

Artikel Penelitian

## Implikasi Hukum terhadap Perlindungan Data Pribadi dalam Transaksi Fintech

*Febrian, Indrawan Yoswanda Saputra, Diana R.W. Napitupulu**Fakultas Hukum, Prodi Magister Hukum, Universitas Kristen Indonesia, Jakarta, Indonesia*

### INFORMASI ARTIKEL

Diterima Redaksi: 11 Juli 2025  
Revisi Akhir: 25 Juli 2025  
Diterbitkan Online: 27 Agustus 2025

### KATA KUNCI

Financial Technology (Fintech)  
Perlindungan Data Pribadi  
Regulasi Fintech  
Hukum Perlindungan Data  
Undang-Undang Perlindungan Data Pribadi

### KORESPONDENSI

Phone: -  
E-mail: [febrian.hutabarat@gmail.com](mailto:febrian.hutabarat@gmail.com)

### A B S T R A K

Perkembangan industri financial technology (fintech) di Indonesia telah membawa transformasi signifikan dalam layanan keuangan digital. Namun, pesatnya perkembangan ini juga meningkatkan risiko kebocoran dan penyalahgunaan data pribadi pengguna. Implikasi hukum terhadap perlindungan data pribadi dalam transaksi fintech menjadi aspek krusial dalam memastikan keamanan serta kepatuhan terhadap regulasi yang berlaku. Penelitian ini bertujuan untuk menganalisis efektivitas regulasi serta tantangan implementasi hukum dalam melindungi data pribadi pengguna fintech di Indonesia. Analisis ini dilakukan dengan merujuk pada Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta peraturan yang diterbitkan oleh Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan dan konseptual, serta menganalisis regulasi, jurnal akademik, dan laporan dari lembaga terkait. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki kerangka regulasi terkait perlindungan data pribadi, implementasinya masih menghadapi berbagai tantangan. Salah satu tantangan utama adalah ketidaksesuaian standar keamanan data di berbagai platform fintech, lemahnya penegakan hukum terhadap pelanggaran data pribadi, serta kurangnya mekanisme pengawasan yang efektif dari regulator. Banyak penyelenggara fintech yang masih belum sepenuhnya mematuhi standar perlindungan data yang ditetapkan, sehingga meningkatkan risiko eksploitasi dan kebocoran data pengguna.

## PENDAHULUAN

Perkembangan teknologi dan informasi yang masif di dunia, tentunya juga memberikan pengaruh terhadap kebiasaan, ritme pekerjaan, dan budaya umat manusia. Sejak ditemukannya mesin uap di Inggris tahun 1763, itu menandakan revolusi industri telah dimulai atau biasa disebut revolusi industri 1.0. Penemuan ini merupakan cikal bakal perkembangan inovasi teknologi yang mempengaruhi cara manusia bekerja, mencari nafkah, mendapatkan pendidikan dan berbagai aspek lainnya.

Inovasi ini tidak berhenti begitu saja, manusia sebagai makhluk yang memiliki akal dan pemikiran rasional, terus berinovasi untuk menemukan hal-hal yang bertujuan untuk memberikan efisiensi, mempermudah pekerjaan dan memberikan dampak ekonomi bagi kehidupan bermasyarakat. Hingga memasuki awal abad 21 ini, kita sudah memasuki era revolusi industri 4.0. Yang dimaksud dengan revolusi industri 4.0 adalah fase transformasi besar dalam sektor industri yang mengintegrasikan teknologi digital, seperti *Internet of Things* (IoT), kecerdasan buatan (AI), *big data*, dan sistem siber-fisik untuk menciptakan otomatisasi dan efisiensi. Ini lebih luas dari sekadar digitalisasi karena mencakup perubahan fundamental pada proses produksi dan interaksi manusia dengan teknologi.<sup>1</sup>

<sup>1</sup> Schwab, K. (2016). *The Fourth Industrial Revolution*. Geneva: World Economic Forum.  
Hermann, M., Pentek, T., & Otto, B. (2016). *Design Principles for Industrie 4.0 Scenarios*. Institute of Information Management, University of St. Gallen

Sebagaimana yang dijelaskan oleh Schwab diatas, revolusi industri 4.0 sangat berkaitan erat dengan adaptasi teknologi untuk mengubah proses analog menjadi digital dalam berbagai aspek kehidupan dan bisnis, termasuk dalam pengelolaan data, layanan pelanggan, transaksi pembayaran, dan komunikasi. Proses ini biasa disebut dengan digitalisasi yang termasuk salah satu elemen dalam Revolusi Industri 4.0, tetapi tidak mencakup seluruh spektrum transformasi industri.

Digitalisasi telah membawa perubahan besar dalam berbagai aspek kehidupan masyarakat Indonesia, salah satunya adalah kemunculan layanan pinjam meminjam uang berbasis teknologi atau yang biasa disebut fintech. Fintech adalah penggunaan teknologi untuk layanan solusi finansial<sup>2</sup>. Fintech mencakup berbagai layanan seperti pembayaran digital, pinjaman online, investasi berbasis teknologi, hingga asuransi digital. Fintech membantu transaksi jual beli dan sistem pembayaran menjadi lebih efisien dan ekonomis namun tetap efektif<sup>3</sup>.

