK, dengan memperhatikan hierarki peraturan perundang-undangan sebagaimana diatur dalam Undang-Undang Nomor 12 Tahun 2011 (Zainuddin & Karina, 2023). Sinkronisasi horizontal menganalisis harmonisasi antar undang-undang yang setingkat, misalnya antara UU Perbankan, UU ITE, dan UU PDP, guna mengidentifikasi potensi tumpang tindih atau kekosongan norma (Rizkia & Fardiansyah, 2023). Hasil analisis ini kemudian diinterpretasikan secara mendalam untuk menarik kesimpulan normatif mengenai efektivitas perlindungan hukum nasabah bank konvensional dalam menghadapi kejahatan siber di era digital.

Hasil dan Pembahasan

Transformasi Digital Bank Konvensional dan Peningkatan Risiko Kejahatan Siber

Perkembangan teknologi informasi telah mendorong perubahan besar dalam sistem layanan perbankan dari yang sebelumnya bersifat konvensional menjadi berbasis digital. Pada masa lalu, sebagian besar layanan perbankan dilakukan secara langsung di kantor bank, di mana nasabah harus datang untuk melakukan berbagai transaksi seperti transfer dana, penarikan uang, atau pembayaran tagihan. Namun, seiring dengan kemajuan teknologi, layanan perbankan kini telah bertransformasi menjadi layanan digital seperti *mobile banking*, *internet banking*, ATM, dan berbagai aplikasi keuangan berbasis elektronik yang memungkinkan nasabah melakukan transaksi secara lebih cepat, praktis, dan efisien tanpa harus datang ke bank (Farahdiva et al., 2025). Digitalisasi ini bertujuan untuk meningkatkan kualitas layanan, mempercepat proses transaksi, serta memperluas akses

masyarakat terhadap layanan keuangan (Simatangkir et al., 2025). Meskipun memberikan banyak kemudahan, penggunaan sistem digital dalam transaksi perbankan juga meningkatkan risiko kejahatan siber seperti phishing, malware, dan pencurian data yang dapat mengancam keamanan sistem serta data nasabah (Simatangkir et al., 2025). Oleh karena itu, transformasi digital dalam perbankan tidak hanya membawa kemudahan dan efisiensi, tetapi juga meningkatkan kerentanan terhadap ancaman kejahatan siber sehingga diperlukan sistem keamanan yang kuat untuk melindungi transaksi dan data pengguna (Bahram et al., 2024).

Perkembangan teknologi digital telah mengubah cara nasabah berinteraksi dengan lembaga keuangan. Jika sebelumnya hubungan antara nasabah dan bank lebih banyak dilakukan melalui tatap muka di kantor cabang, saat ini interaksi tersebut semakin beralih ke layanan digital seperti mobile banking dan internet banking yang memungkinkan transaksi dilakukan secara lebih praktis dan efisien. Perubahan pola interaksi ini sejalan dengan meningkatnya penggunaan teknologi digital dalam aktivitas masyarakat yang menuntut layanan yang cepat dan mudah diakses (Prayuti, 2024). Melalui layanan digital tersebut, nasabah juga menjadi lebih mandiri karena dapat melakukan berbagai transaksi secara langsung tanpa bantuan petugas bank. Digitalisasi layanan juga membuat proses transaksi menjadi lebih cepat, namun sekaligus meningkatkan ketergantungan terhadap sistem teknologi dan jaringan internet (Andriani, Haris, & Sumardi, 2025). Di sisi lain, meningkatnya penggunaan layanan digital juga memunculkan risiko keamanan seperti pencurian data, phishing, dan berbagai bentuk penipuan daring, terutama bagi pengguna yang memiliki literasi keamanan digital yang masih rendah (Putri, Sari, Fajrina, & Aisyah, 2025). Oleh karena itu, keamanan transaksi menjadi isu yang sangat penting dalam perkembangan layanan perbankan digital.

Kejahatan siber dalam sektor perbankan merupakan bentuk kejahatan modern yang memanfaatkan perkembangan teknologi informasi dan sistem digital dalam layanan keuangan. Dalam praktiknya, kejahatan ini sering dilakukan melalui berbagai modus seperti peretasan sistem (*hacking*), pencurian data nasabah, *phishing*, penyebaran *malware*, serta berbagai bentuk penipuan *online* yang bertujuan memperoleh akses tidak sah terhadap sistem perbankan maupun informasi pribadi nasabah (Azis & Redi, 2025). Pelaku kejahatan umumnya memanfaatkan kelalaian nasabah, rendahnya literasi digital, maupun celah keamanan pada sistem elektronik, sehingga data penting seperti identitas, kata sandi, atau informasi transaksi dapat disalahgunakan untuk melakukan tindak penipuan atau pencurian dana (Salsabila & Ilmih, 2024). Selain itu, kejahatan siber memiliki karakteristik khusus yaitu dilakukan melalui teknologi digital dan jaringan internet, sehingga pelaku dapat berada di lokasi yang berbeda bahkan lintas negara dengan korban, serta sering melibatkan jaringan yang sulit dilacak oleh aparat penegak hukum (Setiawan, 2024). Oleh karena itu, kejahatan siber di bidang perbankan dapat dipahami sebagai kejahatan yang bersifat kompleks, anonim, dan sangat bergantung pada pemanfaatan teknologi digital.

