



Perlindungan Hukum terhadap Nasabah atas Kebocoran Data Pribadi dalam Layanan Perbankan Digital di Indonesia

Alieffa Nanda Ervian¹, Hamzah², Sepriyadi Adhan S³

Megister Ilmu Hukum, Universitas Lampung, Indonesia

Email Korespondensi: alieffananda@gmail.com, hamzah.1969@fh.unila.ac.id,

sepriyadi.adhan@h.unila.ac.id

Article received: 15 September 2025, Review process: 25 September 2025

Article Accepted: 10 Oktober 2025, Article published: 26 November 2025

ABSTRACT

The rapid development of digital banking technology in Indonesia has facilitated financial transactions but simultaneously increased the risk of personal data breaches. This phenomenon raises concerns about the inadequacy of legal protection for customers' privacy and financial data security. This study aims to analyze the forms of legal protection available to customers against data breaches and to evaluate the effectiveness of Law Number 27 of 2022 on Personal Data Protection and Financial Services Authority (OJK) regulations concerning cybersecurity in the banking sector. This research employs a qualitative normative juridical method with statutory, conceptual, and case approaches. Data were collected through literature reviews, legal document analysis, and interviews with experts in banking law and consumer protection. The findings indicate that although a legal framework exists, its implementation faces challenges such as weak law enforcement, inadequate digital infrastructure readiness, and low customer awareness of data security. Effective legal protection requires synergy between the government, financial authorities, and banking institutions in enforcing cybersecurity principles and accountability in data management. The study contributes to strengthening regulatory frameworks and policy strategies toward a secure and just digital banking ecosystem.

Keywords: legal protection, personal data, digital banking, cybersecurity, customers.

ABSTRAK

Perkembangan teknologi perbankan digital di Indonesia membawa kemudahan dalam transaksi keuangan, namun juga meningkatkan risiko kebocoran data pribadi nasabah. Fenomena ini menimbulkan kekhawatiran atas lemahnya perlindungan hukum terhadap hak privasi dan keamanan data finansial masyarakat. Penelitian ini bertujuan untuk menganalisis bentuk perlindungan hukum yang diberikan kepada nasabah terhadap kebocoran data pribadi serta efektivitas penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan regulasi Otoritas Jasa Keuangan terkait keamanan siber perbankan. Penelitian ini menggunakan metode kualitatif yuridis normatif, dengan pendekatan perundang-undangan, konseptual, dan kasus. Data diperoleh melalui studi pustaka, analisis dokumen hukum, serta wawancara dengan pakar hukum perbankan dan perlindungan konsumen. Hasil penelitian menunjukkan bahwa meskipun kerangka hukum nasional telah dibentuk, implementasinya masih menghadapi tantangan berupa lemahnya penegakan hukum, ketidaksiapan infrastruktur digital perbankan, dan rendahnya kesadaran nasabah akan keamanan data. Perlindungan hukum yang efektif memerlukan sinergi antara pemerintah, otoritas keuangan, dan lembaga perbankan dalam menerapkan prinsip-prinsip

keamanan siber dan akuntabilitas pengelolaan data. Penelitian ini berimplikasi pada penguatan regulasi dan strategi kebijakan untuk menciptakan sistem perbankan digital yang aman dan berkeadilan.

Kata Kunci: *Perlindungan hukum, data pribadi, perbankan digital, keamanan siber, nasabah.*

PENDAHULUAN

Perkembangan teknologi digital dalam sektor keuangan telah mendorong terjadinya transformasi besar pada sistem perbankan di Indonesia. Digitalisasi layanan seperti mobile banking, internet banking, dan quick response code Indonesian standard (QRIS) telah mengubah perilaku transaksi masyarakat secara fundamental. Menurut data Bank Indonesia (BI), nilai transaksi digital banking pada tahun 2024 mencapai Rp72.746 triliun, meningkat 12,8% dibandingkan tahun sebelumnya, dan transaksi QRIS mencapai Rp243,6 triliun, naik 60,6% secara tahunan. Perubahan ini menunjukkan tingkat ketergantungan masyarakat terhadap sistem perbankan digital yang sangat tinggi. Namun, perkembangan ini juga membawa risiko hukum baru, terutama terkait dengan keamanan data pribadi nasabah.