Di Indonesia, perkembangan fintech didorong oleh meningkatnya penetrasi internet dan penggunaan ponsel pintar. Menurut laporan Otoritas Jasa Keuangan (OJK), jumlah penyelenggara fintech terus bertambah setiap tahunnya, mencerminkan tingginya permintaan masyarakat terhadap layanan keuangan berbasis digital. Pemerintah melalui berbagai regulasi telah berupaya mengakomodasi pertumbuhan fintech guna mendukung inklusi keuangan nasional. Namun, pesatnya perkembangan industri ini juga menghadirkan tantangan baru, terutama dalam hal perlindungan data pribadi konsumen.

Fintech beroperasi dengan mengumpulkan dan mengolah data pribadi pengguna dalam skala besar. Data ini meliputi informasi identitas, data transaksi, riwayat keuangan, hingga preferensi pengguna. Ada sebuah ungkapan yang pernah di lontarkan oleh seorang matematikawan Inggris, Clive Humby dan kini menjadi populer kembali yaitu "*data is the new oil*". Ungkapan ini mengandung makna yaitu data pribadi menjadi suatu hal primer dan berharga karena data pribadi dapat mempengaruhi keputusan ekonomi di masa depan. Keamanan data pribadi menjadi krusial mengingat data tersebut sering kali digunakan oleh pelaku usaha di bidang digital untuk kepentingan analisis pasar, periklanan, atau bahkan transaksi lintas batas. Dengan semakin kompleksnya penggunaan data, risiko kebocoran dan penyalahgunaan data pribadi juga meningkat. Kasus pelanggaran data pribadi dalam layanan fintech bukan lagi sesuatu yang jarang terjadi, baik dalam bentuk peretasan, pencurian data, maupun penyalahgunaan oleh pihak yang tidak bertanggung jawab<sup>4</sup>.

Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN) yang mencatat lebih dari 500 juta data pribadi telah bocor di Indonesia sejak tahun 2020 adalah salah satu bukti validasi bahwa data pribadi masyarakat Indonesia telah berada di tangan oknum yang tidak bertanggung jawab.

Salah satu permasalahan utama dalam transaksi fintech adalah lemahnya kesadaran pengguna terhadap pentingnya perlindungan data pribadi. Banyak pengguna yang secara tidak sadar memberikan izin akses terhadap informasi pribadinya tanpa memahami konsekuensinya.

Kasus kebocoran data pribadi telah menimbulkan dampak negatif bagi masyarakat, seperti pencurian identitas, penyalahgunaan data untuk kejahatan keuangan, hingga penipuan berbasis digital. Pada tahun-tahun terakhir, terdapat beberapa kasus kebocoran data yang melibatkan perusahaan fintech di Indonesia, yang menunjukkan adanya kelemahan dalam sistem perlindungan data dan penerapan standar keamanan data oleh penyelenggara fintech. Fenomena ini menimbulkan kekhawatiran akan sejauh mana regulasi yang ada mampu memberikan perlindungan yang optimal bagi konsumen.

Dalam konteks hukum, perlindungan data pribadi di Indonesia telah diatur dalam berbagai regulasi, seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya, serta peraturan-peraturan turunan yang dikeluarkan oleh Otoritas Jasa Keuangan (OJK) dan Bank Indonesia (BI). Regulasi ini bertujuan untuk memastikan bahwa data pribadi pengguna fintech dikelola secara aman dan tidak disalahgunakan oleh pihak yang tidak berwenang.

Meskipun sudah ada landasan hukum yang mengatur perlindungan data pribadi, implementasinya masih menghadapi berbagai tantangan. Salah satu tantangan terbesar adalah lemahnya penegakan hukum terhadap pelanggaran data pribadi. Banyak kasus kebocoran data yang terjadi tanpa adanya sanksi yang tegas bagi pihak yang bertanggung jawab, sehingga

---

<sup>2</sup> Douglas Amer, Janos Barberis, dan Ross Buckley. "The Evolution of Fintech: A Ner Post-Crisis Paradigm?", *University of New South Wales Law Research Series No. 2016-62*. <https://ssrn.com/abstract=2676553>

<sup>3</sup> Diah Ayu Septi Fauji, Moch. Wahyu Widodo, *Financial Technology* (Kediri: Penerbit Fakultas Ekonomi Universitas Nusantara PGRI Kediri, 2020), hal. 2.

<sup>4</sup> Douglas Amer, Janos Barberis, dan Ross Buckley. "The Evolution of Fintech: A Ner Post-Crisis Paradigm?", *University of New South Wales Law Research Series No. 2016-62*. <https://ssrn.com/abstract=2676553>

menimbulkan kekhawatiran akan efektivitas regulasi yang ada<sup>5</sup>. Selain itu, masih terdapat praktik-praktik di mana penyelenggara fintech tidak sepenuhnya menerapkan standar keamanan data yang memadai, sehingga meningkatkan potensi kebocoran informasi sensitif.

Urgensi perlindungan hukum terhadap data pribadi dalam transaksi fintech semakin meningkat seiring dengan berkembangnya ancaman siber dan eksploitasi data oleh pihak yang tidak bertanggung jawab. Tanpa adanya regulasi yang ketat dan mekanisme penegakan hukum yang kuat, masyarakat akan terus menghadapi risiko kebocoran dan penyalahgunaan data pribadi<sup>6</sup>. Oleh karena itu, diperlukan penguatan regulasi serta peningkatan kesadaran akan pentingnya perlindungan data pribadi, baik dari sisi pengguna maupun penyelenggara fintech.