Rendahnya literasi digital masyarakat menjadi salah satu faktor utama yang meningkatkan risiko nasabah menjadi korban kejahatan siber dalam sektor perbankan. Tidak semua nasabah memiliki pengetahuan yang memadai mengenai keamanan digital,

sehingga banyak yang belum mampu mengenali berbagai bentuk ancaman siber seperti phishing, malware, maupun penipuan berbasis teknologi. Survei menunjukkan bahwa 36,3% masyarakat Indonesia belum mengetahui ciri-ciri phishing dan sekitar 40,9% belum memahami ancaman virus atau malware, yang menunjukkan masih rendahnya kesadaran keamanan siber di kalangan pengguna layanan digital, termasuk nasabah perbankan (Kementerian Komunikasi dan Informatika Republik Indonesia, 2017). Kondisi ini menyebabkan nasabah sering menjadi korban penipuan melalui tautan palsu, permintaan kode OTP, maupun modus voice phishing di mana pelaku berpura-pura sebagai pihak bank untuk memperoleh akses ke akun korban. Otoritas Jasa Keuangan juga mencatat meningkatnya kasus penipuan melalui SMS atau telepon palsu yang memanfaatkan data pribadi nasabah (Otoritas Jasa Keuangan, 2024). Oleh karena itu, peningkatan literasi keuangan digital dan edukasi keamanan siber oleh Bank Indonesia dan OJK menjadi langkah penting untuk meminimalkan risiko kejahatan siber terhadap nasabah (Otoritas Jasa Keuangan, 2024).

Kerangka Regulasi Perlindungan Hukum Nasabah

a. Prinsip Kehati-hatian (*Prudential Principle)*

Hukum di Indonesia memberikan perlindungan terhadap nasabah bank dari berbagai risiko digital melalui regulasi yang ditetapkan oleh Otoritas Jasa Keuangan dan Bank Indonesia. Regulasi tersebut mewajibkan bank menerapkan prinsip kehati-hatian (*prudential principle*) dalam penyelenggaraan kegiatan perbankan, termasuk dalam penggunaan teknologi informasi dan sistem elektronik. Prinsip kehati-hatian mengharuskan bank untuk mengidentifikasi, mengukur, memantau, dan mengendalikan berbagai risiko operasional yang dapat timbul, termasuk risiko teknologi informasi dan kejahatan siber. Ketentuan ini tercermin dalam berbagai regulasi seperti Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yang menekankan pentingnya pengelolaan risiko teknologi serta perlindungan terhadap data dan transaksi nasabah (Ramadhani, R., & Yudhayana, 2025). Selain itu, bank juga diwajibkan menerapkan manajemen risiko teknologi informasi secara komprehensif yang meliputi pengawasan oleh direksi dan dewan komisaris, penyusunan kebijakan keamanan sistem, serta pengendalian internal terhadap penggunaan teknologi digital dalam layanan perbankan. Perlindungan terhadap nasabah juga diwujudkan melalui penerapan standar keamanan sistem elektronik seperti penggunaan enkripsi data, autentikasi berlapis (*multi-factor authentication*), serta pengamanan server guna mencegah peretasan dan pencurian data nasabah. Di samping itu, bank juga wajib menerapkan prinsip *Good Corporate Governance* (GCG) yang meliputi transparansi, akuntabilitas, tanggung jawab, independensi, dan kewajaran dalam pengelolaan bank (Otoritas Jasa Keuangan, 2024). Penerapan prinsip ini bertujuan untuk memastikan bahwa operasional bank berjalan secara aman, profesional, serta mampu melindungi kepentingan nasabah dan menjaga kepercayaan publik terhadap sistem perbankan (Riyanto, 2023). Dengan demikian, regulasi perbankan di Indonesia menunjukkan bahwa perlindungan hukum terhadap

nasabah tidak hanya dilakukan melalui pengawasan regulator, tetapi juga melalui kewajiban internal bank dalam mengelola risiko digital secara efektif.

b. Prinsip Perlindungan Konsumen

Prinsip perlindungan konsumen dalam sektor perbankan di Indonesia merupakan salah satu dasar penting dalam melindungi nasabah dari berbagai risiko, termasuk risiko digital yang muncul akibat perkembangan layanan perbankan berbasis teknologi. Pengaturan mengenai perlindungan konsumen perbankan ditetapkan oleh Otoritas Jasa Keuangan melalui berbagai regulasi yang menegaskan hak nasabah untuk memperoleh layanan yang aman, transparan, serta mekanisme penyelesaian sengketa yang jelas. Salah satu bentuk perlindungan tersebut adalah hak atas keamanan dan kenyamanan, di mana nasabah berhak mendapatkan layanan perbankan digital yang aman serta sistem transaksi yang mampu melindungi data pribadi dan dana nasabah dari berbagai ancaman seperti kebocoran data, *phishing*, maupun serangan siber. Oleh karena itu, bank berkewajiban memastikan sistem teknologi informasi yang digunakan memiliki standar keamanan yang memadai serta mampu mencegah terjadinya gangguan yang dapat merugikan nasabah (Pesak, Tampongangoy, & Korua, 2024). Selain itu, nasabah juga memiliki hak atas informasi yang benar, sehingga bank wajib memberikan informasi yang jelas dan transparan mengenai penggunaan layanan perbankan digital, potensi risiko transaksi elektronik, serta berbagai bentuk penipuan yang mungkin terjadi. Penyampaian informasi yang akurat sangat penting agar nasabah dapat memahami cara penggunaan layanan secara aman serta mampu menghindari berbagai modus kejahatan siber (Azizah, Anggraeni, & Mustika, 2022). Di samping itu, prinsip perlindungan konsumen juga menjamin hak atas penyelesaian sengketa, di mana nasabah yang mengalami kerugian akibat layanan perbankan dapat mengajukan pengaduan melalui mekanisme internal bank, melalui lembaga alternatif penyelesaian sengketa seperti LAPS, maupun melalui jalur litigasi di pengadilan untuk memperoleh kepastian hukum(Harahap, Saidin, Sukarja, & Leviza, 2022). Dengan demikian, penerapan prinsip perlindungan konsumen menjadi instrumen penting dalam menjaga keamanan transaksi perbankan serta meningkatkan kepercayaan masyarakat terhadap sistem perbankan digital.

