

# PERLINDUNGAN DATA PRIBADI DALAM LAYANAN FINANSIAL DIGITAL BERDASARKAN UNDANG- UNDANG NOMOR 27 TAHUN 2022 TENTANG PERLINDUNGAN DATA PRIBADI

Glatysa Sumilat/Nim. 220711010983

Roy Ronny Lembong  
Veibe V. Sumilat

## Abstraka

Penelitian ini dilakukan dengan tujuan untuk mengetahui bagaimana pengaturan penyelenggara layanan finansial digital (Fintech) menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan bagaimana perlindungan hukum penyelenggara layanan finansial digital (Fintech) menurut Undang-Undang Nomor 27 Tahun 2022. Dengan menggunakan metode penelitian yuridis normative, disimpulkan: 1. Penganturan penyelenggara layanan finansial digital kewajiban penyelenggara fintech sebagai Pengendali Data Pribadi Implementasi menurut UU No. 27 Tahun 2022 mewajibkan penyelenggara layanan finansial digital (*Fintech*) untuk bertindak sebagai Pengendali Data Pribadi yang bertanggung jawab penuh atas pemrosesan data pengguna. Bentuk implementasi utamanya meliputi perubahan mekanisme persetujuan dari *opt-out* (otomatis setuju) menjadi *opt-in* (persetujuan eksplisit dan terpisah), pemenuhan kewajiban transparansi melalui pembaruan kebijakan privasi yang mudah dipahami, serta penerapan standar keamanan teknis enkripsi data. 2. Bentuk Perlindungan Hukum terhadap Hak Subjek Data (Pengguna) UU PDP memberikan perlindungan hukum yang bersifat

preventif dan represif bagi pengguna Fintech dan tantangan yuridis belum terbentuknya Lembaga Penyelenggara Pelindungan Data Pribadi dan belum adanya peraturan turunan (PP/Perpres) menyebabkan ketidakpastian standar operasional serta potensi tumpang tindih kewenangan dengan OJK serta tingginya biaya infrastruktur keamanan siber dan kompleksitas sistem algoritma *Credit Scoring* menyulitkan penerapan prinsip transparansi penuh.

**Kata kunci:** Perlindungan, Data Pribadi, Layanan, Finansial Digital.

## PENDAHULUAN

### A. Latar Belakang

Revolusi digital telah menjadi akselerator utama transformasi ekonomi global pada dekade terakhir, dan Indonesia merupakan salah satu negara yang mengalami dampaknya secara masif. Tingginya tingkat penetrasi internet dan kepemilikan ponsel pintar di tengah masyarakat telah menciptakan ekosistem yang subur bagi inovasi di berbagai sektor, terutama di sektor jasa keuangan.<sup>1</sup> Fenomena ini melahirkan apa yang dikenal sebagai teknologi finansial atau *Financial Technology* (Fintech), sebuah industri yang mengintegrasikan teknologi ke dalam layanan keuangan untuk menghasilkan model bisnis, aplikasi, proses, atau produk yang lebih efisien, cepat, dan mudah diakses.

Kehadiran Fintech di Indonesia telah membawa perubahan paradigmatis. Layanan yang sebelumnya terkonsentrasi pada lembaga keuangan konvensional seperti perbankan, kini dapat diakses oleh masyarakat luas melalui genggaman tangan. Mulai dari sistem pembayaran digital (*digital payment*), layanan pendanaan bersama berbasis teknologi

---

<sup>1</sup><https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang> diakses 11 Oktober 2025, jam 12.00.

informasi (*peer-to-peer lending*), agregator finansial, hingga inovasi keuangan digital lainnya, Fintech berhasil mendorong inklusi keuangan secara signifikan.<sup>2</sup> Data dari Otoritas Jasa Keuangan (OJK) menunjukkan pertumbuhan eksponensial dalam nilai transaksi dan jumlah pengguna platform Fintech dari tahun ke tahun, menegaskan perannya sebagai salah satu pilar utama ekonomi digital nasional. Namun, di balik kemudahan dan manfaat yang ditawarkan, model bisnis Fintech menyimpan sebuah dilema fundamental yang berkaitan dengan privasi dan keamanan data.

Operasionalisasi layanan Fintech sangat bergantung pada pengumpulan, pemrosesan, dan analisis data pribadi pengguna dalam volume yang sangat besar (*big data*). Data ini mencakup informasi yang bersifat umum hingga sangat sensitif, seperti data identitas kependudukan (nama, NIK, alamat), data kontak, data biometrik (sidik jari, pemindaian wajah), data transaksi keuangan, hingga data perilaku digital pengguna.<sup>3</sup> Data-data ini merupakan aset krusial bagi penyelenggara Fintech untuk menjalankan fungsi esensial seperti verifikasi identitas nasabah (*Know Your Customer*), analisis kelayakan kredit (*credit scoring*), personalisasi layanan, dan mitigasi risiko penipuan.

Ketergantungan yang tinggi terhadap data ini secara inheren menciptakan risiko yang signifikan. Data pribadi pengguna menjadi target utama serangan siber dan rentan terhadap berbagai bentuk penyalahgunaan. Dalam beberapa tahun terakhir, publik Indonesia diresahkan oleh maraknya kasus pelanggaran data

pribadi yang bersumber dari sektor Fintech. Kasus pinjaman *online* ilegal (*pinjol ilegal*) yang mengakses seluruh data kontak di gawai peminjam untuk melakukan penagihan yang disertai intimidasi adalah salah satu contoh nyata.<sup>4</sup> Selain itu, insiden kebocoran data berskala besar yang dialami oleh beberapa platform Fintech legal juga menjadi sorotan, di mana data jutaan pengguna diduga diperjualbelikan di forum-forum gelap (*dark web*).<sup>5</sup>

Peristiwa-peristiwa ini tidak hanya merugikan pengguna secara finansial dan psikologis, tetapi juga mengikis kepercayaan publik terhadap ekosistem finansial digital secara keseluruhan. Sebelum tahun 2022, kerangka hukum mengenai perlindungan data pribadi di Indonesia bersifat parsial dan tersebar di berbagai peraturan sektoral, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah No. 71 Tahun 2019, serta beberapa Peraturan Otoritas Jasa Keuangan (POJK). Fragmentasi regulasi ini menimbulkan ketidakpastian hukum dan dianggap belum cukup komprehensif untuk menjawab kompleksitas tantangan di era ekonomi digital. Tuntutan akan adanya sebuah undang-undang payung (*umbrella act*) yang mengatur perlindungan data pribadi secara holistik semakin menguat.