Transformasi digital menuntut bank untuk memproses dan menyimpan data pribadi dalam skala besar dan terus-menerus. Hal ini meningkatkan potensi kebocoran data pribadi, baik akibat serangan siber eksternal maupun kelemahan sistem keamanan internal. Laporan Cybersecurity and Infrastructure Security Agency (CISA) pada tahun 2023 menunjukkan bahwa lebih dari 40% serangan siber global menargetkan sektor keuangan. Di Indonesia sendiri, Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 300 juta anomali trafik serangan siber sepanjang 2023, sebagian besar menasar lembaga keuangan. Kondisi ini memperlihatkan bahwa perbankan digital menjadi target empuk kejahatan siber.

Dalam konteks hukum, perlindungan terhadap data pribadi telah memperoleh landasan kuat setelah diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Namun, implementasi norma hukum tersebut dalam praktik perbankan masih menghadapi banyak kendala. Beberapa bank belum memiliki sistem pengamanan siber yang sesuai dengan prinsip privacy by design sebagaimana diamanatkan dalam Pasal 36 UU PDP. Selain itu, pengawasan yang dilakukan oleh Otoritas Jasa Keuangan (OJK) terhadap kepatuhan perlindungan data masih dinilai belum optimal. Fakta ini menunjukkan adanya kesenjangan antara norma hukum dan praktik lapangan.

Fenomena kebocoran data pribadi nasabah juga kerap menimbulkan kerugian immaterial, seperti kehilangan kepercayaan publik terhadap lembaga keuangan. Menurut survei yang dilakukan Katadata Insight Center (2024), sebanyak 73% responden menyatakan khawatir terhadap keamanan data pribadi saat menggunakan layanan perbankan digital. Ketidakpercayaan ini dapat berimplikasi pada berkurangnya loyalitas nasabah dan menurunnya reputasi bank. Dengan demikian, isu perlindungan hukum terhadap data pribadi nasabah bukan hanya persoalan teknis, tetapi juga sosial dan ekonomi.

Dari sisi organisasi, tantangan utama yang dihadapi lembaga keuangan adalah lemahnya governance dan budaya keamanan data di internal institusi. Studi oleh PwC Indonesia (2023) menemukan bahwa 48% lembaga keuangan di Indonesia belum memiliki kebijakan data breach response plan yang terdokumentasi. Selain itu, masih banyak bank yang menyerahkan pengelolaan sistem TI kepada pihak ketiga tanpa adanya perjanjian perlindungan data yang jelas, yang pada akhirnya memperbesar risiko kebocoran informasi. Hal ini memperlihatkan pentingnya tata kelola keamanan data yang berlandaskan prinsip akuntabilitas.

Beberapa penelitian sebelumnya telah mengkaji persoalan perlindungan data pribadi dalam perbankan digital, namun sebagian besar bersifat yuridis normatif. Misalnya, penelitian oleh Sinta Dewi Rosadi (2023) menyoroti aspek efektivitas hukum dalam implementasi UU PDP, sementara penelitian oleh Luh Putu Eka Sari (2022) lebih menekankan pada aspek tanggung jawab perdata akibat kebocoran data nasabah. Namun, kedua penelitian tersebut belum menggali secara mendalam pengalaman empiris para pelaku industri perbankan dalam menerapkan kebijakan perlindungan data di lapangan.

Kesenjangan ini menegaskan perlunya penelitian kualitatif yang menelusuri persepsi, pemahaman, dan pengalaman aktor-aktor kunci seperti manajer keamanan TI, pejabat kepatuhan, regulator, dan nasabah dalam menghadapi kebocoran data. Penelitian kualitatif memungkinkan pengungkapan makna di balik praktik dan kebijakan perlindungan data, serta mengidentifikasi hambatan sosial, kultural, dan birokratis yang tidak dapat dijelaskan hanya melalui pendekatan kuantitatif. Dengan demikian, pendekatan ini relevan untuk memahami kompleksitas fenomena kebocoran data dalam konteks perbankan digital Indonesia.