c. Perlindungan Data Pribadi Nasabah

Perlindungan data pribadi nasabah merupakan aspek penting dalam sistem perbankan modern, khususnya di tengah berkembangnya layanan perbankan digital. Di Indonesia, perlindungan tersebut diatur melalui berbagai regulasi, antara lain Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi serta berbagai ketentuan yang diterbitkan oleh Otoritas Jasa Keuangan dan Bank Indonesia. Dalam kerangka hukum tersebut, bank ditempatkan sebagai pengendali data yang memiliki kewajiban untuk melindungi dan mengelola data pribadi nasabah secara aman dan bertanggung jawab. Data pribadi yang dimaksud meliputi berbagai informasi penting seperti identitas nasabah, nomor rekening, serta riwayat transaksi yang hanya boleh

digunakan sesuai dengan tujuan pelayanan perbankan dan tidak boleh disalahgunakan oleh pihak mana pun. Oleh karena itu, bank diwajibkan menerapkan berbagai langkah pengamanan seperti sistem enkripsi data, mekanisme autentikasi yang kuat, serta audit keamanan secara berkala untuk memastikan kerahasiaan data tetap terjaga (Azizah, Anggraeni, & Mustika, 2022). Selain itu, bank juga dapat dimintai pertanggungjawaban apabila terjadi kebocoran data pribadi akibat kelalaian sistem atau lemahnya pengamanan teknologi informasi. Dalam kondisi tersebut, bank wajib segera memberikan pemberitahuan kepada nasabah yang terdampak, melakukan perbaikan terhadap sistem yang mengalami kerentanan, serta bertanggung jawab atas kerugian yang timbul akibat insiden tersebut (Bank Indonesia, 2023). Pelanggaran terhadap kewajiban perlindungan data pribadi juga dapat dikenakan sanksi administratif maupun perdata, seperti denda administratif, teguran dari regulator, hingga gugatan ganti rugi oleh nasabah melalui pengadilan. Ketentuan tersebut bertujuan memastikan bank menjalankan pengelolaan data secara bertanggung jawab serta memberikan perlindungan hukum yang memadai bagi nasabah dalam penggunaan layanan perbankan digital (Riyanto, 2023).

Pertanggungjawaban Hukum Bank Konvensional

Bank konvensional sebagai lembaga intermediasi keuangan memiliki kewajiban hukum untuk melindungi dana dan data nasabah dalam setiap kegiatan operasionalnya. Hubungan hukum antara bank dan nasabah pada dasarnya merupakan hubungan kontraktual yang menimbulkan hak dan kewajiban bagi kedua belah pihak. Oleh karena itu, apabila terjadi kerugian yang dialami oleh nasabah akibat kesalahan, kelalaian, maupun tindakan melawan hukum dalam aktivitas perbankan, bank dapat dimintai pertanggungjawaban secara hukum. Pertanggungjawaban tersebut dapat berbentuk tanggung jawab perdata, administratif, maupun pidana, tergantung pada jenis pelanggaran yang terjadi. Dalam konteks hukum di Indonesia, tanggung jawab bank juga berkaitan dengan berbagai peraturan perundang-undangan seperti Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, serta Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Habibi & Liviani, 2020).

a. Tanggung Jawab Perdata

Tanggung jawab perdata bank umumnya muncul dari hubungan kontraktual antara bank dan nasabah yang didasarkan pada perjanjian layanan perbankan. Perjanjian tersebut dapat berupa penyimpanan dana, layanan transfer, maupun penggunaan fasilitas perbankan digital. Apabila bank tidak menjalankan kewajibannya sebagaimana yang telah disepakati dalam perjanjian tersebut, maka bank dapat dianggap melakukan wanprestasi. Wanprestasi terjadi ketika salah satu pihak tidak memenuhi prestasi yang telah diperjanjikan sehingga menimbulkan kerugian bagi pihak lain. Dalam kondisi ini, nasabah yang dirugikan memiliki hak untuk menuntut ganti rugi terhadap kerugian yang dialaminya.Selain wanprestasi, tanggung jawab perdata bank juga dapat timbul akibat perbuatan melawan hukum (PMH) sebagaimana

diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata. PMH dapat terjadi apabila tindakan atau kelalaian bank menimbulkan kerugian bagi nasabah, misalnya kegagalan sistem keamanan perbankan yang menyebabkan pencurian dana atau kebocoran data pribadi nasabah. Dalam era digital saat ini, perkembangan teknologi informasi juga meningkatkan potensi terjadinya kejahatan siber yang dapat merugikan masyarakat, termasuk nasabah bank. Oleh karena itu, bank memiliki kewajiban untuk menjaga keamanan sistem elektronik serta melindungi data nasabah dari berbagai ancaman kejahatan digital (Hapsari & Pambayun, 2023). Dalam teori pertanggungjawaban hukum dikenal pula konsep *fault liability dan strict liability*. *Fault liability* menekankan bahwa tanggung jawab hanya dapat dibebankan apabila terbukti adanya kesalahan atau kelalaian dari pihak bank. Sementara itu, dalam konsep strict liability, bank dapat dimintai pertanggungjawaban meskipun unsur kesalahan tidak dapat dibuktikan secara langsung, selama kerugian yang dialami nasabah berkaitan dengan aktivitas usaha bank. Pendekatan ini sering digunakan untuk memberikan perlindungan hukum yang lebih kuat bagi konsumen jasa keuangan.