Menjawab kebutuhan mendesak tersebut, Dewan Perwakilan Rakyat (DPR) bersama Pemerintah Republik Indonesia mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada tanggal 17 Oktober 2022. Kehadiran UU PDP merupakan sebuah tonggak sejarah dalam penegakan

---

<sup>2</sup> <https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-P2P-Lending-Periode-Desember-2024.aspx> diakses 11 Oktober 2025, jam 12.00.

<sup>3</sup> Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika, 2023.

<sup>4</sup> [https://setkab.go.id/inilah-upaya-pemerintah-lindungi-masyarakat-dari-pinjaman-online-ilegal/?TSPD\\_101\\_R0=086c094b6eab20002b5985](https://setkab.go.id/inilah-upaya-pemerintah-lindungi-masyarakat-dari-pinjaman-online-ilegal/?TSPD_101_R0=086c094b6eab20002b5985)

[d847527f2807c54106b83cedf8f439c2856dc1345058e33a7e4ffb79a308915bb0e0143000a81903063352dd8d088abd7f63ad3ecc81e8ad0b84073b75c3b96a846f29ae189d2cb47ff2899df0bb8ad27227158b12](https://www.kompas.com/tren/read/2021/05/22/205006565/7-data-bocor-yang-diungkap-raid-forums-sebelum-diblokir-kominfo?page=all) diakses 11 Oktober 2025, jam 12.00

<sup>5</sup> <https://www.kompas.com/tren/read/2021/05/22/205006565/7-data-bocor-yang-diungkap-raid-forums-sebelum-diblokir-kominfo?page=all> diakses 11 Oktober 2025, jam 13.00

hak privasi di Indonesia. Undang-undang ini mengadopsi prinsip-prinsip perlindungan data yang diakui secara global, seperti *General Data Protection Regulation* (GDPR) di Uni Eropa. UU PDP secara tegas mendefinisikan jenis-jenis data pribadi, mengatur hak-hak subjek data, serta menetapkan kewajiban dan tanggung jawab bagi Pengendali Data Pribadi dan Prosesor Data Pribadi, yang dalam konteks ini termasuk penyelenggara layanan Fintech.<sup>6</sup> Selain itu, UU PDP juga memperkenalkan sanksi administratif dan pidana yang berat bagi pelaku pelanggaran data pribadi.

Berlakunya UU PDP, seluruh penyelenggara Fintech diwajibkan untuk melakukan penyesuaian fundamental terhadap tata kelola data mereka, mulai dari kebijakan privasi, mekanisme perolehan persetujuan (*consent*), sistem keamanan, hingga prosedur penanganan insiden kebocoran data. Implementasi undang-undang ini di sektor Fintech menjadi sebuah area yang sangat krusial untuk diteliti. Sifat industri Fintech yang sangat dinamis, inovatif, dan sarat dengan pemrosesan data berisiko tinggi menjadikannya sebagai tolok ukur utama efektivitas penerapan UU PDP. Keberhasilan implementasi ini akan menjadi kunci untuk menciptakan keseimbangan antara inovasi layanan keuangan digital dengan perlindungan hak fundamental warga negara atas data pribadi mereka.

Setiap individu dijamin hak konstitusionalnya terutama sebagai bagian dari warga negara Indonesia dalam Undang-Undang Dasar 1945. Jaminan tersebut meliputi perlindungan data diri, keluarga, martabat, kehormatan dan perlindungan dari adanya ancaman. Pemanfaatan Fintech ini juga menimbulkan adanya hambatan dan tantangan terutama dalam perlindungan data pribadi. Data pribadi merupakan sebuah privasi yang

dimiliki oleh setiap orang karena data tersebut memuat hal-hal pribadi pemilik baik itu bersifat sensitif atau tidak dapat disebarluaskan karena jika hal itu tersebar kepada pihak yang tidak bertanggung jawab mengakibatkan adanya kerugian baik secara personal, finansial dan dapat menjadi ancaman keselamatan si pemilik data. Disaat data pribadi telah diinput kedalam sistem aplikasi, informasi mengenai data tersebut tidak lagi berada dalam pengendalian yang ketat oleh pemiliknya, dan bisa diakses serta diproses secara otomatis oleh sistem informasi. Sehingga hal tersebut menimbulkan kekhawatiran serius di tengah masyarakat terkait penggunaan dari informasi pribadi. Penyebaran data pribadi ini merupakan pelanggaran hukum yang dapat berkaitan dengan hak asasi manusia karena berkaitan dengan data pribadi.