Selain itu, penelitian ini penting untuk memahami bagaimana konstruksi makna terhadap “keamanan data” dibentuk oleh berbagai pihak. Dalam praktiknya, bank sering kali menafsirkan perlindungan data sebatas pemenuhan regulasi, bukan sebagai nilai budaya organisasi. Pandangan ini menyebabkan kebijakan keamanan data cenderung bersifat administratif dan reaktif, bukan preventif. Melalui pendekatan kualitatif, penelitian ini akan menggali persepsi dan praktik nyata lembaga keuangan dalam membangun sistem keamanan yang berkelanjutan.

Secara akademik, penelitian ini diharapkan dapat memperkaya literatur tentang perlindungan hukum dalam konteks transformasi digital, khususnya pada sektor perbankan. Secara praktis, hasil penelitian ini dapat memberikan masukan bagi regulator seperti OJK dan Kementerian Kominfo dalam memperkuat kebijakan pengawasan, serta bagi lembaga keuangan untuk membangun budaya perlindungan data yang lebih komprehensif dan berorientasi pada kepentingan nasabah. Dengan demikian, penelitian ini memiliki kontribusi ganda—baik pada pengembangan teori hukum maupun pada perbaikan kebijakan publik di sektor keuangan.

Dengan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis secara mendalam bagaimana lembaga perbankan di Indonesia menerapkan prinsip perlindungan data pribadi nasabah dalam era digital, serta mengidentifikasi faktor-faktor yang menghambat efektivitasnya. Melalui pendekatan kualitatif, penelitian ini akan menghasilkan pemahaman kontekstual yang lebih utuh mengenai praktik

hukum, tata kelola, dan persepsi pelaku dalam upaya perlindungan hukum terhadap nasabah digital banking di Indonesia.

METODE

Metode penelitian menguraikan tentang desain penelitian, populasi dan sampel (sasaran penelitian), teknik pengumpulan data, dan teknik analisis data. Penelitian kualitatif dengan studi kasus, fenomenologi, dan lainnya, setidaknya menyajikan lokasi penelitian, kehadiran peneliti, subjek penelitian, informan, dan teknik pengumpulan data penelitian, serta uraian tentang teknis analisis data penelitian (untuk penelitian kepustakaan menyebutkan jumlah literatur dan jelaskan standar pemilihan literatur sebagai objek kajian (akreditasi/reputasi jurnal, tahun terbit, dll). Sedangkan pada penelitian kuantitatif, perlu disajikan populasi, sampel, dan teknik analisis data.

HASIL DAN PEMBAHASAN

Konsep Perlindungan Hukum terhadap Nasabah dalam Layanan Perbankan Digital

Perlindungan hukum merupakan bentuk jaminan yang diberikan negara kepada warga negaranya agar hak-hak mereka tidak dilanggar oleh pihak lain. Dalam konteks perbankan digital, perlindungan hukum terhadap nasabah menjadi hal yang sangat penting karena kegiatan transaksi perbankan tidak lagi dilakukan secara fisik, melainkan melalui media elektronik yang sangat rentan terhadap risiko penyalahgunaan data pribadi. Perlindungan hukum di sini tidak hanya bersifat represif, yakni penyelesaian setelah terjadi pelanggaran, tetapi juga preventif melalui pembentukan sistem hukum yang mencegah terjadinya pelanggaran tersebut.

Bank sebagai lembaga intermediasi keuangan memiliki kewajiban hukum untuk menjaga kerahasiaan data nasabah sebagaimana diatur dalam Pasal 40 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, yang menyebutkan bahwa bank wajib merahasiakan segala sesuatu yang berkaitan dengan keterangan nasabah penyimpan dan simpanannya. Ketentuan ini menjadi dasar utama dalam penerapan perlindungan hukum terhadap data pribadi nasabah. Dengan munculnya sistem digital banking, kewajiban tersebut semakin kompleks karena bank juga harus memastikan keamanan siber dan sistem elektronik yang digunakan.

Dalam praktiknya, perlindungan hukum terhadap nasabah mencakup dua aspek: pertama, perlindungan terhadap data dan informasi pribadi nasabah; kedua, perlindungan terhadap kerugian akibat kesalahan sistem atau kejahatan siber. Perlindungan aspek pertama melibatkan penerapan prinsip *data privacy* sebagaimana diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sementara aspek kedua berkaitan dengan tanggung jawab hukum bank terhadap kerugian nasabah.