Selain aspek regulasi, peran otoritas pengawas seperti OJK dan BI juga menjadi krusial dalam memastikan bahwa penyelenggara fintech mematuhi standar keamanan data yang ditetapkan<sup>7</sup>. Otoritas ini harus dapat berperan aktif dalam melakukan pengawasan, memberikan sanksi kepada pelanggar, serta mengedukasi masyarakat terkait pentingnya perlindungan data pribadi dalam ekosistem digital. Langkah ini diperlukan agar industri fintech dapat berkembang secara berkelanjutan tanpa mengorbankan hak-hak konsumen dalam hal keamanan data pribadi.

Selain itu, penting bagi masyarakat sebagai pengguna fintech untuk lebih memahami hak-haknya dalam perlindungan data pribadi. Sosialisasi dan edukasi mengenai literasi digital harus terus ditingkatkan agar masyarakat lebih bijak dalam berbagi data pribadi serta memahami risiko yang mungkin timbul. Kesadaran yang lebih tinggi dari pengguna dapat menjadi faktor penting dalam mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab<sup>8</sup>.

Dengan adanya penelitian ini, diharapkan dapat memberikan kontribusi bagi pengembangan regulasi perlindungan data pribadi di Indonesia serta memberikan rekomendasi bagi para pemangku kepentingan dalam meningkatkan sistem perlindungan data dalam transaksi fintech. Perlindungan data pribadi merupakan aspek yang krusial dalam mewujudkan ekosistem keuangan digital yang aman dan terpercaya, sehingga perlu perhatian lebih dari berbagai pihak, baik regulator, pelaku industri, maupun masyarakat sebagai pengguna layanan fintech.

### ***Rumusan Masalah***

1. Bagaimana regulasi yang mengatur perlindungan data pribadi dalam transaksi fintech di Indonesia?
2. Apa saja tantangan yang dihadapi dalam implementasi perlindungan data pribadi di sektor fintech?
3. Bagaimana strategi hukum yang dapat diterapkan untuk memperkuat perlindungan data pribadi dalam transaksi fintech di Indonesia?

### ***Tujuan Penelitian***

1. Menganalisis regulasi yang mengatur perlindungan data pribadi dalam transaksi fintech di Indonesia.
2. Mengidentifikasi tantangan dalam implementasi perlindungan data pribadi di sektor fintech.
3. Merumuskan strategi hukum yang dapat diterapkan untuk meningkatkan perlindungan data pribadi dalam transaksi fintech di Indonesia.

## **METODE PENELITIAN**

Penelitian ini menggunakan metode normatif yuridis dengan pendekatan perundang-undangan serta analisis kasus kebocoran data fintech di Indonesia. Sumber data terdiri dari regulasi terkait, laporan lembaga pengawas seperti OJK dan BSSN, serta studi literatur.

## **HASIL DAN PEMBAHASAN**

### ***Konsep dan Urgensi Perlindungan Data Pribadi dalam Fintech***

<sup>5</sup> Edmon Makarim, "Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi," *Hukumonline.com*, 9 Juli 2020, <https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef/> (diakses tanggal 15 Maret 2025).

<sup>6</sup> Croys Diansyah A. dkk., "Perlindungan Data Pribadi Konsumen Finansial Technology (Fintech) Berdasarkan Peraturan Otoritas Jasa Keuangan Nomor: 77/Pojk.01/2016 dan Peraturan Bank Indonesia Nomor: 22/20/PBI/2020," *Madani* Vol. 1, No. 5 (2023): hal. 228 – 240.

<sup>7</sup> Elvira Fitriyani Pakpahan, Lionel Ricky Chandra, Ananta Aria Dewa, "Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology," *Veritas et Justitia* Vol. 6, No. 2 (2020): hal. 298 - 323

<sup>8</sup> Dwi Fajar Saputra, "Literasi Digital untuk Perlindungan Data Pribadi," *Jurnal Ilmu Kepolisian* Vol. 17, No. 3 (2023): hal. 1-8.

Perkembangan fintech telah membawa perubahan signifikan dalam sektor keuangan, terutama dalam kemudahan akses layanan keuangan digital. Namun, di balik kemajuan ini, terdapat tantangan serius terkait perlindungan data pribadi konsumen. Perlindungan data pribadi dalam sektor fintech merupakan isu yang sangat penting, mengingat meningkatnya penggunaan layanan keuangan digital yang mengelola informasi pribadi yang sangat sensitif. Data pribadi dalam sektor fintech mencakup informasi yang dapat mengidentifikasi individu, seperti nama lengkap, alamat, informasi keuangan, nomor identitas, dan data transaksi. Data ini menjadi sangat rentan terhadap penyalahgunaan, baik dari pihak internal yang tidak bertanggung jawab maupun pihak eksternal yang dapat mengeksploitasi celah keamanan.

Perlindungan data pribadi dalam sektor fintech memiliki urgensi yang tinggi. Setiap transaksi finansial digital mengandung risiko terhadap kebocoran data yang dapat merugikan konsumen dan penyelenggara fintech. Data yang bocor bisa disalahgunakan untuk melakukan penipuan identitas, pencurian finansial, atau bahkan manipulasi data pribadi yang dapat menyebabkan kerugian lebih besar bagi individu maupun perusahaan. Keamanan data yang buruk juga dapat mengurangi kepercayaan konsumen terhadap layanan fintech, yang pada gilirannya dapat berdampak negatif pada industri secara keseluruhan.