Pasal 26 Peraturan Otoritas Jasa Keuangan Nomor 77 Tahun 2016 tentang Layanan Pinjaman Uang Berbasis Teknologi Informasi, Penyelenggara Fintech mempunyai kewajiban dalam menjalankan usahannya untuk menjaga dan merahasiakan data yang diperoleh meliputi:

1. Melindungi kerahasiaan dan integritas data yaitu dengan tetap menjaga kerahasiaan kelengkapan data pribadi sampai data tersebut akhirnya dimusnahkan.
2. Menjamin keaslian dan keabsahan pengolahan data. Penyelenggara wajib memastikan adanya proses autentikasi, verifikasi, dan validasi yang memastikan bahwa setiap akses serta pemrosesan data dilakukan secara resmi dan dapat dipertanggungjawabkan.
3. Segala bentuk pengumpulan, penggunaan, pemanfaatan, hingga pengungkapan data pribadi, data transaksi, dan data keuangan hanya boleh dilakukan atas dasar persetujuan

6

<https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022> diakses 11 Oktober 2025, jam 13.00

- dari pemilik data, kecuali ada ketentuan hukum yang memperbolehkan sebaliknya.
4. Memberikan alternatif saluran komunikasi. Memastikan layanan tetap berjalan dengan baik, dengan tersedianya media komunikasi lain selain sistem elektronik.
  5. Jika terjadi pelanggaran terhadap kerahasiaan data pribadi, data transaksi, atau data keuangan, penyelenggara wajib memberikan pemberitahuan secara tertulis kepada pemilik data yang terkait.

Kewajiban penyelenggara layanan Fintech ini menunjukkan bahwa data yang wajib dilindungi terhadap penerima pinjaman mencakup tiga jenis data, yaitu data pribadi, data transaksi, dan data keuangan. Dalam Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77 Tahun 2016, tidak secara khusus diatur mengenai data pribadi apa saja yang boleh diakses oleh penyelenggara fintech. Hal ini menyebabkan semua data pribadi dapat diakses oleh penyelenggara, baik yang disimpan dalam perangkat penyimpanan handphone maupun tempat penyimpanan lainnya. Izin akses dapat didapatkan melalui "persetujuan" aplikasi fintech.

Pengguna aplikasi harus memberikan izin akses antara lain seperti daftar kontak nomor ponsel, akses galeri, hingga lokasi. Data pribadi yang diperoleh dapat dipakai untuk mengetahui dan menganalisis saat proses pemberian pinjaman online tersebut dan juga dapat digunakan oleh penyelenggara apabila peminjam telah wanprestasi atau dalam keadaan gagal bayar. Peminjam yang tidak dapat memenuhi kewajibannya dalam membayar pinjaman, maka penyelenggara akan menagih pembayaran. Permasalahan mulai timbul pada saat pihak penyelenggara fintech melakukan penagihan dengan mengabaikan prinsip itikad baik yaitu dengan memaksa, mengintimidasi penerima pinjaman agar membayar dari waktu yang ditentukan.

Pelanggaran tersebut meliputi

pengambilan data informasi pada gawai peminjam, penyebaran data pribadi baik berupa foto ataupun informasi pribadi serta penyalahgunaan data KTP tanpa seizin pemiliknya. Penyimpangan data pribadi diatur pada Pasal 67 ayat (1) Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Orang yang mengumpulkan atau memperoleh data pribadi milik orang lain demi keuntungan pribadi secara melawan hukum akan dikenai sanksi pidana. Dalam merespons pelanggaran ini, OJK telah mengeluarkan perintah pembatasan akses data pribadi yang dimiliki oleh penerima pinjaman smartphone. Hal ini diatur melalui Surat OJK Nomor S-72/NB. 213/2019 tentang Pembatasan Akses Data Pribadi pada HP Pengguna, yang berisi larangan bagi penyelenggara untuk mengakses data pribadi kecuali dalam tiga hal tertentu, yaitu (i) lokasi, (ii) kamera, dan (iii) mikrofon (Agusta, 2020:165).

Pasal 26 Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam sistem elektronik, menyatakan pemilik juga berhak menjaga kerahasiaan data pribadinya serta dapat melakukan pengaduan apabila terjadi kebocoran dalam perlindungan data tersebut. Pada tataran praktik dan fakta yang terjadi di Masyarakat bahwa walaupun Pemerintah telah memberlakukan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Di sisi lain, Otoritas Jasa Keuangan memiliki regulasi dan mekanisme pengawasan terhadap penyelenggara fintech legal. Namun, implementasi undang undang ini dalam praktik Fintech masih ditemukan berbagai pelanggaran serta penyalahgunaan data pribadi, dimana hal ini disebabkan oleh karena dari segi kejelasan norma, efektivitas pengawasan, maupun penegakan sanksi yang tidak efektif dan sangat meresakan dan merugikan masyarakat /public. Oleh karena itu, penting untuk mengkaji secara normatif mengenai regulasi tentang data pribadi

dalam layanan Fintech serta sejauh mana pelaksanaan Undang Undang Perlindungan Data Pribadi dapat mengatasi praktik-praktik penyalahgunaan data oleh penyelenggara Fintech. Data pribadi yang dimanfaatkan oleh aplikasi pinjaman tersebut tidak boleh diungkapkan kepada orang yang tidak berwenang, tidak boleh digunakan dalam hal lain selain tujuan pengumpulan data pribadi, serta harus dilindungi secara memadai.

Banyaknya kasus penyalahgunaan data diri pribadi yang dilakukan oleh penyelenggara Fintech.<sup>7</sup>

1. Penyebaran data oleh fintech illegal/ peer-to-peer lending illegal. Fintech illegal sering melakukan penagihan dengan cara yang kasar dan menyebarkan data pribadi peminjam kepada pihak ketiga sebagai tekanan agar membayar, melalui SMS, telepon, WhatsApp, bahkan ancaman.
2. Akses ke data yang tidak semestinya (over-permission) / aplikasi mengakses kontak, SMS, file pribadi. Fintech ilegal menggunakan aplikasi yang meminta akses sangat luas (misal akses kontak, inbox SMS, galeri, dll). Akses ini bisa dimanfaatkan untuk menyebarkan data pribadi atau menyebarkan data ke publik / pihak lain.
3. Foto KTP dan swafoto dengan KTP disalahgunakan. Untuk verifikasi, fintech (terutama ilegal) meminta foto KTP dan selfie dengan KTP. Ternyata data ini bisa bocor atau dijual secara bebas di internet.
4. Kasus bocornya data KREDITPLUS. Ada indikasi bahwa data nasabah fintech KREDITPLUS bocor dan dijual bebas di internet, melibatkan ratusan ribu data.
5. Pelanggaran kerahasiaan data berdasarkan POJK. Ada penelitian kasus di mana fintech pinjol menyalahgunakan data pribadi peminjam yang bertentangan dengan

Pasal 26 POJK No.77 Tahun 2016 tentang Kerahasiaan Data. Salah satu studi menyebutkan PT. Kredit Utama Fintech Indonesia (KUFI).