b. Tanggung Jawab Administratif

Selain pertanggungjawaban perdata, bank juga dapat dikenai sanksi administratif apabila melanggar ketentuan regulasi perbankan. Pengawasan terhadap sektor perbankan di Indonesia dilakukan oleh Otoritas Jasa Keuangan (OJK). Tanggung jawab administratif diatur oleh Otoritas Jasa Keuangan (OJK) melalui Peraturan OJK No. 38/POJK.03/2016 mengenai Manajemen Risiko Teknologi Informasi (Syafa Widya Annafa, 2024). OJK memiliki kewenangan untuk memastikan bahwa bank menjalankan kegiatan operasionalnya sesuai dengan prinsip kehati-hatian serta tata kelola yang baik. Pengawasan tersebut menjadi penting mengingat perkembangan teknologi juga membawa risiko baru dalam sistem keuangan, termasuk potensi kejahatan siber yang dapat mengancam keamanan sistem perbankan (Mahendra & Pinatih, 2023). Apabila bank terbukti melakukan pelanggaran terhadap ketentuan yang berlaku, OJK dapat menjatuhkan berbagai bentuk sanksi administratif. Sanksi tersebut dapat berupa teguran tertulis, denda administratif, pembatasan kegiatan usaha, hingga pencabutan izin usaha dalam kasus pelanggaran yang berat. Pengenaan sanksi administratif ini bertujuan untuk menjaga stabilitas sistem keuangan serta memberikan perlindungan bagi nasabah sebagai pengguna jasa perbankan. Dengan adanya pengawasan dan sanksi tersebut, bank diharapkan dapat menjalankan operasionalnya secara lebih transparan, akuntabel, serta sesuai dengan ketentuan hukum yang berlaku.

c. Tanggung Jawab Pidana

Selain tanggung jawab administratif, bank juga dapat dimintai pertanggungjawaban pidana apabila terbukti melakukan pelanggaran hukum yang berkaitan dengan perlindungan data pribadi nasabah. Ketentuan mengenai perlindungan data pribadi diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang memberikan sanksi pidana terhadap pihak yang secara

melawan hukum memperoleh, mengakses, mengumpulkan, atau menyebarkan data pribadi tanpa persetujuan pemiliknya. Dalam Pasal 65 undang-undang tersebut ditegaskan bahwa setiap orang yang melakukan perbuatan tersebut dapat dikenakan pidana penjara dan/atau denda (Syafa Widya Annafa, 2024). Dalam konteks perbankan, ketentuan ini dapat berlaku apabila terdapat kebocoran atau penyalahgunaan data nasabah yang terjadi akibat kesengajaan maupun kelalaian dalam pengelolaan sistem perbankan. Tanggung jawab pidana dalam sektor perbankan umumnya muncul apabila terdapat unsur kesengajaan atau kelalaian yang serius dalam menjaga keamanan sistem teknologi informasi. Salah satu contohnya adalah kegagalan bank dalam melindungi sistem elektronik yang menyebabkan terjadinya pembobolan rekening atau pencurian data nasabah oleh pihak yang tidak bertanggung jawab. Selain itu, tanggung jawab pidana juga dapat timbul akibat *insider fraud*, yaitu tindakan kecurangan yang dilakukan oleh pihak internal bank seperti karyawan atau pejabat bank, misalnya penggelapan dana, manipulasi transaksi, atau penyalahgunaan akses terhadap sistem perbankan. Perkembangan teknologi digital yang semakin pesat juga meningkatkan potensi terjadinya berbagai bentuk kejahatan siber di sektor perbankan (Kemal Idris Balaka, 2024). Oleh karena itu, diperlukan sistem keamanan teknologi informasi yang kuat, pengawasan internal yang efektif, serta penegakan hukum yang tegas untuk mencegah terjadinya penyalahgunaan data pribadi nasabah dan menjaga kepercayaan masyarakat terhadap layanan perbankan digital.

Dengan demikian, pertanggungjawaban hukum bank konvensional memiliki peran penting dalam menjaga kepercayaan masyarakat terhadap sistem perbankan. Melalui mekanisme tanggung jawab perdata, administratif, dan pidana, bank diharapkan mampu menjalankan prinsip kehati-hatian serta memberikan perlindungan hukum yang memadai bagi nasabah dalam menghadapi berbagai risiko yang muncul dalam perkembangan teknologi dan sistem keuangan modern.

