Ekopedia: Jurnal Ilmiah Ekonomi
Online ISSN 3089-8374
Vol. 1, No. 2, Juni 2025
doi.org/10.63822/qwcqac2
Hal. 120-129

Beranda Jurnal https://indojurnal.com/index.php/ekopedia

Perlindungan Hukum Nasabah Terhadap Penyalahgunaan Data Pribadi oleh Pihak Ketiga dalam Kerja Sama Perbankan Digital

Arya Salman Aziz[1], Muhammad Abyan Zaidan[2]
Universitas Negeri Semarang[1,2]

*Email:
aryasalman2016@students.unnes.ac.id; abyanmuhammad576@students.unnes.ac.id

Diterima: 06-05-2025 | Disetujui: 07-05-2025 | Diterbitkan: 08-05-2025

ABSTRACT

The development of information technology has driven the transformation of the banking sector towards digital services that are increasingly integrated with third parties, such as fintech and technology service providers. However, this collaboration poses potential risks to the protection of customers' personal data, especially in terms of misuse by third parties. This article discusses legal protection for digital banking customers against misuse of personal data by banking cooperation partners. The research method used is normative juridical with a statutory approach and case analysis. The results of the study show that although there are regulations such as the Personal Data Protection Law (UU PDP), the Banking Law, and OJK regulations, there are still legal gaps in supervision and legal responsibility for data leaks by third parties. Law enforcement also still faces challenges, such as low digital literacy of customers and limited effective complaint mechanisms. Therefore, it is necessary to strengthen regulations in the form of clear cooperation agreements between banks and third parties, increased supervision by authorities, and legal and digital education for customers. Personal data protection is an integral part of the right to privacy and must be guaranteed effectively in the ever-growing digital banking ecosystem.

Keywords: *Legal Protection, Personal Data, Customers, Digital Banking, Third Parties, Data Misuse, Regulation.*

ABSTRAK

Perkembangan teknologi informasi telah mendorong transformasi sektor perbankan menuju layanan digital yang semakin terintegrasi dengan pihak ketiga, seperti fintech dan penyedia layanan teknologi. Namun, kerja sama ini menimbulkan potensi risiko terhadap perlindungan data pribadi nasabah, terutama dalam hal penyalahgunaan oleh pihak ketiga. Artikel ini membahas perlindungan hukum bagi nasabah perbankan digital terhadap penyalahgunaan data pribadi oleh mitra kerja sama perbankan. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan analisis kasus. Hasil penelitian menunjukkan bahwa meskipun terdapat regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Perbankan, dan regulasi OJK, masih terdapat celah hukum dalam pengawasan dan tanggung jawab hukum atas kebocoran data oleh pihak ketiga. Penegakan hukum juga masih menghadapi tantangan, seperti rendahnya literasi digital nasabah dan keterbatasan mekanisme pengaduan yang efektif. Oleh karena itu, diperlukan penguatan regulasi dalam bentuk perjanjian kerja sama yang jelas antara bank dan pihak ketiga, peningkatan pengawasan oleh otoritas, serta edukasi hukum dan digital bagi nasabah. Perlindungan data pribadi merupakan bagian integral dari hak privasi dan harus dijamin secara efektif dalam ekosistem perbankan digital yang terus berkembang.

Keywords: Perlindungan Hukum, Data Pribadi, Nasabah, Perbankan Digital, Pihak Ketiga, Penyalahgunaan Data, Regulasi.

Bagaimana Cara Sitasi Artikel ini:

Arya Salman Aziz, & Muhammad Abyan Zaidan. (2025). Perlindungan Hukum Nasabah Terhadap Penyalahgunaan Data Pribadi oleh Pihak Ketiga dalam Kerja Sama Perbankan Digital. Ekopedia: Jurnal Ilmiah Ekonomi, 1(2), 120-129. https://doi.org/10.63822/qwcqac2

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan signifikan dalam layanan perbankan. Digitalisasi perbankan memungkinkan kemudahan akses layanan keuangan, efisiensi operasional, dan peningkatan pengalaman nasabah. Dalam proses transformasi ini, bank tidak jarang menjalin kerja sama dengan pihak ketiga, seperti perusahaan teknologi finansial (fintech), penyedia cloud service, hingga platform pihak ketiga lainnya yang terlibat dalam pengelolaan dan pemrosesan data pribadi nasabah.