Berdasarkan pemaparan latar belakang di atas, penulis mengambil judul skripsi ini dengan judul, yaitu: **Perlindungan Data Pribadi Dalam Layanan Finansial Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.**

## B. Rumusan Masalah

1. Bagaimana pengaturan penyelenggara layanan finansial digital (Fintech) menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi?
2. Bagaimana perlindungan hukum penyelenggara layanan finansial digital (Fintech) menurut Undang-Undang Nomor 27 Tahun 2022 ?

## C. Metode Penelitian.

Penelitian Untuk menjawab rumusan masalah dan mencapai tujuan penelitian, metode yang digunakan adalah penelitian hukum normatif (*normative legal research*). (Marzuki, 2017). Penelitian skripsi ini menggunakan metode penelitian hukum normatif (*normative legal research*). Pendekatan ini dilakukan dengan cara mengkaji secara mendalam berbagai peraturan perundang-undangan dan literatur hukum yang relevan (bahan hukum primer dan sekunder). Fokus utamanya adalah menelaah implementasi Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) pada sektor layanan finansial digital (Fintech), serta mengidentifikasi tantangan dan potensi konflik norma dengan regulasi sektoral yang ada. Selain itu, penelitian ini

---

<sup>7</sup> [www.google.com](http://www.google.com) Kasus Penyalahgunaan Data Diri Pribadi selang tahun 2024, diakses 14 Oktober 2025 pkl 21.00

juga menganalisis sejauh mana UU PDP mampu memberikan perlindungan yang efektif terhadap hak-hak subjek data (konsumen), sekaligus menyingkap celah hukum yang dapat dieksploitasi dalam pemrosesan data oleh penyelenggara Fintech.

## PEMBAHASAN

### A. Pengaturan Penyelenggara Layanan Finansial Digital (Fintech) Menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Dalam ekosistem ekonomi digital, penyelenggara layanan finansial digital atau *Financial Technology (Fintech)* memegang peran sentral dalam pengelolaan data masyarakat. Berdasarkan ketentuan Pasal 1 angka 4 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), pihak yang menentukan tujuan dan melakukan kendali atas pemrosesan Data Pribadi dikategorikan sebagai Pengendali Data Pribadi. Oleh karena itu, setiap perusahaan Fintech, baik yang bergerak di sektor *Peer-to-Peer Lending*, pembayaran digital (*e-wallet*), maupun *equity crowdfunding*, secara hukum berstatus sebagai Pengendali Data Pribadi yang memikul tanggung jawab penuh atas data pengguna yang dikelolanya.

Implementasi kewajiban ini menjadi krusial mengingat sektor Fintech memiliki karakteristik *high risk* dan *high regulation*. Data yang diproses tidak hanya bersifat umum (seperti nama dan alamat), tetapi juga mencakup data spesifik berupa data keuangan pribadi yang perlindungannya diamanatkan secara ketat. Berikut adalah analisis mendalam mengenai implementasi kewajiban-kewajiban utama penyelenggara Fintech berdasarkan UU PDP:

#### 1. Pemenuhan Dasar Pemrosesan Data Pribadi (Legal Basis)

Kewajiban paling mendasar bagi penyelenggara Fintech sebagai Pengendali Data Pribadi adalah memastikan bahwa setiap aktivitas pemrosesan data memiliki dasar hukum yang sah sebagaimana diatur dalam Pasal 20 UU PDP. Dalam praktiknya, implementasi ini terwujud melalui dua mekanisme utama: persetujuan yang sah (*consent*) dan pemenuhan kewajiban kontrak. Sebelum berlakunya UU PDP, praktik yang lazim terjadi adalah penggunaan klausul baku dalam syarat dan ketentuan yang sering kali bersifat "memaksa" pengguna untuk menyetujui seluruh pemrosesan data (*bundled consent*). Namun, Pasal 22 UU PDP menegaskan bahwa persetujuan harus dilakukan secara eksplisit, tertulis atau terekam, dan tidak boleh digabungkan.

Implementasi kewajiban ini mengharuskan penyelenggara Fintech untuk mengubah antarmuka pengguna (*User Interface*) pada aplikasi mereka. Mekanisme *opt-out* (persetujuan otomatis kecuali dibatalkan) tidak lagi relevan dan harus digantikan dengan mekanisme *opt-in*. Penyelenggara Fintech wajib menyediakan formulir persetujuan elektronik terpisah untuk tujuan pemrosesan yang berbeda. Sebagai contoh, persetujuan untuk penilaian skor kredit (*credit scoring*) harus terpisah dari persetujuan untuk tujuan pemasaran (*marketing*). Jika Fintech gagal memisahkan hal ini, maka pemrosesan data dianggap cacat hukum dan batal demi hukum.