Efektivitas Mekanisme Penyelesaian Sengketa

Perkembangan teknologi digital dalam sektor perbankan meningkatkan efisiensi operasional dan mempermudah nasabah bertransaksi melalui layanan seperti *mobile banking, internet banking,* dan sistem pembayaran digital. Transformasi ini mendorong integrasi teknologi informasi untuk meningkatkan kualitas layanan, namun juga menimbulkan risiko keamanan siber, kebocoran data pribadi, serta kebutuhan investasi besar pada infrastruktur teknologi, sehingga diperlukan tata kelola dan sistem keamanan yang memadai (Eka Indrayani, 2025). Di era digital, kejahatan perbankan semakin kompleks seiring perkembangan teknologi informasi. Modus seperti *phishing, carding,* dan *skimming* memanfaatkan celah keamanan sistem maupun kelalaian nasabah untuk memperoleh data penting seperti PIN, kata sandi, dan kode OTP sehingga pelaku dapat mengakses rekening dan melakukan transaksi ilegal. Oleh karena itu, diperlukan peningkatan keamanan sistem perbankan, pengawasan yang lebih ketat, serta literasi digital masyarakat dalam menggunakan layanan perbankan elektronik (Maria Tesalonika Bawintil, 2026). Digitalisasi perbankan melalui sistem elektronik memberikan kemudahan

dan efisiensi layanan, namun juga menimbulkan risiko penyalahgunaan data pribadi, kebocoran informasi, dan akses tidak sah terhadap sistem perbankan. Risiko tersebut dapat merugikan nasabah dan menurunkan kepercayaan masyarakat, sehingga diperlukan perlindungan hukum yang kuat, termasuk pengaturan perlindungan data pribadi, kewajiban bank menjaga keamanan data, serta mekanisme penyelesaian sengketa yang efektif (Muhammad Faisal Aziz, 2025).

Mekanisme pertama yang dapat ditempuh oleh nasabah adalah *internal dispute resolution* (IDR) atau penyelesaian sengketa secara internal di bank. Mekanisme pengaduan nasabah di bank merupakan bentuk penyelesaian sengketa secara internal yang wajib disediakan oleh setiap bank untuk menampung dan menindaklanjuti keluhan nasabah. Proses ini bertujuan memberikan penyelesaian secara cepat, efisien, dan sederhana sebelum sengketa berkembang ke proses hukum yang lebih formal (Subaidah Ratna Juita, 2023). Dalam praktiknya, bank memiliki kewajiban untuk menerima pengaduan nasabah, melakukan investigasi, dan memberikan tanggapan atau penyelesaian dalam jangka waktu tertentu sesuai dengan ketentuan perlindungan konsumen sektor jasa keuangan. Mekanisme ini merupakan bagian dari sistem perlindungan hukum bagi nasabah sebelum sengketa diselesaikan melalui lembaga eksternal (Ririn Puspita Dewi, 2024). Meskipun penyelesaian sengketa secara internal di bank dimaksudkan untuk memberikan penyelesaian yang cepat dan efisien, dalam praktiknya masih terdapat berbagai kendala, seperti ketidakseimbangan posisi antara bank dan nasabah serta kesulitan pembuktian dalam kasus kejahatan siber yang melibatkan sistem teknologi perbankan (Maria Tesalonika Bawintil, 2026).

Apabila penyelesaian sengketa melalui mekanisme internal bank tidak mencapai kesepakatan, nasabah dapat menempuh penyelesaian melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK) sebagai forum penyelesaian sengketa di luar pengadilan. Lembaga ini menyediakan mekanisme mediasi, ajudikasi, dan arbitrase yang bertujuan memberikan proses penyelesaian yang lebih sederhana, cepat, dan berbiaya ringan dibandingkan litigasi. Keberadaannya merupakan bagian dari sistem perlindungan konsumen di sektor jasa keuangan yang difasilitasi oleh Otoritas Jasa Keuangan guna memberikan akses penyelesaian sengketa yang lebih efektif bagi masyarakat (Ni'ma Ulinihayati, 2022). Dalam kajiannya, Kharisma (2021) menjelaskan bahwa pembentukan LAPS SJK dilatarbelakangi oleh kebutuhan akan mekanisme penyelesaian sengketa yang lebih efisien di sektor jasa keuangan, khususnya dalam menghadapi perkembangan teknologi keuangan yang semakin kompleks. LAPS SJK berfungsi sebagai forum alternatif yang mampu memberikan penyelesaian sengketa secara lebih cepat dan fleksibel dibandingkan proses peradilan, sekaligus memperkuat perlindungan konsumen melalui prosedur penyelesaian yang lebih sederhana dan terjangkau. Sementara itu, Rafika (2022) menegaskan bahwa mekanisme penyelesaian sengketa melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK) memberikan kesempatan bagi konsumen jasa keuangan untuk memperoleh keadilan yang lebih seimbang karena prosesnya dilakukan oleh pihak independen yang kompeten di bidang jasa keuangan. Melalui mekanisme ini, sengketa antara nasabah dan lembaga jasa

keuangan dapat diselesaikan secara profesional tanpa melalui proses peradilan yang memerlukan waktu lebih lama, sehingga diharapkan mampu meningkatkan efektivitas perlindungan hukum bagi konsumen di sektor jasa keuangan.