Namun, di tengah kemajuan tersebut, muncul persoalan serius terkait perlindungan data pribadi nasabah. Data pribadi yang dikumpulkan dan diproses dalam ekosistem perbankan digital sangat rentan terhadap penyalahgunaan, terutama ketika melibatkan pihak ketiga yang tidak memiliki standar perlindungan data yang memadai. Beberapa kasus kebocoran dan penyalahgunaan data pribadi telah memunculkan kekhawatiran publik dan menguji efektivitas regulasi yang ada.

Perlindungan hukum terhadap data pribadi nasabah menjadi isu krusial, mengingat data merupakan aset penting yang berkaitan langsung dengan hak privasi. Oleh karena itu, penting untuk mengkaji sejauh mana perlindungan hukum yang diberikan kepada nasabah dalam konteks kerja sama antara perbankan digital dan pihak ketiga. Penelitian ini berfokus pada identifikasi celah regulasi, analisis tanggung jawab para pihak, serta rekomendasi untuk memperkuat perlindungan hukum bagi nasabah dalam ekosistem perbankan digital.

METODE PENELITIAN

Penelitian ini menggunakan metode yuridis normatif, yaitu pendekatan yang bertumpu pada analisis terhadap peraturan perundang-undangan, asas hukum, dan doktrin yang relevan dengan perlindungan data pribadi dalam konteks kerja sama perbankan digital dengan pihak ketiga. Pendekatan ini dipilih untuk menelaah kesesuaian dan efektivitas norma hukum yang berlaku dalam memberikan perlindungan kepada nasabah atas potensi penyalahgunaan data pribadi. Penelitian ini juga dilengkapi dengan pendekatan komparatif dan konseptual guna memperkaya analisis melalui perbandingan dengan sistem hukum di negara lain serta pemahaman teoritis mengenai hak privasi dan tanggung jawab hukum para pihak dalam ekosistem digital. Sumber data dalam penelitian ini terdiri dari bahan hukum primer, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan, serta peraturan Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI) yang mengatur kerja sama perbankan dengan pihak ketiga. Selain itu, digunakan juga bahan hukum sekunder berupa literatur, jurnal ilmiah, dan hasil penelitian sebelumnya. Teknik pengumpulan data dilakukan melalui studi kepustakaan (library research), sedangkan analisis data dilakukan secara deskriptif-analitis untuk menguraikan dan menilai implementasi norma hukum yang berlaku terhadap perlindungan data pribadi nasabah.

HASIL PEMBAHASAN

Bentuk Kerja Sama Antara Perbankan Digital dengan Pihak Ketiga yang Melibatkan Pengelolaan Data Pribadi Nasabah

Dalam era transformasi digital, perbankan digital kian memperluas jangkauan layanannya melalui kerja sama strategis dengan pihak ketiga, terutama dalam konteks pengelolaan data pribadi nasabah. Model kerja sama ini tidak hanya menjadi fondasi dari efisiensi operasional dan inovasi layanan, tetapi juga menjadi instrumen utama dalam mengakselerasi pertumbuhan ekosistem keuangan digital yang inklusif dan terintegrasi. Bentuk kerja sama ini sangat beragam, dan umumnya melibatkan pemrosesan, penyimpanan, dan penggunaan data nasabah sebagai bagian integral dari ekosistem layanan keuangan digital.