Kebocoran data pribadi bukanlah isu yang baru. Pada tahun 2019, salah satu perusahaan fintech terbesar di Indonesia, Tokopedia, mengalami kebocoran data yang mencakup informasi pribadi lebih dari 91 juta pengguna. Kasus ini menunjukkan betapa rentannya data pribadi terhadap serangan dunia maya yang dapat mengancam keamanan finansial dan privasi individu. Kebocoran semacam ini, selain merugikan konsumen, juga merusak reputasi perusahaan dan industri fintech secara keseluruhan, mengurangi tingkat adopsi layanan fintech di masyarakat. Dalam kasus Tokopedia, lebih dari 91 juta data pengguna yang bocor mencakup informasi sensitif yang sangat rentan untuk disalahgunakan oleh pihak yang tidak bertanggung jawab<sup>9</sup>.

Dari perspektif hukum, kebocoran data pribadi berpotensi memicu tuntutan hukum terhadap penyelenggara fintech. Hal ini mencakup klaim ganti rugi oleh konsumen yang terdampak kebocoran data, yang bisa sangat merugikan pihak perusahaan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) serta perubahannya mengatur aspek keamanan informasi dalam transaksi elektronik, namun implementasi yang efektif masih menjadi tantangan besar. Meskipun hukum sudah ada, pelaksanaannya seringkali tertinggal dengan cepatnya perkembangan teknologi dan metode serangan dunia maya yang semakin canggih<sup>10</sup>. Di sisi ekonomi, kebocoran data pribadi dapat menurunkan kepercayaan publik terhadap penyelenggara fintech, yang mengarah pada penurunan jumlah transaksi dan penurunan volume bisnis. Ini akan menghambat pertumbuhan sektor fintech yang saat ini sedang berkembang pesat. Sebagai contoh, menurut laporan oleh PwC pada tahun 2020, hampir 60% konsumen yang mengalami kebocoran data pribadi di sektor fintech memilih untuk tidak lagi menggunakan layanan tersebut, yang jelas menunjukkan hubungan antara kebocoran data dan hilangnya kepercayaan konsumen<sup>11</sup>.

Pentingnya regulasi dalam perlindungan data pribadi semakin mendesak. Beberapa negara telah mengadopsi regulasi ketat yang membatasi pengelolaan dan distribusi data pribadi. Sebagai perbandingan, Uni Eropa melalui peraturan *General Data Protection Regulation (GDPR)* telah menetapkan standar tinggi bagi pengelolaan data pribadi, yang meliputi hak individu untuk mengakses, mengubah, dan menghapus data mereka, serta persetujuan eksplisit untuk pengumpulan data pribadi. Regulasi seperti ini memberikan perlindungan yang lebih jelas dan memberikan kewajiban yang lebih besar bagi penyelenggara fintech untuk menjaga keamanan data yang mereka kelola.

Di Indonesia, meskipun ada upaya untuk memperbarui regulasi perlindungan data pribadi, seperti melalui Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang sedang dibahas, implementasinya belum sepenuhnya memberikan perlindungan yang setara dengan standar internasional. Oleh karena itu, adopsi regulasi yang lebih tegas dan konkret sangat diperlukan agar sektor fintech dapat berkembang dengan lebih aman dan terpercaya.

Misalnya, di Eropa, lembaga-lembaga pendidikan publik secara aktif mengedukasi masyarakat mengenai hak-hak mereka menurut GDPR. Ini termasuk cara bagaimana konsumen dapat mengakses data mereka, menghapusnya, atau bahkan menuntut ganti rugi jika data mereka disalahgunakan. Di Indonesia, meskipun ada peningkatan kesadaran tentang pentingnya perlindungan data, banyak konsumen yang masih kurang memahami hak-hak mereka dalam transaksi fintech. Selain regulasi yang ketat, penting untuk meningkatkan kesadaran masyarakat mengenai hak-hak mereka dalam perlindungan data pribadi. Edukasi yang tepat dapat membantu konsumen memahami pentingnya menjaga kerahasiaan data mereka serta mengidentifikasi potensi risiko yang dapat muncul dari penyalahgunaan data. Penyuluhan mengenai

<sup>9</sup>Fauzi Rifa & Maslihati Nur Hidayati, "Perlindungan Data Pribadi dalam Industri Fintech Indonesia," *Jurnal Teknologi dan Keamanan Informasi*, 2024.

<sup>10</sup>Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 26.

<sup>11</sup>PwC, "Consumer Data Privacy: Global Survey 2020," *PricewaterhouseCoopers International Limited*, 2020.

cara-cara aman dalam menggunakan layanan fintech dan kewajiban penyelenggara untuk melindungi data pribadi akan sangat mendukung upaya perlindungan yang lebih efektif.

Keberadaan regulasi yang jelas memberikan dasar hukum bagi perlindungan data pribadi, namun implementasi yang efektif tetap menjadi tantangan utama (Fauzi Rifa dan Maslihati Nur Hidayati, 2024). Penyelenggara fintech harus memastikan bahwa sistem mereka memiliki standar keamanan yang tinggi guna mencegah kebocoran dan penyalahgunaan data pribadi konsumen. Selain itu, masyarakat juga perlu diberikan edukasi mengenai hak-hak mereka dalam perlindungan data pribadi.

Pentingnya perlindungan data pribadi dalam transaksi fintech tidak hanya terkait dengan aspek hukum, tetapi juga berkaitan dengan aspek ekonomi. Kebocoran data pribadi dapat mengakibatkan kerugian finansial yang besar, baik bagi individu yang terkena dampak maupun bagi perusahaan yang kehilangan kepercayaan pelanggan. Oleh karena itu, perlindungan data pribadi harus menjadi prioritas utama dalam pengembangan ekosistem fintech di Indonesia<sup>12</sup>.