Nasabah yang mengalami kerugian akibat transaksi perbankan, termasuk akibat kejahatan siber, dapat menempuh jalur litigasi dengan mengajukan gugatan perdata terhadap bank. Gugatan tersebut dapat didasarkan pada wanprestasi apabila bank tidak memenuhi kewajiban kontraktualnya, atau pada perbuatan melawan hukum apabila terdapat kelalaian bank dalam menjaga keamanan sistem perbankan serta melindungi dana dan data pribadi nasabah (Subaidah Ratna Juita, 2023). Melalui mekanisme gugatan perdata di pengadilan, nasabah dapat menuntut ganti kerugian atas kerugian yang dialaminya akibat kejahatan siber di sektor perbankan. Tuntutan tersebut dapat meliputi kerugian materiil berupa hilangnya dana nasabah maupun kerugian immateriil yang timbul akibat terganggunya rasa aman dan kepercayaan nasabah terhadap sistem perbankan (Maria Tesalonika Bawintil, 2026). Meskipun jalur litigasi memberikan kepastian hukum melalui putusan pengadilan, proses penyelesaian sengketa melalui pengadilan pada umumnya membutuhkan waktu yang relatif lama serta biaya yang cukup besar. Kondisi tersebut seringkali menjadi pertimbangan bagi nasabah untuk memilih mekanisme penyelesaian sengketa di luar pengadilan terlebih dahulu sebelum menempuh jalur litigasi (Pahrudin Azis, 2024). Dengan demikian, dalam menghadapi perkembangan digitalisasi perbankan yang diiringi meningkatnya risiko kejahatan siber, diperlukan sistem perlindungan hukum yang efektif bagi nasabah melalui penguatan keamanan sistem perbankan serta penyediaan mekanisme penyelesaian sengketa yang berjenjang, baik melalui penyelesaian internal bank, melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan, maupun melalui jalur litigasi di pengadilan, guna menjamin perlindungan hak dan kepastian hukum bagi konsumen di sektor jasa keuangan.

Studi Kasus

Perkembangan teknologi informasi dalam sektor perbankan mendorong penggunaan layanan digital seperti internet banking yang memudahkan nasabah melakukan berbagai transaksi keuangan secara cepat dan efisien. Namun, di balik kemudahan tersebut terdapat risiko keamanan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Hal ini terlihat dalam penelitian yang dilakukan oleh (Nida Rafa Arofah, 2020) mengenai penggunaan internet banking pada nasabah PT. Bank Rakyat Indonesia (Persero) Tbk Kantor Cabang Tegal. Penelitian tersebut menjelaskan bahwa internet banking memungkinkan nasabah melakukan transaksi seperti transfer dana, pengecekan saldo, dan pembayaran tagihan secara online tanpa harus datang ke bank atau ATM. Meskipun demikian, penggunaan teknologi berbasis internet juga membuka peluang terjadinya cyber crime, seperti akses ilegal terhadap akun nasabah, pencurian data pribadi, hingga pembobolan rekening. Data sensitif seperti nomor rekening, PIN, dan informasi kartu kredit sering menjadi sasaran pelaku untuk memperoleh keuntungan secara ilegal. Hasil penelitian menunjukkan bahwa penggunaan internet banking memiliki pengaruh positif dan signifikan terhadap terjadinya cyber crime dengan koefisien regresi sebesar

0,261, yang menunjukkan bahwa peningkatan penggunaan internet banking dapat meningkatkan potensi terjadinya kejahatan siber. Fenomena tersebut juga tercermin dalam kasus hilangnya dana nasabah pada aplikasi perbankan digital Jenius milik BTPN akibat tindakan phishing sebagaimana dibahas oleh (Yosefine, 2023). Kasus ini bermula ketika nasabah menerima panggilan dari pihak yang mengaku sebagai layanan pelanggan Jenius dan diminta mengakses tautan tertentu terkait pembaruan kartu debit. Karena menyerupai komunikasi resmi bank, nasabah mengikuti instruksi tersebut dan memasukkan data yang diminta. Setelah itu akun nasabah keluar dari sistem dan tidak dapat diakses kembali, sementara dana dalam rekening telah dipindahkan ke rekening lain tanpa sepengetahuan pemiliknya. Tindakan tersebut termasuk kejahatan siber berupa phishing, yaitu upaya memperoleh informasi sensitif seperti username, password, atau PIN melalui situs atau komunikasi palsu yang menyerupai pihak resmi. Data yang diperoleh kemudian digunakan untuk mengakses akun korban dan melakukan transaksi ilegal. Dalam kasus ini, pihak bank menyediakan mekanisme pengaduan dan melakukan investigasi untuk mengetahui penyebab kerugian, serta meningkatkan sistem keamanan guna mencegah kejadian serupa di masa mendatang.

Simpulan

Berdasarkan keseluruhan pembahasan, dapat disimpulkan bahwa transformasi digital dalam perbankan konvensional membawa implikasi ganda berupa peningkatan efisiensi layanan sekaligus eskalasi risiko kejahatan siber yang semakin kompleks, sehingga menuntut penguatan perlindungan hukum bagi nasabah secara komprehensif. Meskipun kerangka regulasi di Indonesia telah relatif memadai melalui pengaturan mengenai prinsip kehati-hatian, perlindungan konsumen, dan perlindungan data pribadi, implementasinya masih menghadapi berbagai kendala, seperti lemahnya keamanan sistem, rendahnya literasi digital masyarakat, serta belum optimalnya efektivitas mekanisme penyelesaian sengketa. Kondisi ini menunjukkan bahwa perlindungan hukum tidak hanya bergantung pada norma yang ada, tetapi juga pada efektivitas penegakan dan kesiapan institusi dalam merespons dinamika kejahatan siber. Oleh karena itu, diperlukan langkah strategis berupa peningkatan investasi bank dalam sistem keamanan siber, penguatan pengawasan oleh regulator, serta intensifikasi edukasi kepada nasabah terkait keamanan digital. Selain itu, optimalisasi mekanisme penyelesaian sengketa, baik melalui jalur internal maupun alternatif seperti LAPS SJK, perlu terus didorong agar lebih responsif dan berkeadilan. Untuk penelitian selanjutnya, disarankan dilakukan kajian empiris yang menguji efektivitas implementasi regulasi dan praktik penyelesaian sengketa di lapangan, serta pengembangan model perlindungan hukum yang adaptif terhadap perkembangan teknologi dan pola kejahatan siber di sektor perbankan.