Salah satu bentuk yang paling umum adalah kerja sama melalui integrasi *Application Programming Interface* (API) dengan perusahaan teknologi finansial (fintech). Skema ini memungkinkan interkoneksi sistem antara bank dan pihak ketiga untuk mengakses data nasabah secara terbatas dan berbasis *real-time*, dengan syarat adanya persetujuan eksplisit dari nasabah. Layanan yang umumnya disediakan melalui skema ini meliputi manajemen keuangan pribadi (personal finance management), *credit scoring*, hingga identifikasi digital (digital identity verification) (Arner, Barberis & Buckley, 2017:12). API menjadi medium teknis yang efisien namun secara hukum menimbulkan tantangan pengawasan, mengingat integrasi lintas sistem ini sering kali dilakukan dalam waktu singkat dan melalui alur persetujuan yang tidak sepenuhnya dipahami oleh nasabah.

Selain itu, bank digital juga melakukan kerja sama dalam bentuk alih daya atau *outsourcing* pengelolaan data kepada penyedia layanan teknologi informasi, khususnya layanan komputasi awan (*cloud computing*). Kerja sama ini memberikan efisiensi dari sisi penyimpanan dan kecepatan pemrosesan data, sekaligus memperluas kapasitas infrastruktur digital perbankan tanpa harus membangun sistem sendiri. Dalam konteks ini, data nasabah dapat diproses dan disimpan oleh pihak ketiga yang memiliki infrastruktur teknologi tinggi, dengan tetap mengedepankan prinsip kerahasiaan, integritas, dan keamanan informasi sebagai bentuk kepatuhan terhadap prinsip keamanan data (*data security*) (Zetzsche et al., 2020:59). Namun demikian, ketergantungan terhadap sistem cloud publik atau multinasional yang berada di luar yurisdiksi nasional menimbulkan risiko tambahan, seperti kesulitan penegakan hukum lintas negara ketika terjadi pelanggaran atau insiden kebocoran data.

Tidak hanya itu, banyak bank juga menjalin kemitraan dengan penyedia layanan penilaian kredit digital untuk memanfaatkan *alternative data* dalam proses analisis kelayakan kredit. Data tersebut mencakup informasi dari luar sektor perbankan seperti riwayat transaksi e-commerce, perilaku media sosial, hingga pola penggunaan aplikasi digital oleh nasabah (Rachmawati, 2022:45). Meskipun pendekatan ini meningkatkan inklusi keuangan dengan menjangkau segmen yang tidak memiliki riwayat kredit formal, praktik ini juga menimbulkan kekhawatiran terkait prinsip minimalisasi data dan validitas dasar hukum pemrosesan data nasabah di luar layanan utama bank.

Perbankan digital juga menjalin kerja sama dengan platform e-commerce atau aplikasi digital lainnya, yang memungkinkan integrasi layanan perbankan langsung dalam aplikasi pihak ketiga. Contohnya adalah fitur pembukaan rekening digital, layanan dompet digital (*e-wallet*), hingga fasilitas pinjaman instan yang seluruhnya memanfaatkan data pribadi dan transaksi nasabah yang diolah bersama-sama oleh kedua belah pihak (Bank Indonesia, 2020). Integrasi ini merupakan manifestasi dari model *open*

banking berbasis *customer consent*, di mana nasabah memberikan persetujuan eksplisit agar datanya dapat diakses dan digunakan oleh pihak ketiga untuk layanan tertentu (Otoritas Jasa Keuangan, 2021). Namun dalam praktiknya, bentuk persetujuan ini sering kali bersifat "sekali klik", tanpa penjelasan yang rinci dan tersegmentasi, sehingga melemahkan esensi dari prinsip *informed consent* yang seharusnya dijunjung dalam pemrosesan data pribadi.

Namun demikian, bentuk kerja sama tersebut memunculkan tantangan hukum yang serius, terutama terkait tanggung jawab perlindungan data pribadi. Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta Peraturan Otoritas Jasa Keuangan (POJK) Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital, setiap bentuk kerja sama antara bank dan pihak ketiga yang melibatkan data nasabah wajib tunduk pada prinsip-prinsip perlindungan data, termasuk keabsahan dasar pemrosesan data, keamanan sistem, serta transparansi penggunaan data (UU No. 27 Tahun 2022: Pasal 20–26). Prinsip-prinsip ini mencakup keharusan adanya dasar hukum yang sah dalam pemrosesan, kejelasan dalam tujuan penggunaan data, serta kemampuan bank untuk mempertanggungjawabkan setiap proses pemrosesan data oleh mitra pihak ketiga.