#### 2. Kewajiban Transparansi dan Pemberitahuan (Notice)

Pasal 21 UU PDP mewajibkan Pengendali Data Pribadi untuk menyampaikan informasi mengenai legalitas, tujuan, jenis data yang diproses, hingga jangka waktu retensi data sebelum data tersebut dikumpulkan. Dalam konteks Fintech, implementasi kewajiban ini tercermin dalam dokumen Kebijakan Privasi (*Privacy Policy*). Namun, tantangan implementasinya terletak pada kejelasan

informasi. Seringkali, dokumen Kebijakan Privasi disusun dengan bahasa hukum yang rumit dan sulit dipahami oleh orang awam. Berdasarkan UU PDP, penyelenggara Fintech wajib menyusun pemberitahuan ini dengan bahasa yang sederhana dan mudah dimengerti. Implementasi yang sesuai dengan regulasi ini dapat dilihat pada aplikasi Fintech yang menyediakan ringkasan ("*summary*") poin-poin penting penggunaan data sebelum pengguna menekan tombol "Setuju". Selain itu, transparansi juga mencakup keterbukaan mengenai transfer data. Banyak penyelenggara Fintech bekerja sama dengan pihak ketiga, seperti *credit bureau*, penyedia tanda tangan elektronik, atau mitra asuransi. Sesuai UU PDP, identitas pihak ketiga ini harus diungkapkan kepada Subjek Data (pengguna) sejak awal, sehingga pengguna memahami kepada siapa saja data mereka akan mengalir.

### 3. Penerapan Keamanan Teknis dan Organisasional

Sebagai industri yang sangat bergantung pada teknologi, kewajiban perlindungan data dalam Pasal 35 UU PDP menjadi tulang punggung operasional Fintech. Pasal ini mewajibkan Pengendali Data untuk menyusun dan menerapkan langkah-langkah teknis dan operasional untuk melindungi Data Pribadi dari gangguan, akses tidak sah, atau penghancuran. Secara teknis, implementasi ini diwujudkan melalui penerapan standar keamanan sistem informasi, seperti penggunaan enkripsi *End-to-End* (E2EE) pada setiap transaksi data, penerapan *Two-Factor Authentication* (2FA) atau biometrik untuk akses akun, serta penggunaan *firewall* berlapis pada *server* penyimpanan data. Penyelenggara Fintech juga dituntut untuk mematuhi standar internasional seperti ISO 27001 tentang Sistem Manajemen Keamanan Informasi, yang kini menjadi salah satu tolak ukur kepatuhan terhadap prinsip keamanan dalam UU PDP.

Secara organisasional, implementasi ini mengharuskan adanya penunjukan Pejabat atau Petugas Perlindungan Data Pribadi (*Data Protection Officer/DPO*) sebagaimana diamanatkan dalam Pasal 53 UU PDP. Penunjukan DPO menjadi wajib bagi Fintech karena kegiatan inti mereka melibatkan pemrosesan data secara sistematis, rutin, dan dalam skala besar. DPO bertugas memastikan kepatuhan internal perusahaan terhadap regulasi dan menjadi narahubung dengan otoritas pengawas.

### 4. Kewajiban Merespons Permintaan Hak Subjek Data

UU PDP memberikan kendali kembali kepada pemilik data melalui serangkaian hak, seperti hak untuk memperbaiki data, hak untuk mengakses data, dan hak untuk menghapus data (*right to be forgotten*). Sebagai Pengendali Data, penyelenggara Fintech wajib menyediakan mekanisme yang mudah bagi pengguna untuk mengajukan hak-hak tersebut.

Implementasi teknis dari kewajiban ini adalah penyediaan fitur "Pusat Privasi" atau "*Privacy Center*" di dalam aplikasi. Melalui fitur ini, pengguna seharusnya dapat mengunduh rekam jejak transaksi mereka (hak portabilitas data), memperbaiki data alamat atau pendapatan yang salah (hak perbaikan), atau mengajukan penutupan akun sekaligus penghapusan data (hak penghapusan) sesuai dengan masa retensi yang berlaku. Kegagalan penyelenggara Fintech dalam merespons permintaan ini dalam kurun waktu 3 x 24 jam (sesuai standar kepatutan layanan) dapat dikategorikan sebagai pelanggaran administratif.

### 5. Kewajiban Pemberitahuan Kegagalan Perlindungan Data (Data Breach Notification)

Salah satu terobosan terbesar dalam UU PDP adalah kewajiban yang diatur dalam Pasal 46. Jika terjadi kegagalan

perlindungan data (kebocoran data), penyelenggara Fintech wajib memberitahukan hal tersebut secara tertulis kepada Subjek Data Pribadi dan lembaga pengawas dalam waktu paling lambat 3 x 24 jam. Implementasi pasal ini menuntut penyelenggara Fintech untuk memiliki *Incident Response Plan* (Rencana Tanggap Insiden) yang matang. Pemberitahuan tersebut tidak boleh sekadar formalitas, melainkan harus memuat data apa saja yang bocor, kapan kejadiannya, dan upaya penanggulangan apa yang telah dilakukan. Dalam praktiknya, hal ini memaksa perusahaan Fintech untuk lebih jujur dan terbuka, berbeda dengan praktik masa lalu di mana banyak perusahaan cenderung menutupi insiden siber demi menjaga reputasi.

Secara keseluruhan, implementasi kewajiban penyelenggara Fintech sebagai Pengendali Data Pribadi berdasarkan UU No. 27 Tahun 2022 menuntut perubahan paradigma dari pendekatan yang berpusat pada bisnis (*business-centric*) menjadi pendekatan yang berpusat pada privasi pengguna (*privacy-centric*). Kepatuhan terhadap UU PDP tidak hanya berhenti pada pembaruan dokumen syarat dan ketentuan, melainkan menyentuh aspek arsitektur sistem IT, prosedur operasional standar (SOP), hingga budaya organisasi dalam menangani data nasabah. Penyelenggara Fintech yang mampu mengimplementasikan kewajiban-kewajiban tersebut secara komprehensif akan memiliki legitimasi hukum yang kuat dan kepercayaan publik yang lebih tinggi di tengah persaingan ekonomi digital.