Referensi

Andriani, D., Haris, A., & Sumardi. (2025). Strategi keamanan transaksi elektronik dalam pelayanan publik berbasis e-government. *PENA Bangsa: Bisnis dan Tata Kelola Publik Adaptif*, 1(2), 134–147. https://doi.org/10.69616/pb.v1i2.563

Ariningsih, N. D., Pamungkas, Z. B., & Lestari, T. I. (2023). Perlindungan hukum terhadap konsumen pengguna jasa perbankan. Fakultas Hukum Universitas Duta Bangsa Surakarta.

Asmaru Amru, N. A. (2025). Perlindungan Hukum Terhadap Penanggulangan Kejahatan Siber Di Sektor Perbankan Digital Indonesia. *Journal of Scientech Research and Development, 7*(1), 586-598.

Azis, A., & Redi, A. (2025). Kejahatan siber dalam sektor perbankan dan perlindungan hukum terhadap nasabah. *Jurnal Hukum dan Teknologi Informasi,* 5(1), 1–10.

Azizah, R., Anggraeni, R., & Mustika, Y. S. B. (2022). Peran perlindungan konsumen dalam era digitalisasi perbankan bagi konsumen. *Locus Journal of Academic Literature Review,* 1(8), 465

Bahram, M., et al. (2024). Kejahatan digital dan upaya pencegahannya di era teknologi informasi. *SENTRI: Jurnal Riset Ilmiah*, 1737–1745.

Bank Indonesia. (2023). Pelindungan data pribadi di Bank Indonesia dan lembaga jasa keuangan. https://www.bi.go.id/id/publikasi/kajian/Pages/Pelindungan-Data-Pribadi-Di-Bank-Indonesia-Dan-Lembaga-Jasa-Keuangan.aspx

Benuf, K., & Azhar, M. (2020). Metodologi penelitian hukum sebagai instrumen mengurai permasalahan hukum kontemporer. Gema Keadilan, 7(1), 20-33.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan hukum terhadap nasabah atas kejahatan phising dan hacking pada layanan bank digital ditinjau berdasarkan hukum positif Indonesia. Hakim: Jurnal Ilmu Hukum dan Sosial, 3(1), 1-16.

Eka Indrayani, S. B. (2025). Peran Digitalisasi dalam Meningkatkan Kinerja Perbankan di Era Transformasi Teknologi. *PESHUM: Jurnal Pendidikan, Sosial dan Humaniora, 4*(3), 4835-4842.

Farahdiva, A. T., Mulyana, S. L., & Asri, T. P. (2025). Implementasi cyber security dalam sistem transaksi keuangan digital. *Jurnal Ilmiah Ekonomi Manajemen Bisnis dan Akuntansi (JEMBA),* 2(4), 276–289. https://doi.org/10.61722/jemba.v2i4.1157

Harahap, M. D. S., Saidin, O. K., Sukarja, D., & Leviza, J. (2022). Yurisdiksi LAPS dalam penyelesaian sengketa konsumen sektor jasa keuangan.

Habibi, Miftakhur Rokhman dan Isnatul Liviani. (2020). Kejahatan Teknologi Informasi (*Cyber Crime*) dan Penanggulangannya dalam Sistem Hukum Indonesia.

Hapsari, Rian Dwi dan Kuncoro Galih Pambayun. (2023). Ancaman Cybercrime di Indonesia: Sebuah Tinjauan Pustaka Sistematis.

Keliat, V. U. (2024). Peran regulasi terkini dalam mengatasi tantangan hukum perbankan di era digital. *Jurnal Ilmiah* (Nama Jurnal tidak tercantum dalam file), 323-330.

Kemal Idris Balaka, A. R. (2024). Pencurian Informasi NasabahDi Sektor Perbankan: Ancaman Serius Di Era Digital. *Yustitiabelen, 10*(2), 105-130.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2017). Riset kesadaran keamanan siber di masyarakat masih rendah. https://www.kominfo.go.id/content/detail/9992/riset-kesadaran-keamanan-siber-di-masyarakat-masih-rendah/0/sorotan_media

Kharisma, D. B. (2021). Tantangan LAPS Sektor Jasa Keuangan Sebagai Alternatif Penyelesaian Sengketa Di Sektor Financial Technology. *PERSPEKTIF, 26*(3), 216-220.

Mahendra, Yustika Citra dan Ni Komang Desy Setiawati Arya Pinatih. (2023). Strategi Penanganan Keamanan Siber di Indonesia.

Maria Tesalonika Bawintil, F. P. (2026). Perlindungan Hukum Nasabah Bank Terhadap Tindak Pidana Penipuan Dan Pencurian Data Nasabah Perbankan Melalui Modus Siber Dan Elektronik. *Lex Crimen Jurnal Fakultas Hukum Unsrat, 14*(4), 1-11.

Muhammad Faisal Aziz, H. S. (2025). Perlindungan Hukum terhadap Nasabah atas Penyalahgunaan Data Pribadi oleh Pihak Bank di Era Digitalisasi Perbankan. *Al-Zayn: Jurnal Ilmu Sosial & Hukum, 3*(6), 8840-8852.