### ***Regulasi Perlindungan Data Pribadi dalam Transaksi Fintech di Indonesia***

Perlindungan data pribadi dalam transaksi fintech di Indonesia telah diatur dalam berbagai regulasi, baik di tingkat undang-undang maupun peraturan otoritas terkait. UU PDP menjadi payung hukum utama dalam mengatur perlindungan data pribadi di Indonesia, termasuk dalam sektor fintech. UU ini mengatur kewajiban penyelenggara layanan fintech dalam mengelola dan melindungi data konsumen dengan prinsip transparansi, akuntabilitas, dan keamanan.

Dalam konteks hukum yang ada di Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) telah mengatur hak dan kewajiban para pihak dalam pengelolaan data pribadi. Regulasi ini menegaskan pentingnya persetujuan pemilik data dalam pengelolaan informasi pribadinya. UU PDP merupakan produk hukum yang mengadopsi General Data Protection Regulation (GDPR) yang terlebih dahulu diberlakukan di Uni Eropa. Berikut ini adalah beberapa asas-asas yang memiliki kesamaan antara UUPDP dan GDPR:

ASAS	GDPR	UU PDP
Lawfulness, Fairness, and Transparency	YA	YA
Purpose Limitation	YA	YA
Data Minimization	YA	YA
Accuracy	YA	YA
Storage Limitation	YA	YA
Integrity and Confidentiality	YA	YA
Accountability	YA	YA

Secara keseluruhan, GDPR dan UU PDP memiliki kesamaan yang signifikan dalam prinsip-prinsip dasar perlindungan data pribadi. Keduanya menetapkan bahwa pemrosesan data pribadi harus dilakukan dengan cara yang sah, adil, transparan, aman, dan terbatas pada tujuan yang jelas. Dengan disahkannya UU PDP, memberikan landasan hukum yang lebih jelas terkait perlindungan data pribadi konsumen dalam sektor fintech. Misalnya, penyelenggara fintech wajib mendapatkan persetujuan eksplisit dari pengguna sebelum memproses data pribadi mereka, dan konsumen memiliki hak untuk mengetahui bagaimana data mereka digunakan serta hak untuk meminta akses atau perbaikan data. Praktik ini membantu meningkatkan kepercayaan konsumen terhadap layanan fintech, yang sangat penting dalam sektor yang berbasis digital.

UU PDP juga mengatur standar keamanan yang tinggi dalam penyimpanan data pribadi. Dalam sektor fintech, hal ini berarti penyelenggara fintech harus menggunakan sistem keamanan yang lebih baik untuk menghindari kebocoran data, yang dapat berdampak pada reputasi dan kerugian finansial besar. Peraturan ini juga mendorong fintech untuk mematuhi prinsip-prinsip transparansi dan akuntabilitas, yang dapat mempengaruhi cara fintech beroperasi. UU PDP menetapkan sanksi yang tegas, termasuk denda dan sanksi pidana bagi penyelenggara fintech yang melanggar ketentuan perlindungan data pribadi. Hal ini memberikan insentif yang kuat bagi penyelenggara untuk memperhatikan aspek perlindungan data dalam operasi mereka.

<sup>12</sup> Mochamad Januar Rizki, "Perlindungan Data Konsumen Harus Jadi Prioritas Industri Fintech," Hukumonline.com, 23 September 2019, <https://www.hukumonline.com/berita/a/perlindungan-data-konsumen-harus-jadi-prioritas-industri-fintech-lt5d887b1ba7f91/> (diakses tanggal 15 Maret 2025).

Selain UU PDP, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) serta perubahannya juga memberikan landasan hukum bagi transaksi elektronik yang aman dan terpercaya. Relevansi dari undang-undang ini mengatur ketentuan mengenai transaksi elektronik, keamanan data, dan perlindungan data pribadi yang diproses dalam layanan fintech. Di Indonesia, perkembangan fintech yang pesat mengharuskan adanya pengaturan yang jelas terkait dengan transaksi elektronik dan perlindungannya, dan UU ITE menjadi dasar hukum yang mengatur sebagian besar aspek tersebut. Dalam hal pelanggaran, UU ITE juga menetapkan sanksi bagi pelaku yang menyalahgunakan data pribadi.

Berikut ini adalah beberapa hal yang diatur dalam UU ITE dalam kaitannya dengan fintech antara lain:

1. Perlindungan Data Pribadi

Pasal 26 UU ITE (Perlindungan Data Pribadi)

- (1) Setiap orang dilarang untuk mengungkapkan informasi pribadi atau data pribadi seseorang tanpa persetujuan dari yang bersangkutan, kecuali ada ketentuan perundang-undangan yang mengatur lain.
- (2) Setiap orang berhak untuk memperoleh informasi terkait dengan data pribadinya yang disimpan, diproses, dan digunakan oleh penyelenggara sistem elektronik.