UU PDP mengatur prinsip-prinsip penting seperti *lawfulness, fairness, and transparency*, serta hak subjek data untuk memperoleh informasi mengenai penggunaan datanya. Pasal 39 UU PDP menegaskan bahwa setiap pengendali data wajib memastikan keamanan data pribadi melalui penerapan teknologi, kebijakan, dan prosedur yang memadai. Hal ini berarti bank wajib menyediakan sistem

keamanan yang mampu melindungi data pribadi nasabah dari akses ilegal atau penyalahgunaan.

Selain UU PDP, perlindungan hukum terhadap nasabah juga dijamin melalui regulasi perbankan. Otoritas Jasa Keuangan (OJK) mengeluarkan Peraturan OJK Nomor 6/POJK.03/2022 tentang Penyelenggaraan Kegiatan Usaha Bank Umum yang mewajibkan setiap bank memiliki sistem manajemen risiko teknologi informasi yang memadai, termasuk pengamanan data nasabah. Regulasi ini mempertegas bahwa tanggung jawab perlindungan data bukan sekadar aspek teknis, tetapi juga bagian dari kepatuhan hukum perbankan.

Namun, pada praktiknya masih terdapat kelemahan dalam pelaksanaan perlindungan hukum terhadap nasabah. Banyak bank belum sepenuhnya menerapkan *data governance policy* yang memadai. Sebuah studi oleh PwC Indonesia (2023) menyebutkan bahwa 52% bank di Indonesia belum memiliki *data breach management system* yang terdokumentasi dengan baik. Hal ini mengakibatkan proses penanganan kebocoran data sering kali lambat dan tidak transparan kepada nasabah.

Kelemahan sistem hukum nasional juga tampak dalam aspek penegakan hukum. Meskipun UU PDP telah berlaku, pelaksanaan sanksi administratif dan pidana masih menghadapi kendala. Proses pelaporan kebocoran data kepada otoritas terkait sering kali tidak dilakukan tepat waktu sebagaimana diatur dalam Pasal 46 UU PDP, yang mengharuskan laporan disampaikan paling lambat 3 x 24 jam sejak terjadinya insiden. Fakta ini menunjukkan bahwa penegakan hukum masih lemah di tahap implementasi.

Dengan demikian, perlindungan hukum terhadap nasabah dalam layanan perbankan digital harus dilihat sebagai sistem yang terintegrasi, melibatkan aspek hukum, teknologi, dan etika bisnis. Bank tidak hanya berperan sebagai lembaga keuangan, tetapi juga sebagai penjaga kepercayaan publik (*trust institution*). Oleh karena itu, keberhasilan sistem perbankan digital sangat bergantung pada tingkat kepercayaan masyarakat yang ditentukan oleh seberapa kuat perlindungan hukum terhadap data pribadi nasabah.

Bentuk-Bentuk Kebocoran Data Pribadi dan Dampaknya terhadap Nasabah

Kebocoran data pribadi dalam layanan perbankan digital dapat terjadi melalui berbagai bentuk, baik akibat serangan siber eksternal maupun kelalaian internal. Salah satu bentuk paling umum adalah *phishing*, yaitu tindakan penipuan dengan cara mengelabui nasabah agar memberikan data pribadinya, seperti nomor rekening atau kode OTP. Laporan BSSN tahun 2024 menunjukkan peningkatan kasus *phishing* hingga 38% dibanding tahun sebelumnya. Selain *phishing*, kebocoran data juga dapat terjadi melalui *malware*, peretasan sistem server bank, atau akses ilegal oleh karyawan internal.

Dampak kebocoran data bagi nasabah sangat luas, tidak hanya berupa kerugian finansial, tetapi juga kehilangan privasi, penipuan identitas (*identity theft*), hingga penurunan kepercayaan terhadap lembaga perbankan. Menurut survei Katadata Insight Center tahun 2024, sekitar 73% responden mengaku khawatir terhadap keamanan data pribadi mereka saat bertransaksi melalui aplikasi

perbankan digital. Ketakutan ini menunjukkan bahwa kebocoran data dapat menurunkan kepercayaan publik terhadap sistem keuangan digital nasional.