Ni'ma Ulinihayati, Y. H. (2022). Penyelesaian Sengketa Perasuransian Melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK). *JURNAL MASALAH-MASALAH HUKUM, 51*(3), 209-221.

Nida Rafa Arofah, Y. P. (2020). INTERNET BANKING DAN CYBER CRIME : SEBUAH STUDI KASUS DI PERBANKAN NASIONAL. *Jurnal Pendidikan Akuntansi Indonesia, 18*(2), 107-119.

Otoritas Jasa Keuangan. (2024). OJK imbau nasabah waspadai penipuan SMS menggunakan OTP. https://rakyat.news/read/134879/ojk-imbau-nasabah-waspadai-penipuan-sms-menggunakan-otp

Pahrudin Azis, M. K. (2024). Perbandingan Lembaga Penyelesaian Sengketa: Litigasi Dan Non-Litigasi. *Qanuniya : Jurnal Ilmu Hukum, 1*(2), 12-21.

Pesak, V. Y., Tampongangoy, G. H., & Korua, J. M. (2024). Tanggung jawab hukum bank umum atas risiko layanan digital berdasarkan peraturan Otoritas Jasa Keuangan. *OPTIMAL: Jurnal Ekonomi dan Manajemen,* 4(2), 221–233. https://doi.org/10.55606/optimal.v4i2.3489

Prayuti, Y. (2024). Dinamika perlindungan hukum konsumen di era digital: Analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di Indonesia. *Jurnal Interpretasi Hukum,* 5(1), 903–913. https://doi.org/10.55637/juinhum.5.1.8482.903-913

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan online dalam media sosial: Pentingnya perlindungan data pribadi di era digital (Studi kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1). https://doi.org/10.35870/jpni.v6i1.1097

Rafika, R. (2022). Penyelesaian Sengketa Asuransi Melalui Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan. *SALAM: Jurnal Sosial dan Budaya Syar-i, 9*(4), 1209-1222.

Ramadhani, R., & Yudhayana, S. W. (2025). Implementasi prinsip kehati-hatian dalam praktik kredit perbankan: Tinjauan yuridis terhadap tanggung jawab bank. *Jurnal Hukum*, 1(1).

Republik Indonesia. (1999). *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*.

Republik Indonesia. (1998). *Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan*.

Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.

Ririn Puspita Dewi, D. W. (2024). Perlindungan Hukum Nasabah atas Peretasan Data Pribadi ditinjau dari Undang Undang. *Jurnal Riset Ilmu Hukum (JRIH), 4*(2), 95-100.

Riyanto, D. Z. (2023). Perlindungan hukum dan HAM terhadap nasabah bank korban cyber crime dalam internet banking berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik (Tesis magister, Universitas Darul Ulum Islamic Centre Sudirman GUPPI).

Rizkia, N. D., & Fardiansyah, H. (2023). Metode penelitian hukum (Normatif dan empiris). Widina Media Utama.

Salsabila, N., & Ilmih, A. A. (2024). Analisis kejahatan siber pada layanan perbankan digital dan perlindungan hukum nasabah. *Al-Adalah: Jurnal Hukum dan Politik Islam*, 2(4), 176–181.

Sari, S. A., Fardiansyah, A. I., & Tamza, F. B. (2025). Analisis normatif aspek yuridis tindak pidana perbankan sebagai bentuk kejahatan ekonomi. Justicia Sains: Jurnal Ilmu Hukum, 10(2), 519-528.

Setiawan, R. (2024). Cybercrime dalam sistem perbankan digital dan upaya penanggulangannya. *Jurnal Teknologi Informasi dan Hukum,* 3(2), 45–53.

Simatangkir, D. W. E., Nur Afifah, E. F., & Faliha, N. S. (2025). Keamanan siber dalam perbankan serta tantangan dan solusi di era digital. *Jurnal Multidisiplin Ilmu Akademik,* 2(1), 33–42. https://doi.org/10.61722/jmia.v2i1.3119

Subaidah Ratna Juita, D. I. (2023). PerlindunganHukumTerhadap Nasabah Bank Korban Kejahatan Skimming. *Jurnal USM Law Review, 6*(1), 407-419.

Syafa Widya Annafa, H. P. (2024). Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah. *Jurnal Multidisiplin Ilmu Akademik, 1*(6), 129-135.

Utomo, S., Ramadoni, S. R., dkk. (2024). Perlindungan hukum terhadap data nasabah dari serangan siber di sektor perbankan. *RENATA Jurnal Pengabdian Masyarakat Kita Semua, 2*(2), 165-172.

Wiraguna, S. A. (2024). Metode normatif dan empiris dalam penelitian hukum: Studi eksploratif di Indonesia. *Public Sphere: Jurnal Sosial Politik, Pemerintahan dan Hukum, 3*(3), 57-65.

Yosefine, R. S. (2023). Perlindungan Hukum terhadap Nasabah BTPN Jenius akibat Tindakan Phishing (Studi Kasus Bank Tabungan Pensiunan Nasional Jenius). *YUSTISIA TIRTAYASA : JURNAL TUGAS AKHIR, 3*(1), 57-72.

Zainuddin, M., & Karina, A. D. (2023). Penggunaan metode yuridis normatif dalam membuktikan kebenaran pada penelitian hukum. *Smart Law Journal, 2*(2), 114-123.