UU ITE memberikan pengaturan mengenai perlindungan data pribadi dalam transaksi elektronik, terutama terkait dengan keamanan data pribadi dan keamanan sistem elektronik. Pasal 26 ayat (1) mengatur bahwa setiap orang dilarang mengungkapkan data pribadi tanpa persetujuan yang bersangkutan, kecuali ada ketentuan dalam peraturan perundang-undangan lain yang mengatur. Dalam konteks fintech, data pribadi yang dimaksud mencakup informasi sensitif seperti data identitas (nama, nomor KTP, alamat), data transaksi (riwayat pinjaman, pembayaran, dan transaksi lainnya) dan data keuangan (riwayat kredit, saldo rekening). Persetujuan pengguna sangat penting dalam pengelolaan data pribadi oleh penyelenggara fintech. Sebagai contoh, penyelenggara pinjaman online atau platform pembayaran digital harus meminta izin eksplisit dari pengguna sebelum mengumpulkan, mengolah, atau membagikan data pribadi mereka ke pihak ketiga (misalnya mitra bisnis atau iklan berbasis data).

Dalam industri fintech, pengguna sering kali memberikan data pribadi secara sukarela tanpa sepenuhnya menyadari risiko dan konsekuensinya. Pasal 26 memastikan bahwa penyelenggara fintech memiliki kewajiban untuk memperoleh persetujuan eksplisit dari pengguna sebelum data mereka digunakan atau dibagikan. Sebagai contoh adalah sebuah aplikasi pinjaman online yang mengumpulkan informasi pengguna (seperti nomor KTP, riwayat transaksi, alamat) harus meminta izin terlebih dahulu untuk menggunakan data tersebut. Tanpa persetujuan, tindakan pengumpulan data bisa dianggap melanggar hukum. Persetujuan yang jelas tidak hanya terbatas pada pengumpulan data, tetapi juga pada bagaimana data tersebut akan digunakan (misalnya, untuk analisis pasar atau periklanan) dan disimpan (misalnya untuk jangka waktu tertentu).

Pasal 26 ayat (2) memberikan hak kepada setiap orang untuk memperoleh informasi terkait data pribadi mereka yang disimpan atau diproses oleh penyelenggara sistem elektronik. Ini sangat relevan dengan konteks fintech, di mana pengguna memiliki hak untuk mengetahui data apa yang telah dikumpulkan tentang mereka, bagaimana data tersebut diproses, dan apakah ada pihak ketiga yang menerima data mereka. Sebagai contoh adalah misalnya pengguna fintech memiliki hak untuk meminta akses terhadap data pribadi mereka yang disimpan oleh aplikasi pinjaman atau platform pembayaran, termasuk informasi transaksi atau status pinjaman mereka. Hal ini sangat penting untuk memberi pengguna kendali atas data mereka, serta untuk meminimalkan potensi penyalahgunaan data pribadi di dunia digital.

### ***Akses Ilegal dan Keamanan Data Pribadi***

Pasal 30 UU ITE (Akses Ilegal)

- (1) Setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, akan dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
- (2) Dalam hal tindak pidana sebagaimana dimaksud pada ayat (1) mengakibatkan kerugian atau penyalahgunaan data pribadi, maka pelaku dapat dikenakan pidana tambahan sesuai ketentuan peraturan perundang-undangan yang berlaku.

Dalam industri fintech, perlindungan data pribadi sangat krusial, karena fintech mengumpulkan dan mengelola data sensitif dalam jumlah besar. Pasal 30 UU ITE sangat relevan di sini karena memberikan dasar hukum untuk menangani pelanggaran yang terjadi akibat akses ilegal terhadap data pribadi yang dikumpulkan oleh fintech. Di Indonesia, selain UU ITE, UU PDP No. 27 Tahun 2022 mengatur lebih lanjut tentang kewajiban penyelenggara untuk menjaga data pribadi dan melindungi pengguna. Ketika terjadi kebocoran data, Pasal 30 ini menjadi alat untuk memberikan hukuman kepada pihak yang bertanggung jawab atas kebocoran data melalui akses ilegal.

### ***Penegakan Hukum dan Sanksi***

UU ITE juga memberikan ketentuan terkait dengan penegakan hukum bagi pelaku yang melanggar ketentuan dalam transaksi elektronik dan penggunaan sistem elektronik. Fintech yang tidak mematuhi ketentuan dalam UU ITE, seperti yang berhubungan dengan perlindungan data atau yang terlibat dalam penipuan online, dapat dikenakan sanksi pidana atau denda sesuai dengan ketentuan dalam UU ITE. Misalnya, platform pinjaman online yang menawarkan produk secara ilegal atau yang melanggar ketentuan perlindungan data pribadi dapat dikenakan hukuman yang diatur dalam UU ITE. Hal ini terdapat dalam Pasal 27-37 (Pelanggaran Transaksi Elektronik dan Sanksi)

### ***Penyelesaian Sengketa dalam Transaksi Elektronik***

UU ITE juga mengatur mekanisme penyelesaian sengketa dalam transaksi elektronik, termasuk yang melibatkan platform fintech. Dalam industri fintech, seringkali ada sengketa antara pengguna dan penyedia layanan terkait transaksi atau pengelolaan data pribadi. UU ITE memberikan aturan tentang bagaimana sengketa dapat diselesaikan, baik melalui mekanisme mediasi atau melalui pengadilan. Penyelesaian sengketa dalam transaksi elektronik diatur dalam Pasal 45B-45I (Sengketa Elektronik).

Otoritas Jasa Keuangan (OJK) sebagai regulator sektor keuangan juga telah mengeluarkan POJK No. 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. Regulasi ini mengatur kewajiban penyelenggara fintech dalam melindungi data konsumen dan menerapkan prinsip perlindungan konsumen yang ketat.