Oleh karena itu, perbankan digital diwajibkan untuk memiliki perjanjian kerja sama tertulis yang mengatur hak dan kewajiban masing-masing pihak, termasuk mekanisme pengawasan dan audit terhadap penggunaan data pribadi nasabah (POJK No. 13/POJK.02/2018: Pasal 12 ayat (2)). Perjanjian ini berfungsi sebagai dasar hukum untuk memastikan bahwa pihak ketiga tunduk pada standar yang sama dalam perlindungan data sebagaimana yang diwajibkan kepada pengendali data. Selain itu, perjanjian tersebut seharusnya juga mencantumkan mekanisme *incident response* apabila terjadi insiden keamanan data, serta ketentuan ganti rugi yang adil bagi nasabah sebagai subjek data yang dirugikan.

Dengan demikian, meskipun kerja sama antara perbankan digital dan pihak ketiga memberikan efisiensi dan kemudahan layanan keuangan berbasis teknologi, perlindungan terhadap data pribadi nasabah tetap menjadi aspek krusial yang harus diatur secara ketat demi menjaga kepercayaan publik dan kepatuhan terhadap regulasi yang berlaku. Penguatan pengawasan oleh otoritas sektor jasa keuangan, harmonisasi regulasi antar sektor, serta edukasi berkelanjutan kepada nasabah mengenai hak-haknya atas data pribadi menjadi langkah strategis yang tidak dapat ditunda untuk menciptakan sistem keuangan digital yang aman, inklusif, dan berkeadilan.

Potensi Penyalahgunaan Data Pribadi Nasabah oleh Pihak Ketiga dalam Ekosistem Perbankan Digital

Perkembangan perbankan digital yang mengandalkan teknologi informasi dan kolaborasi dengan pihak ketiga dalam menyediakan layanan keuangan telah membuka peluang baru dalam optimalisasi data pribadi nasabah. Inovasi seperti mobile banking, layanan berbasis cloud, hingga integrasi dengan platform teknologi finansial (fintech) memungkinkan bank memberikan layanan yang lebih cepat, personal, dan efisien. Namun di balik kemajuan tersebut, terdapat risiko yang signifikan terhadap penyalahgunaan data pribadi, khususnya ketika data nasabah dikelola di luar kontrol langsung bank, yakni oleh mitra teknologi, penyedia aplikasi, atau perusahaan pihak ketiga yang terintegrasi dalam sistem digital bank. Risiko ini kian meningkat apabila tidak terdapat mekanisme pengawasan dan kontrol yang memadai dari bank terhadap pihak ketiga yang mengakses dan memproses data nasabah (Weichert, 2021).

Salah satu bentuk penyalahgunaan yang sering menjadi sorotan adalah pemanfaatan data pribadi nasabah untuk kepentingan komersial di luar tujuan perbankan, seperti profiling untuk iklan, penawaran pinjaman tanpa persetujuan, atau bahkan penjualan data ke pihak lain secara ilegal (Albrecht, 2016). Praktik ini biasanya terjadi karena adanya insentif ekonomi yang besar bagi penyedia teknologi atau pihak ketiga untuk mengeksplorasi data nasabah demi keuntungan bisnis. Hal ini dimungkinkan karena tingginya ketergantungan bank terhadap teknologi berbasis big data dan algoritma kecerdasan buatan (AI) yang dikembangkan oleh mitra teknologi eksternal, yang pada praktiknya tidak selalu transparan dalam tata kelola dan perlindungan data pribadi (Zuboff, 2019). Ketiadaan transparansi tersebut memperburuk situasi karena bank sebagai institusi keuangan sering kali tidak memiliki akses penuh terhadap mekanisme teknis pemrosesan data yang dilakukan oleh mitra teknologi mereka.