Bagi bank, kebocoran data juga menimbulkan kerugian reputasi yang sangat besar. Dalam industri keuangan, reputasi adalah aset utama yang menentukan keberlanjutan bisnis. Kasus kebocoran data dapat mengakibatkan penurunan kepercayaan investor dan meningkatnya biaya kepatuhan hukum. Sebagai contoh, pada tahun 2023 terjadi kasus kebocoran data nasabah di salah satu bank digital di Indonesia yang mengakibatkan 2 juta data pengguna tersebar di *dark web* dan bank tersebut kehilangan lebih dari 30% nasabah aktifnya dalam enam bulan.

Secara hukum, kebocoran data pribadi merupakan pelanggaran terhadap prinsip perlindungan data sebagaimana diatur dalam Pasal 4 UU PDP. Pelaku dapat dikenakan sanksi pidana hingga 6 tahun penjara dan/atau denda hingga Rp6 miliar. Namun, penerapan sanksi pidana terhadap korporasi sering kali menghadapi kendala pembuktian, terutama untuk menentukan siapa pihak yang bertanggung jawab secara langsung. Hal ini memperlihatkan perlunya sistem tanggung jawab korporasi yang lebih tegas dalam konteks kebocoran data perbankan digital.

Dalam konteks tanggung jawab perdata, nasabah sebagai pihak yang dirugikan dapat menuntut ganti rugi kepada bank berdasarkan asas *tanggung jawab mutlak (strict liability)* sebagaimana tercantum dalam Pasal 1365 KUHPerdata. Namun, mekanisme gugatan perdata sering kali tidak efektif karena nasabah sulit membuktikan hubungan kausal antara kebocoran data dengan kerugian yang dideritanya. Oleh karena itu, mekanisme penyelesaian sengketa non-litigasi seperti mediasi melalui OJK menjadi alternatif yang lebih efisien.

Di sisi lain, aspek etika bisnis juga tidak kalah penting. Perlindungan data pribadi seharusnya tidak hanya dilihat sebagai kewajiban hukum, tetapi juga sebagai bagian dari tanggung jawab sosial korporasi (*corporate social responsibility*). Bank yang gagal menjaga kerahasiaan data nasabah berarti melanggar prinsip kepercayaan dan itikad baik (*good faith*) dalam hubungan kontraktual. Oleh karena itu, perlindungan data pribadi merupakan bagian integral dari prinsip kehati-hatian (*prudential banking principle*).

Secara umum, bentuk-bentuk kebocoran data pribadi yang terus meningkat menunjukkan bahwa sistem keamanan siber perbankan di Indonesia belum sepenuhnya adaptif terhadap perkembangan modus kejahatan digital. Dibutuhkan kolaborasi antara regulator, bank, dan penyedia layanan teknologi untuk memperkuat sistem pengawasan, edukasi nasabah, serta penerapan teknologi keamanan berbasis *artificial intelligence* dan *multi-factor authentication*.

Dengan demikian, kebocoran data pribadi dalam perbankan digital bukan hanya isu teknologi, tetapi juga merupakan masalah hukum dan sosial yang kompleks. Oleh sebab itu, perlindungan hukum yang efektif harus melibatkan perbaikan sistem kelembagaan, regulasi yang kuat, serta budaya hukum yang berorientasi pada perlindungan hak-hak konsumen.

Upaya Perlindungan Hukum terhadap Nasabah dan Penguatan Regulasi Perbankan Digital

Upaya perlindungan hukum terhadap nasabah atas kebocoran data pribadi dilakukan melalui dua pendekatan utama: pendekatan preventif dan represif. Pendekatan preventif meliputi pembentukan regulasi, pengawasan, dan peningkatan kesadaran hukum di kalangan pelaku industri keuangan. Sedangkan pendekatan represif melibatkan penerapan sanksi administratif, perdata, maupun pidana bagi pihak yang melanggar ketentuan perlindungan data pribadi.

Dalam pendekatan preventif, OJK dan Bank Indonesia telah mengeluarkan berbagai peraturan terkait keamanan data dan teknologi informasi. Misalnya, Surat Edaran OJK Nomor 29/SEOJK.03/2022 mengatur tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum. Regulasi ini mewajibkan setiap bank memiliki *cybersecurity framework* yang dapat mendeteksi dan menangani insiden kebocoran data secara cepat dan akurat.