## **B. Perlindungan Hukum Penyelenggara Layanan Finansial Digital (Fintech) Menurut Undang-Undang Nomor 27 Tahun 2022**

Perlindungan hukum bagi pengguna layanan *Financial Technology* (Fintech) merupakan isu sentral dalam era ekonomi digital, mengingat posisi tawar pengguna

(*user*) yang sering kali lebih lemah dibandingkan penyelenggara layanan. Dalam perspektif ilmu hukum, perlindungan hukum dibagi menjadi dua kategori utama: perlindungan hukum preventif (pencegahan) dan perlindungan hukum represif (penindakan). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) hadir untuk memperkuat kedua bentuk perlindungan ini dengan memberikan serangkaian hak eksklusif kepada Subjek Data Pribadi. Dalam konteks layanan Fintech, di mana data bukan sekadar identitas melainkan aset ekonomi (untuk *credit scoring*, profil risiko, dan pemasaran), bentuk perlindungan hukum yang diberikan oleh UU PDP dapat dianalisis melalui pembedahan hak-hak Subjek Data sebagaimana diatur dalam Pasal 5 hingga Pasal 14.

Berikut adalah analisis mendalam mengenai bentuk-bentuk perlindungan tersebut:

### **1. Perlindungan Preventif Terhadap Hak atas Informasi dan Transparansi**

Bentuk perlindungan hukum yang paling mendasar adalah hak untuk mengetahui (*right to be informed*). Pasal 5 UU PDP menegaskan bahwa Subjek Data Pribadi berhak mendapatkan informasi mengenai kejelasan identitas, dasar kepentingan hukum, tujuan permintaan dan penggunaan, serta akuntabilitas pihak yang meminta Data Pribadi. Dalam praktik layanan Fintech sebelumnya, pengguna sering kali dihadapkan pada "klausula baku" yang panjang dan rumit, di mana mereka tidak menyadari bahwa data kontak darurat atau lokasi perangkat mereka diambil. Perlindungan hukum preventif dalam UU PDP mengubah paradigma ini. Penyelenggara Fintech kini diwajibkan untuk transparan di awal ("*notice at collection*").

Perlindungan ini memitigasi risiko penyalahgunaan data di kemudian hari. Misalnya, dalam layanan *Peer-to-Peer (P2P) Lending*, pengguna berhak

mengetahui apakah data transaksi *e-commerce* mereka akan digunakan untuk menentukan batas kredit (*limit*) atau hanya untuk verifikasi identitas. Jika Fintech tidak menginformasikan tujuan spesifik ini secara transparan, maka pemrosesan data tersebut menjadi tidak sah (ilegal). Dengan demikian, hak ini melindungi pengguna dari praktik "predatory lending" yang memanfaatkan data pribadi secara diam-diam untuk menjebak konsumen dalam siklus utang.

## 2. Hak Mengakses dan Memperbaiki Data (*Right to Rectification*)

Dalam ekosistem Fintech, akurasi data adalah segalanya. Kesalahan satu digit pada data penghasilan atau riwayat pembayaran dapat menyebabkan pengguna masuk dalam daftar hitam (*blacklist*) atau gagal bayar. Oleh karena itu, Pasal 6 UU PDP memberikan perlindungan berupa hak untuk melengkapi, memperbarui, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan Data Pribadi.

Bentuk perlindungan ini sangat krusial dalam mekanisme *Credit Scoring* dan *Know Your Customer* (KYC). Sebelum adanya UU PDP, pengguna sering kesulitan mengoreksi data yang salah pada *database* Fintech karena tidak adanya saluran pengaduan yang jelas. Dengan berlakunya UU PDP, penyelenggara Fintech wajib menyediakan mekanisme perbaikan data. Sebagai contoh, jika seorang pengguna *Paylater* telah melunasi tagihannya namun sistem masih mencatatnya sebagai penunggak utang, pengguna memiliki dasar hukum kuat untuk menuntut koreksi data tersebut. Jika Fintech menolak atau mengabaikan permintaan ini, mereka dapat dikenakan sanksi administratif. Hak ini memberikan perlindungan hukum terhadap kerugian finansial dan reputasi yang mungkin diderita pengguna akibat kelalaian sistem penyelenggara.

## 3. Hak untuk Mengakhiri Pemrosesan dan Penghapusan Data (*Right to Erasure/Right to be Forgotten*)

Salah satu bentuk perlindungan hukum progresif dalam UU PDP adalah hak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan Data Pribadi (Pasal 8). Dalam konteks Fintech, hak ini relevan ketika pengguna memutuskan untuk menutup akun *e-wallet* atau telah melunasi pinjaman di aplikasi *P2P Lending*. Seringkali, meskipun pengguna sudah tidak aktif (uninstall aplikasi), data mereka tetap disimpan dan diperdagangkan untuk tujuan pemasaran. Perlindungan hukum melalui Pasal 8 memberikan wewenang kepada pengguna untuk menarik kembali persetujuan (*withdraw consent*) yang telah diberikan. Ketika persetujuan ditarik, landasan hukum bagi Fintech untuk memproses data tersebut menjadi gugur.

Perlindungan ini tidak bersifat mutlak (*absolute rights*) karena harus disandingkan dengan regulasi sektor keuangan lainnya, seperti Peraturan Otoritas Jasa Keuangan (POJK) yang mewajibkan penyimpanan data transaksi (retensi) selama minimal 5 tahun untuk keperluan audit dan anti-pencucian uang. Dalam hal ini, perlindungan hukum bagi pengguna berwujud pada "pembatasan pemrosesan"; data boleh disimpan untuk kepatuhan hukum, namun dilarang keras digunakan untuk tujuan komersial atau analitik bisnis setelah pengguna mengajukan penghapusan.

## 4. Perlindungan Represif: Hak Menggugat dan Menuntut Ganti Rugi

Perlindungan preventif Ketika gagal dan terjadi pelanggaran (seperti kebocoran data atau penyalahgunaan data), UU PDP menyediakan instrumen perlindungan represif. Pasal 12 UU PDP secara eksplisit menyatakan bahwa Subjek Data Pribadi berhak menggugat dan menerima ganti rugi atas pelanggaran pemrosesan Data Pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan. Ini adalah bentuk perlindungan "pamungkas". Sebelumnya, pengguna Fintech yang menjadi korban kebocoran data sering kali menemui jalan

bantu karena sulitnya membuktikan kerugian riil (*actual loss*) dalam rezim hukum perdata konvensional.