Lebih lanjut, masih ditemukan celah dalam regulasi teknis yang mengatur standar keamanan, audit digital, dan pembagian tanggung jawab hukum antara bank dan pihak ketiga yang mengakses data tersebut (OECD, 2020). Di Indonesia, meskipun telah terdapat kerangka hukum perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, implementasinya masih menghadapi tantangan struktural, khususnya dalam hal penetapan standar teknis perlindungan data pada sektor-sektor strategis seperti perbankan. Tanpa kejelasan mengenai standar minimal pengamanan data dan sistem audit digital yang ketat, pengawasan terhadap mitra pihak ketiga berisiko menjadi lemah, membuka peluang terjadinya kebocoran atau penyalahgunaan data secara sistematis.

Situasi ini diperparah oleh lemahnya pemahaman nasabah terhadap hak-haknya atas data pribadi, termasuk hak untuk membatasi, menarik kembali persetujuan, dan mengetahui sejauh mana datanya digunakan oleh pihak ketiga. Dalam praktiknya, persetujuan yang diberikan nasabah sering kali bersifat umum dan tidak spesifik (blanket consent), sehingga rawan dimanipulasi untuk pembenaran penggunaan data di luar konteks layanan utama (Rachmawati, 2022). Padahal, menurut prinsip *purpose limitation* dalam regulasi perlindungan data, setiap pemrosesan data pribadi harus dilakukan secara terbatas dan proporsional sesuai dengan tujuan yang dinyatakan secara eksplisit kepada pemilik data (Pasal 21 dan Pasal 39 UU No. 27 Tahun 2022). Penerapan prinsip ini menjadi sangat penting dalam memastikan bahwa setiap pemrosesan data oleh pihak ketiga tidak menyimpang dari maksud awal pengumpulan data.

Potensi penyalahgunaan data oleh pihak ketiga juga menimbulkan tantangan dalam aspek pembuktian dan penegakan hukum. Ketika terjadi kebocoran atau penyalahgunaan data, nasabah sering kali mengalami kesulitan dalam menelusuri pihak yang bertanggung jawab secara langsung, terutama apabila kerja sama antara bank dan pihak ketiga tidak transparan atau tidak dilengkapi dengan perjanjian tanggung jawab hukum yang jelas (ELSAM, 2021). Bahkan dalam beberapa kasus, tidak jarang perjanjian kerja sama tersebut tidak mengatur secara tegas mengenai konsekuensi hukum atas pelanggaran perlindungan data, sehingga memperlemah posisi nasabah sebagai subjek data dalam proses penegakan haknya.

Dalam konteks ini, bank sebagai pengendali data (data controller) semestinya tetap memikul tanggung jawab utama atas perlindungan data nasabah yang dikelola dalam seluruh rantai kemitraan digitalnya (European Data Protection Board, 2020). Hal ini sejalan dengan prinsip *accountability*, yang menegaskan bahwa setiap pengendali data harus mampu menunjukkan kepatuhan terhadap prinsip-prinsip perlindungan data secara proaktif, termasuk ketika data diproses oleh pihak lain atas nama atau atas kerja sama dengan pengendali data tersebut. Oleh karena itu, penting bagi bank untuk menerapkan kebijakan *due*

diligence yang ketat terhadap mitra pihak ketiga, memastikan keberadaan kontrak pemrosesan data yang eksplisit, serta membangun mekanisme audit dan pelaporan yang memungkinkan deteksi dini atas potensi pelanggaran data.