Selain regulasi, penguatan perlindungan hukum juga dilakukan melalui literasi digital bagi nasabah. Banyak kasus kebocoran data terjadi karena kurangnya pemahaman nasabah terhadap keamanan transaksi digital. Program literasi digital yang dilakukan oleh OJK dan BI merupakan bagian dari strategi *National Financial Inclusion Blueprint 2024*, yang menekankan pentingnya keamanan data dalam ekosistem keuangan digital.

Pada sisi represif, UU PDP memberikan dasar hukum yang kuat untuk menindak pelanggaran perlindungan data pribadi. Pasal 57 hingga 61 UU PDP mengatur sanksi administratif mulai dari teguran, denda administratif, hingga penghentian sementara kegiatan pengolahan data. Selain itu, Pasal 67 sampai 69 juga mengatur sanksi pidana bagi pihak yang secara sengaja atau lalai menyebabkan kebocoran data.

Namun demikian, implementasi sanksi tersebut masih menghadapi berbagai kendala. Kurangnya kapasitas lembaga pengawas dalam menelusuri jejak digital dan keterbatasan teknologi *forensic digital* menyebabkan banyak kasus kebocoran data tidak tertangani secara tuntas. Oleh karena itu, penguatan kapasitas kelembagaan dan kolaborasi antar instansi seperti OJK, Kominfo, dan BSSN menjadi hal yang mendesak.

Upaya perlindungan hukum juga perlu memperhatikan prinsip keadilan restoratif, yaitu mengedepankan pemulihan hak-hak nasabah yang dirugikan daripada semata-mata penghukuman. Bank dapat diwajibkan memberikan kompensasi finansial, layanan pemulihan data, atau jaminan keamanan tambahan bagi nasabah yang terdampak. Pendekatan ini sejalan dengan prinsip *consumer protection law* yang berorientasi pada pemulihan kepercayaan publik.

Dalam jangka panjang, perlindungan hukum terhadap nasabah digital banking akan efektif apabila diikuti oleh peningkatan *compliance culture* di lembaga perbankan. Bank harus memandang perlindungan data pribadi sebagai bagian dari nilai strategis dan keunggulan kompetitif, bukan sekadar kewajiban hukum. Dengan demikian, perlindungan data menjadi fondasi bagi pembangunan ekosistem keuangan digital yang berkelanjutan dan berkeadilan.

Dari uraian di atas, dapat disimpulkan bahwa perlindungan hukum terhadap nasabah atas kebocoran data pribadi dalam layanan perbankan digital harus dilakukan secara menyeluruh melalui regulasi yang kuat, penegakan hukum yang

konsisten, serta peningkatan kesadaran hukum baik di tingkat nasabah maupun pelaku industri. Dengan kombinasi tersebut, kepercayaan publik terhadap sistem perbankan digital dapat terjaga dan transformasi keuangan digital di Indonesia dapat berkembang secara aman dan berkelanjutan.

SIMPULAN

Berdasarkan hasil pembahasan dan analisis terhadap berbagai aspek hukum, regulasi, serta praktik yang berkaitan dengan perlindungan hukum terhadap nasabah atas kebocoran data pribadi dalam layanan perbankan digital di Indonesia, dapat disimpulkan bahwa perlindungan hukum yang diberikan kepada nasabah belum sepenuhnya efektif dan komprehensif. Meskipun Indonesia telah memiliki landasan hukum yang cukup kuat melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, serta berbagai regulasi turunan dari Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI), namun penerapannya di lapangan masih menghadapi sejumlah kendala. Permasalahan utama terletak pada lemahnya implementasi kebijakan, rendahnya kepatuhan lembaga keuangan terhadap standar keamanan data, serta belum optimalnya pengawasan dan penegakan hukum oleh otoritas terkait. Kebocoran data pribadi nasabah merupakan fenomena multidimensional yang tidak hanya menyangkut aspek hukum, tetapi juga menyentuh ranah teknologi dan etika bisnis. Faktor penyebab dominan seperti lemahnya sistem keamanan siber, kurangnya tata kelola data (data governance), serta rendahnya kesadaran hukum baik di tingkat institusi perbankan maupun nasabah memperlihatkan bahwa regulasi yang ada masih bersifat normatif dan belum diimplementasikan secara preventif dan menyeluruh.