UU PDP memperkuat posisi hukum pengguna dengan dua jalur: Ganti Rugi Materiil dan Imateriil: Pengguna dapat menuntut ganti rugi tidak hanya atas kehilangan uang (misal: saldo *e-wallet* terkuras), tetapi juga kerugian imateriil seperti tercemarnya nama baik akibat data pribadi disebar oleh *debt collector* atau tekanan psikologis akibat teror. Sanksi Administratif: Selain gugatan perdata, perlindungan represif juga hadir melalui peran negara (Lembaga Pengawas PDP) yang dapat menjatuhkan denda administratif hingga 2% dari total pendapatan tahunan terhadap penyelenggara Fintech yang lalai. Meskipun denda ini masuk ke kas negara, sanksi ini memberikan efek jera yang secara tidak langsung melindungi kepentingan kolektif pengguna.

#### 5. Mekanisme Penyelesaian Sengketa

Perlindungan hukum tidak akan efektif tanpa adanya forum yang jelas untuk menuntut hak. UU PDP mengatur bahwa penyelesaian sengketa perlindungan data pribadi dapat dilakukan melalui arbitrase atau pengadilan. Dalam konteks Fintech, hal ini memberikan kepastian hukum (*legal certainty*). Sebelumnya, klausula baku dalam aplikasi Fintech sering kali membatasi hak pengguna untuk menuntut di pengadilan negeri dan memaksa penyelesaian sengketa melalui arbitrase internasional yang mahal dan tidak terjangkau. Dengan semangat perlindungan konsumen dalam UU PDP, mekanisme penyelesaian sengketa haruslah mudah diakses, cepat, dan berbiaya murah. Pengguna kini memiliki opsi untuk melaporkan sengketa ke Lembaga Penyelenggara Pelindungan Data Pribadi

(Lembaga PDP) sebagai langkah non-litigasi sebelum melangkah ke pengadilan.

Secara keseluruhan, bentuk perlindungan hukum yang ditawarkan UU PDP terhadap pengguna layanan Fintech menandai pergeseran dari prinsip *Caveat Emptor* (pembeli harus berhati-hati) menuju prinsip *Product Liability* dan *Strict Liability* dalam pengelolaan data. Beban perlindungan kini tidak lagi bertumpu sepenuhnya pada kehati-hatian pengguna dalam menjaga data, melainkan beralih menjadi beban kewajiban hukum bagi penyelenggara Fintech untuk menjamin keamanan sistemnya.

## PENUTUP

### A. Kesimpulan

1. Implementasi Kewajiban Penyelenggara Fintech sebagai Pengendali Data Pribadi Implementasi UU No. 27 Tahun 2022 mewajibkan penyelenggara layanan finansial digital (*Fintech*) untuk bertindak sebagai Pengendali Data Pribadi yang bertanggung jawab penuh atas pemrosesan data pengguna. Bentuk implementasi utamanya meliputi perubahan mekanisme persetujuan dari *opt-out* (otomatis setuju) menjadi *opt-in* (persetujuan eksplisit dan terpisah), pemenuhan kewajiban transparansi melalui pembaruan Kebijakan Privasi yang mudah dipahami, serta penerapan standar keamanan teknis enkripsi data. Namun, dalam pelaksanaannya, masih ditemukan kendala kepatuhan, terutama terkait kewajiban penghapusan data secara tuntas dan pemisahan tujuan pemrosesan data yang sering kali masih digabungkan dalam satu klausula baku (*bundled consent*).
2. Bentuk Perlindungan Hukum terhadap Hak Subjek Data (Pengguna) UU PDP memberikan perlindungan hukum yang bersifat

preventif dan represif bagi pengguna Fintech.

- Perlindungan Preventif: Terwujud melalui hak pengguna untuk mendapatkan informasi yang jelas mengenai tujuan penggunaan data sebelum transaksi dilakukan, serta hak untuk menolak pemrosesan data yang tidak relevan dengan layanan utama (misalnya data kontak darurat).
- Perlindungan Represif: Terwujud melalui hak pengguna untuk menuntut ganti rugi materiil maupun imateriil atas kebocoran data (Pasal 12), hak koreksi data (*right to rectification*) untuk memperbaiki skor kredit yang salah, serta hak penghapusan data (*right to erasure*) setelah masa retensi berakhir. Mekanisme ini mengubah posisi tawar pengguna yang sebelumnya lemah menjadi setara dengan penyelenggara layanan. Sedangkan upaya Penegakan Hukum UU PDP di sektor Fintech menghadapi tiga tantangan utama:
  - Tantangan Yuridis: Belum terbentuknya Lembaga Penyelenggara Pelindungan Data Pribadi dan belum adanya peraturan turunan (PP/Perpres) menyebabkan ketidakpastian standar operasional serta potensi tumpang tindih kewenangan dengan OJK.
  - Tantangan Teknis: Tingginya biaya

infrastruktur keamanan siber dan kompleksitas sistem algoritma *Credit Scoring* menyulitkan penerapan prinsip transparansi penuh.

- Tantangan Sosial: Rendahnya literasi digital masyarakat yang memicu fenomena "Paradoks Privasi", di mana pengguna cenderung mengabaikan keamanan data demi kemudahan layanan.
- Upaya Mengatasinya: Diperlukan harmonisasi regulasi antara Lembaga PDP dan OJK, penerapan standar ISO 27701 bagi industri Fintech, serta edukasi publik yang masif agar tercipta ekosistem digital yang patuh hukum.