Dengan demikian, potensi penyalahgunaan data pribadi oleh pihak ketiga dalam ekosistem perbankan digital merupakan tantangan nyata yang menuntut penguatan regulasi teknis, transparansi kontraktual, dan edukasi kepada nasabah mengenai hak-haknya atas data pribadi. Tanpa pengawasan dan akuntabilitas yang ketat, transformasi digital di sektor perbankan justru dapat membuka celah pelanggaran hak atas privasi yang bertentangan dengan prinsip negara hukum yang demokratis. Penguatan peran otoritas pengawas, seperti Otoritas Jasa Keuangan (OJK) dan Komisi Perlindungan Data Pribadi, menjadi krusial untuk menciptakan ekosistem digital yang aman, akuntabel, dan berpihak pada perlindungan hak fundamental warga negara dalam era ekonomi digital.

Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Nasabah dalam Kerja Sama Perbankan Digital Menurut Hukum Positif di Indonesia

Dalam konteks hukum positif di Indonesia, perlindungan terhadap data pribadi nasabah dalam kerja sama perbankan digital telah memperoleh perhatian serius, khususnya sejak diundangkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Kehadiran UU ini menjadi tonggak penting dalam pembentukan kerangka hukum nasional yang setara dengan *General Data Protection Regulation* (GDPR) Uni Eropa. UU PDP menetapkan prinsip-prinsip dasar pemrosesan data pribadi, seperti asas keabsahan, tujuan terbatas, transparansi, akuntabilitas, serta prinsip minimasi data. Prinsip-prinsip ini mengharuskan setiap pemrosesan data pribadi dilakukan secara sah, proporsional, dan hanya untuk tujuan yang dinyatakan secara eksplisit kepada subjek data.

Dalam konteks kerja sama antara bank digital dan pihak ketiga, posisi bank sebagai pengendali data (*data controller*) memiliki makna penting. Bank memiliki tanggung jawab hukum utama untuk menjamin bahwa seluruh proses pengumpulan, penyimpanan, pengolahan, hingga distribusi data pribadi nasabah dilakukan berdasarkan persetujuan yang valid dan dapat dibuktikan secara hukum (UU PDP, Pasal 20–26). Persetujuan ini tidak boleh diperoleh melalui cara manipulatif atau implisit, melainkan harus bersifat eksplisit, terinformasikan (*informed consent*), serta mudah ditarik kembali oleh nasabah apabila dikehendaki.

Pasal 20 hingga Pasal 26 UU PDP secara tegas memuat kewajiban pengendali data, termasuk kewajiban untuk memastikan keamanan sistem pemrosesan, menjaga integritas dan kerahasiaan data, serta menyediakan mekanisme pelaporan dan penanganan insiden kebocoran data. Dalam kerja sama bank dengan pihak ketiga seperti penyedia cloud, fintech, atau platform e-commerce, bank tetap berkewajiban menjamin bahwa mitra digitalnya tunduk pada prinsip dan standar perlindungan data yang sama (Penjelasan Pasal 22 dan 25 UU PDP). Hal ini diperkuat dengan prinsip *due diligence*, di mana bank wajib melakukan penilaian terhadap kapasitas teknis dan kepatuhan hukum dari pihak ketiga sebelum menjalin kerja sama. Apabila dalam praktiknya terjadi penyalahgunaan data oleh pihak ketiga, bank tetap dapat dimintai pertanggungjawaban apabila terbukti lalai dalam proses seleksi, pengawasan, atau perumusan perjanjian kerja sama yang memadai (ELSAM, 2022).

Selain UU PDP, regulasi sektoral juga berperan penting dalam mengisi kekosongan norma teknis dan pengaturan khusus di sektor jasa keuangan. Salah satu regulasi yang relevan adalah Peraturan Otoritas Jasa Keuangan (POJK) No. 11/POJK.03/2022 tentang Penyelenggaraan Produk Bank Umum Berbasis Teknologi Informasi. POJK ini menegaskan kewajiban bank untuk memastikan bahwa seluruh pihak ketiga dalam ekosistem digital perbankan memiliki sistem keamanan teknologi informasi yang memadai dan sesuai dengan standar yang ditetapkan oleh OJK (Pasal 16–18). Ketentuan ini sejalan dengan prinsip *security by design*, di mana perlindungan data harus menjadi bagian integral dari desain teknologi yang digunakan dalam operasional perbankan.