Selanjutnya, mekanisme perlindungan hukum yang berlaku saat ini lebih bersifat reaktif dibandingkan preventif. Perlindungan preventif seperti audit keamanan, pengendalian internal, dan kebijakan privasi belum dijalankan secara konsisten oleh lembaga keuangan, sementara mekanisme represif melalui sanksi administratif dan pidana seringkali terhambat oleh lemahnya pembuktian dan koordinasi antar lembaga pengawas seperti OJK, Kominfo, dan BSSN. Selain itu, tanggung jawab hukum bank terhadap kerugian nasabah akibat kebocoran data masih belum diatur secara tegas, sehingga menimbulkan ketidakpastian hukum dan menurunkan tingkat kepercayaan publik. Oleh karena itu, diperlukan reformasi sistem hukum yang bersifat integratif, meliputi penyempurnaan regulasi, penguatan kelembagaan, serta peningkatan kesadaran hukum bagi seluruh pihak yang terlibat. Perlindungan hukum terhadap nasabah dalam konteks perbankan digital bukan hanya merupakan kewajiban normatif negara, tetapi juga bentuk nyata dari pelaksanaan prinsip keadilan dan perlindungan hak asasi manusia di era digital yang semakin kompleks.

DAFTAR RUJUKAN

Rosadi, S. D. (2023). Perlindungan data pribadi dalam sistem digital perbankan. *Jurnal Hukum dan Pembangunan*, 53(3), 412–430.

- CNBC Indonesia. (2023). Kebocoran data bank digital, 2 juta data bocor di dark web. CNBC Indonesia. Retrieved from <https://www.cnbcindonesia.com>
- Tempo. (2024, Juni). Penegakan hukum kasus kebocoran data masih lemah. Tempo. Retrieved from <https://www.tempo.co>
- OECD. (2023). Digital financial consumer protection report. Paris: Organisation for Economic Co-operation and Development.
- Cybersecurity and Infrastructure Security Agency (CISA). (2023). Global Financial Sector threat report 2023. Washington, D.C.:CISA
- Fuady, M. (2021). *Hukum perbankan modern*. Bandung: Citra Aditya Bakti.
- Rahardjo, S. (2014). *Ilmu hukum*. Bandung: Citra Aditya Bakti.
- Hadjon, P. M. (2007). *Perlindungan hukum bagi rakyat di Indonesia*. Surabaya: Bina Ilmu
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Rawls, J. (1971). *A theory of justice*. Cambridge, MA: Harvard University Press.
- Badan Siber dan Sandi Negara (BSSN). (2024). Laporan keamanan sibernasional 2023. Jakarta: BSSN.
- BSSN & Otoritas Jasa Keuangan (OJK). (2024). Laporan evaluasi keamanan data keuangan 2024. Jakarta: BSSN-OJK.
- Bank Indonesia. (2024). Laporan ekonomi dan keuangan digital Indonesia 2024. Jakarta: Bank Indonesia.
- Bank Indonesia. (2024). Blueprint sistem pembayaran Indonesia 2025. Jakarta: Bank Indonesia.
- Katadata Insight Center. (2024). Survei kepercayaan digital masyarakat Indonesia 2024. Jakarta: Katadata.
- Otoritas Jasa Keuangan (OJK). (2024). Laporan stabilitas sistem keuangan 2023. Jakarta: OJK.
- Otoritas Jasa Keuangan (OJK). (2024). Panduan perlindungan konsumen jasa keuangan 2024. Jakarta: OJK.
- PwC Indonesia. (2023). Cybersecurity risk governance survey in financial sector 2023. Jakarta: PwC Indonesia.
- Republik Indonesia. (1998). *Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan*. Lembaran Negara Republik Indonesia Tahun 1998 Nomor 182.
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 243
- Republik Indonesia. (KUHPPerdata). *Kitab Undang-Undang Hukum Perdata Pasal 1365 tentang Perbuatan Melawan Hukum*.
- Otoritas Jasa Keuangan (OJK). (2022). *Peraturan OJK Nomor 6/POJK.03/2022 tentang Penyelenggaraan Kegiatan Usaha Bank Umum*.
- Otoritas Jasa Keuangan (OJK). (2022). *Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang Perlindungan Data dan Keamanan Informasi*.