### ***Implikasi Hukum atas Pelanggaran Perlindungan Data Pribadi oleh Fintech***

Pelanggaran terhadap perlindungan data pribadi dalam sektor fintech dapat memberikan implikasi hukum yang signifikan, baik bagi penyelenggara layanan fintech maupun konsumen. Dalam konteks Indonesia, pelanggaran ini tidak hanya berdampak pada reputasi dan kepercayaan konsumen, tetapi juga bisa berujung pada tuntutan hukum yang melibatkan sanksi administratif maupun pidana. Berdasarkan pembahasan sebelumnya mengenai konsep dan urgensi perlindungan data pribadi serta regulasi yang berlaku, implikasi hukum yang timbul dari pelanggaran perlindungan data pribadi oleh fintech di Indonesia dapat dijelaskan dalam beberapa poin berikut:

### ***Tuntutan Hukum Terhadap Penyelenggara Fintech***

Sebagaimana diungkapkan dalam pembahasan mengenai kebocoran data pribadi yang terjadi pada perusahaan fintech besar di Indonesia, pelanggaran terhadap perlindungan data pribadi dapat memicu tuntutan hukum dari konsumen yang dirugikan akibat kebocoran atau penyalahgunaan data pribadi mereka. Hal ini sejalan dengan ketentuan dalam UU PDP No. 27 Tahun 2022, yang mengatur kewajiban penyelenggara untuk memastikan bahwa data pribadi yang mereka kelola dilindungi secara sah dan aman.

### ***Kerugian Reputasi dan Penurunan Kepercayaan Konsumen***

Pelanggaran terhadap perlindungan data pribadi dapat merusak reputasi penyelenggara fintech, yang pada gilirannya berdampak pada kepercayaan konsumen. Seperti yang dijelaskan dalam bagian sebelumnya, keamanan data yang buruk dapat mengurangi kepercayaan konsumen terhadap layanan fintech, yang berakibat pada penurunan jumlah transaksi dan penurunan volume bisnis. Hal ini akan memperlambat pertumbuhan sektor fintech yang sedang berkembang pesat di Indonesia. Oleh karena itu, pelanggaran terhadap data pribadi dapat memiliki dampak hukum yang lebih luas, tidak hanya pada penyelenggara fintech tetapi juga pada perkembangan industri secara keseluruhan<sup>13</sup>.

### ***Pengawasan dan Penegakan Hukum oleh Regulator***

Dalam menghadapi pelanggaran perlindungan data pribadi, peran regulator seperti OJK dan Kominfo sangat penting dalam memastikan penegakan hukum yang efektif. Seperti yang telah dibahas dalam bagian 2, pengawasan yang lebih ketat terhadap implementasi regulasi oleh penyelenggara fintech, bersama dengan sanksi yang lebih tegas, dapat meningkatkan kepatuhan terhadap perlindungan data pribadi. OJK, BI, dan Kominfo memiliki peran strategis dalam menyusun kebijakan yang jelas, memberikan edukasi kepada konsumen, serta mengawasi praktik fintech agar tetap sesuai dengan standar perlindungan data pribadi yang diatur dalam UU PDP dan UU ITE<sup>14</sup>.

<sup>13</sup> Suwono, A. (2021). *Kepercayaan Konsumen dan Keamanan Data dalam Industri Fintech di Indonesia*, Jurnal Teknologi dan Bisnis, Vol. 19, hlm. 63-68.

<sup>14</sup> Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Pasal 59.

### ***Penyelesaian Sengketa dan Mekanisme Pengaduan***

Pelanggaran perlindungan data pribadi juga dapat berujung pada sengketa hukum antara konsumen dan penyelenggara fintech. Dalam hal ini, konsumen dapat mengajukan pengaduan kepada OJK atau lembaga penyelesaian sengketa yang ditunjuk. Hal ini sejalan dengan ketentuan dalam POJK No. 6/POJK.07/2022 yang mewajibkan penyelenggara fintech untuk memiliki mekanisme pengaduan yang jelas dan efisien. Penyelesaian sengketa ini diharapkan dapat memberikan keadilan bagi konsumen dan memastikan bahwa pelanggaran terhadap perlindungan data pribadi diselesaikan secara adil<sup>15</sup>.

### ***Tantangan dan Rekomendasi Penguatan Regulasi***

Meskipun regulasi terkait perlindungan data pribadi dalam fintech telah cukup berkembang, masih terdapat berbagai tantangan dalam implementasinya. Salah satu tantangan utama adalah lemahnya penegakan hukum terhadap pelanggaran perlindungan data pribadi. Banyak kasus kebocoran data yang tidak ditindaklanjuti dengan sanksi yang tegas, sehingga menimbulkan celah bagi pelaku untuk terus melakukan pelanggaran.

Pada Mei 2020, Tokopedia, salah satu *platform e-commerce* terbesar di Indonesia yang juga menawarkan layanan fintech, mengalami kebocoran data pribadi yang mencakup informasi lebih dari 91 juta akun pengguna. Data yang bocor termasuk nama pengguna, alamat email, nomor telepon, dan informasi terkait transaksi<sup>16</sup>.