Lebih jauh, Pasal 18 POJK No. 11/POJK.03/2022 menyatakan bahwa bank wajib memiliki perjanjian kerja sama tertulis dengan mitra digital, yang secara eksplisit mengatur tentang kewajiban perlindungan data pribadi, ruang lingkup akses data, mekanisme audit, hingga sanksi apabila terjadi pelanggaran (Pasal 18 ayat (2) huruf c). Dengan adanya pengaturan kontraktual ini, pembagian tanggung jawab hukum menjadi lebih jelas dan dapat digunakan sebagai dasar pembuktian apabila terjadi sengketa antara nasabah, bank, dan pihak ketiga.

Dari sisi hukum pidana, penyalahgunaan data pribadi juga dapat dijerat melalui Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 30 ayat (2) dan (3), yang melarang akses ilegal terhadap sistem elektronik. Ketentuan ini mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak mengakses sistem elektronik milik orang lain, terutama yang memiliki muatan data pribadi, dapat dipidana dengan pidana penjara dan/atau denda (UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016, Pasal 30). Dalam konteks kerja sama digital banking, ketentuan ini dapat diberlakukan terhadap mitra digital atau karyawan bank yang menyalahgunakan akses terhadap sistem elektronik untuk tujuan di luar perjanjian kerja sama atau yang melanggar asas *purpose limitation*.

Namun demikian, efektivitas perlindungan hukum terhadap data pribadi nasabah belum sepenuhnya optimal, karena masih terdapat sejumlah tantangan implementatif. Pertama, kapasitas kelembagaan aparat penegak hukum dan otoritas pengawas untuk memahami kompleksitas teknologi yang digunakan dalam ekosistem digital banking masih terbatas. Masih sering dijumpai ketidaksiapan dalam melakukan audit forensik digital secara mendalam maupun menelusuri *log* akses dalam sistem multi-entitas. Kedua, belum tersedianya regulasi turunan dari UU PDP yang menjabarkan secara teknis standar audit keamanan data, prosedur pelaporan insiden, serta pedoman klasifikasi risiko kerja sama pihak ketiga, menjadi kendala dalam penerapan prinsip akuntabilitas.

Ketiga, ketidakjelasan alur pertanggungjawaban hukum antara bank dan mitra kerja samanya kerap menjadi celah dalam penyelesaian sengketa perlindungan data. Dalam banyak kasus, nasabah sebagai subjek data berada dalam posisi yang lemah karena tidak memiliki informasi yang cukup mengenai siapa pihak yang mengakses datanya, serta tidak tersedia mekanisme pengaduan yang cepat dan transparan. Dalam kondisi seperti ini, harmonisasi regulasi menjadi kebutuhan mendesak. Harmonisasi antara UU PDP, UU ITE, serta regulasi sektoral seperti POJK dan regulasi Bank Indonesia perlu dilakukan untuk menghindari konflik norma, tumpang tindih kewenangan, serta untuk memastikan bahwa tidak ada celah yang dimanfaatkan oleh pelaku usaha yang tidak bertanggung jawab (Yulianto, 2023).

Dengan demikian, perlindungan hukum terhadap data pribadi nasabah dalam ekosistem perbankan digital bukan hanya menjadi urusan kepatuhan administratif, tetapi menyangkut pemenuhan hak

konstitusional warga negara atas privasi dan keamanan data pribadi. Upaya memperkuat posisi nasabah sebagai subjek data harus menjadi agenda utama dalam reformasi regulasi digital banking, yang didukung oleh pengawasan aktif otoritas, peningkatan literasi digital masyarakat, serta penegakan hukum yang konsisten dan berbasis teknologi.