## B. Saran

Berdasarkan kesimpulan di atas, penulis mengajukan beberapa saran yang diharapkan dapat bermanfaat bagi pengembangan hukum dan praktik perlindungan data pribadi di Indonesia:

1. Bagi Pemerintah (Regulator)
  - Segera membentuk Lembaga Penyelenggara Pelindungan Data Pribadi dan menerbitkan peraturan pelaksana teknis agar tidak terjadi kekosongan hukum (*rechtsvacuum*) dalam pengawasan.
  - Melakukan harmonisasi regulasi dengan Otoritas Jasa Keuangan (OJK) dan Bank Indonesia melalui Peraturan Bersama atau MoU untuk memperjelas

batasan kewenangan pengawasan dan mekanisme penjatuhan sanksi administratif, sehingga memberikan kepastian usaha bagi industri Fintech.

meminta perbaikan data jika terdapat kesalahan, dan segera melaporkan kepada otoritas terkait apabila menemukan indikasi penyalahgunaan data pribadi.

#### Bagi Penyelenggara Layanan Fintech (Pelaku Usaha)

- Wajib menerapkan prinsip *Privacy by Design* dan *Privacy by Default* dalam pengembangan aplikasinya, bukan hanya sebagai fitur tambahan.
- Segera menunjuk Pejabat Perlindungan Data Pribadi (*Data Protection Officer/DPO*) yang kompeten dan independen guna memastikan kepatuhan internal perusahaan serta menjadi jembatan komunikasi dengan otoritas pengawas dan konsumen.
- Menyederhanakan bahasa dalam Kebijakan Privasi (*Privacy Policy*) agar benar-benar dapat dipahami oleh pengguna awam, serta menghentikan praktik *dark patterns* (desain antarmuka yang manipulatif) dalam meminta persetujuan data.

#### 2. Bagi Masyarakat (Pengguna Layanan)

- Meningkatkan kewaspadaan dan literasi digital dengan selalu membaca syarat dan ketentuan sebelum memberikan persetujuan akses data.
- Aktif menggunakan hak-haknya sebagai Subjek Data Pribadi, seperti rutin mengecek riwayat transaksi,

### DAFTAR PUSTAKA

#### Buku :

- Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles*. Toronto: Information and Privacy Commissioner of Ontario.
- Djafar, W. (2019). Hukum perlindungan data pribadi di Indonesia: lanskap, urgensi dan kebutuhan pembaruan. *Seminar Hukum dalam Era Analisis Big Data* (pp. 1-14). Program Pasca Sarjana Fakultas Hukum UGM.
- Fasa, M. I. (2024). Transformasi Digital Era Industri 4.0 Revolusi Layanan Yang Mengubah Lanskap Perbankan Syariah Di Indonesia. *Jurnal Intelek Dan Cendekiawan Nusantara*, 1(5), 7653-7665.
- Hadi, S. (2005). *Methodologi Research*. Yogyakarta: Yayasan Penerbitan UGM.
- Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.
- Lintott, A. W. (1999). *Violence in republican Rome*. Oxford University Press.
- Locke, J. (1980). *Second Treatise of Government*. 1690. Ed. CB Macpherson Indianapolis: Hackett.
- Marzuki, P. M. (2017). *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group.
- Rosadi, S. D. (2023). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta: Sinar Grafika.

- Simpson, P. L. (2000). *The politics of Aristotle*. Univ of North Carolina Press.
- Soekanto, S., & Mamudji, S. (2001). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat, Edisi 1*. Jakarta: PT Raja Grafindo Persada.
- Solove, D. J., & Schwartz, P. M. (2022). *An overview of privacy law in 2022*.
- Solove, D. J. (2020). *The Myth of the Privacy Paradox*. George Washington University Law School Public Law and Legal Theory Paper.
- Ustaran, E. (2012). *The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach.* In *Beyond Data Protection: Strategic Case Studies and Practical Guidance*. Springer Berlin Heidelberg, 135-156.
- Wiranata, I. G. (2005.). *Aspek Hukum Periklanan dalam Perspektif Perlindungan Konsumen*. Citra Aditya Bakti.
- Warren, S. D., & Brandeis, L. D. (1980). *The Right to Privacy* (Vol. 4). Harvard Law Review.
- Jurnal :**
- Faizah, Fitrahul, A., Rosadi, S. D., Pratama, G. G., & Dharmawan, A. F. (2023). Penguatan pelindungan data pribadi melalui otoritas pengawas di Indonesia berdasarkan perbandingan hukum Hong Kong dan Singapura. *Hakim: Jurnal Ilmu Hukum Dan Sosial*, 1(3), 01-27.
- Novita, D., Mulyono, M., & Retnowati, A. (2024). Perkembangan Hukum Siber di Indonesia: Studi Literatur tentang Tantangan dan Solusi Keamanan Nasional. *Innovative: Journal Of Social Science Research*, 4(6), 1179-1186.
- Sautumnida, L. (2018). *Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia*. *Kanun Jurnal Ilmu Hukum*, 20(2), 369-384.
- Sitompul, M. G. (2018). Urgensi legalitas financial technology (Fintech): Peer to peer (P2p) lending Di Indonesia . *Jurnal Yuridis Unaja*, 1(2), 68-79.
- William L. Prosser. (1960). "Privacy," *California Law Review*, Vol. 48, No. 3.
- Peraturan Perundang-undangan :**
- Undang Undang Dasar Republik Indonesia Tahun 1945.
- Kitab Undang Undang Hukum Pidana Undang Undang Nomor 7 Tahun 2022 Tentang Perlindungan Data Pribadi.
- Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Otoritas Jasa Keuangan.
- Website :**
- <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang> diakses 11 Oktober 2025, jam 12.00.
- <https://ojk.go.id/id/kanal/iknb/data-dan-statistik/fintech/Pages/Statistik-P2P-Lending-Periode-Desember-2024.aspx> diakses 11 Oktober 2025, jam 12.00.