KESIMPULAN

Kerja sama antara perbankan digital dan pihak ketiga, seperti penyedia teknologi finansial (fintech), membawa kemajuan signifikan dalam penyediaan layanan keuangan yang lebih cepat, efisien, dan terjangkau. Namun, di sisi lain, kolaborasi ini juga membuka celah terhadap potensi pelanggaran data pribadi nasabah. Data pribadi yang semestinya bersifat rahasia justru berisiko disalahgunakan untuk kepentingan komersial tanpa persetujuan nasabah, terutama apabila pengelolaannya tidak disertai dengan standar keamanan data yang ketat.

Secara normatif, Indonesia telah memiliki kerangka hukum yang mengatur perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Undang-Undang Perbankan, serta peraturan dari OJK dan Bank Indonesia. Namun, implementasi di lapangan masih menghadapi sejumlah tantangan, seperti disharmoni regulasi, belum optimalnya pengawasan, serta rendahnya kesadaran hukum baik dari pihak perbankan maupun konsumen.

Untuk menjamin perlindungan hukum yang efektif bagi nasabah, diperlukan upaya sistematis, antara lain: harmonisasi regulasi sektoral dan umum terkait perlindungan data pribadi, penerapan prinsip kehati-hatian dalam perjanjian kerja sama dengan pihak ketiga, penguatan kapasitas pengawasan oleh otoritas keuangan, serta peningkatan literasi digital bagi masyarakat. Dengan demikian, transformasi digital dalam sektor perbankan dapat berjalan seiring dengan perlindungan hak-hak fundamental nasabah, khususnya hak atas privasi dan keamanan data pribadi.

REFERENSI

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *Fintech and RegTech: Impact on Regulators and Banks*. Journal of Banking Regulation, 19(3), 12–24..

Zetzsche, D. A. et al. (2020). *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*. NYU Journal of Law & Business, 16(1), 59–102.

Rachmawati, I. (2022). *Perlindungan Data Pribadi dalam Era Fintech: Antara Kepastian Hukum dan Inovasi*. Jurnal Hukum dan Teknologi, 8(2), 45–60.

Bank Indonesia. (2020). *Blueprint Sistem Pembayaran Indonesia 2025*. Jakarta: Bank Indonesia.

Otoritas Jasa Keuangan. (2021). *Pedoman Pengawasan Inovasi Keuangan Digital (IKD)*.

Pasal 20–26 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Pasal 12 ayat (2) Peraturan OJK No. 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan.

Weichert, T. (2021). *Third Parties and Data Protection: Risk in Outsourcing in the Financial Sector*. Data Privacy Journal, 5(2), 34–49.

Albrecht, J. P. (2016). *How the GDPR Will Change the World*. European Data Protection Law Review, 2(3), 287–289.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

OECD. (2020). *Digital Disruption in Banking: Supervision Challenges*. Paris: OECD Publishing.

Rachmawati, I. (2022). *Persetujuan Nasabah dalam Perlindungan Data Digital*. Jurnal Hukum dan Etika Teknologi, 6(1), 22–35.

Pasal 21 dan Pasal 39 UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Lembaga Studi dan Advokasi Masyarakat (ELSAM). (2021). *Analisis Kelemahan Regulasi Perlindungan Data di Sektor Perbankan Digital*.

European Data Protection Board. (2020). *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR.*

Pasal 20–26 Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Penjelasan Pasal 22 dan 25 UU PDP mengenai kewajiban pengendali data dalam kerja sama dengan pemroses data pihak ketiga.

Lembaga Studi dan Advokasi Masyarakat (ELSAM). (2022). *Analisis Tanggung Jawab Pengendali Data dalam Ekosistem Keuangan Digital*.

POJK No. 11/POJK.03/2022 tentang Penyelenggaraan Produk Bank Umum Berbasis Teknologi Informasi, Pasal 16–18.

Ibid., Pasal 18 ayat (2) huruf c.

Pasal 30 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah dengan UU No. 19 Tahun 2016.

Yulianto, A. (2023). *Urgensi Harmonisasi Regulasi Perlindungan Data dalam Sektor Perbankan Digital*. Jurnal Hukum Siber Indonesia, 4(1), 1–19.