Meskipun kasus ini tidak berujung pada denda langsung yang dijatuhkan oleh regulator, Tokopedia mendapat kecaman luas dari publik dan regulator terkait keamanan data pribadi. Pemerintah Indonesia melalui Kominfo dan OJK memperingatkan Tokopedia tentang pentingnya meningkatkan langkah-langkah keamanan data dan kepatuhan terhadap regulasi perlindungan data pribadi. Kejadian ini juga memicu pembicaraan lebih luas tentang perlunya UU Perlindungan Data Pribadi yang lebih kuat di Indonesia, yang akhirnya disahkan pada tahun 2022. Pada tahun yang sama, platform Bukalapak yang juga beroperasi di sektor *e-commerce* dan fintech, mengalami kebocoran data yang melibatkan 13 juta akun pengguna. Data yang bocor termasuk nama, alamat, nomor telepon, dan alamat email<sup>17</sup>.

Meskipun tidak ada denda formal yang diumumkan secara spesifik oleh Kominfo atau OJK, kasus ini menambah tekanan pada penyelenggara fintech untuk mematuhi regulasi yang lebih ketat terkait perlindungan data pribadi, termasuk UU ITE dan UU PDP yang mengatur kewajiban untuk melindungi data pribadi pengguna. Berbeda hal dengan yang terjadi di beberapa negara lain yang telah menerapkan peraturan terkait dengan perlindungan data pribadi. Contoh dari luar negeri, namun yang relevan untuk menunjukkan bagaimana kebocoran data di fintech dapat dikenakan denda berat, adalah kasus British Airways yang mengalami kebocoran data pribadi sekitar 500.000 pelanggan<sup>18</sup>. Kasus ini terkait dengan penyalahgunaan data pribadi pelanggan akibat serangan dunia maya yang mengakses informasi keuangan mereka. British Airways dikenakan denda sebesar £183 juta (sekitar Rp 3,5 triliun) oleh *Information Commissioner's Office* (ICO) di Inggris, berdasarkan pelanggaran *General Data Protection Regulation* (GDPR). Denda ini diterapkan karena kegagalan perusahaan dalam melindungi data pribadi pelanggan mereka dengan cara yang memadai.

Kasus Equifax, sebuah lembaga kredit dan penyelenggara fintech di AS, menjadi salah satu kebocoran data terbesar yang pernah tercatat, dengan sekitar 147 juta individu terkena dampaknya<sup>19</sup>. Equifax dikenakan denda sebesar \$575 juta (sekitar Rp 8,6 triliun) sebagai bagian dari penyelesaian terhadap gugatan yang diajukan oleh Komisi Perdagangan Federal AS (FTC), yang menyatakan bahwa Equifax gagal melindungi data pribadi konsumen dengan langkah-langkah keamanan yang memadai.

Melihat perbandingan antara Indonesia dengan negara lain, UU PDP dan peraturan teknis lainnya tidak memberikan efek yang signifikan terhadap penyelenggara layanan fintech. Diperlukan upaya lebih lanjut dalam meningkatkan pengawasan terhadap penyelenggara fintech agar patuh terhadap ketentuan perlindungan data pribadi. OJK dan BI perlu memperkuat mekanisme audit dan pemantauan secara berkala untuk memastikan keamanan sistem yang digunakan oleh fintech. Selain itu, diperlukan adanya inisiasi untuk membentuk suatu badan independen yang saling berkoordinasi dengan Kominfo, OJK, BI, BSSN dan lembaga penegak hukum lain yang terkait. Seperti halnya di Inggris dibentuk *Information Commissioner's Office* (ICO). Badan atau lembaga independen ini bertugas untuk melakukan pendampingan audit bersama Kominfo, OJK, BI dalam hal transaksi yang menyangkut dengan fintech.

<sup>15</sup> Peraturan Otoritas Jasa Keuangan (OJK) No. 6/POJK.07/2022 tentang Perlindungan Konsumen di Sektor Jasa Keuangan.

<sup>16</sup> Bappenas. (2020). *Studi Kasus Kebocoran Data dalam Industri Teknologi Finansial: Tokopedia*. Jakarta: Kementerian Perencanaan Pembangunan Nasional.

<sup>17</sup> Kominfo. (2020). *Kebocoran Data Bukalapak: Dampak dan Pelajaran untuk Industri Fintech di Indonesia*. Jurnal Perlindungan Data Pribadi.

<sup>18</sup> Information Commissioner's Office (ICO). (2019). *British Airways Fined £183 Million for Data Breach Under GDPR*. <https://ico.org.uk/>

<sup>19</sup> Federal Trade Commission (FTC). (2019). *Equifax Data Breach Settlement: Overview and Consequences*. <https://www.ftc.gov/>

Kemudian, harmonisasi peraturan yaitu UU PDP yang menjadi dasar hukum perlindungan data pribadi dengan peraturan lainnya agar dapat berjalan beriringan demi melindungi hak privasi warga negara dalam hal ini kaitannya dengan transaksi fintech. Harmonisasi peraturan perlu dikaji secara komprehensif dan berkesinambungan dengan peraturan lainnya. Karena fintech dapat mengandung unsur keperdataan maupun pidana tergantung dari sudut mana yang diambil. UU PDP sejatinya perlu mengatur lebih jelas dan mendefinisikan perlindungan data pribadi sebagai hak privasi yang berdasarkan UUD 1945 Pasal 28G ayat (1).

## KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa perlindungan data pribadi dalam transaksi fintech di Indonesia telah diatur dalam berbagai regulasi, namun implementasinya masih menghadapi tantangan. Penguatan regulasi, penegakan hukum yang lebih efektif, serta peningkatan literasi digital menjadi langkah strategis yang perlu dilakukan guna meningkatkan perlindungan data pribadi dalam ekosistem fintech di Indonesia.

## DAFTAR PUSTAKA

### *Buku*

- Dewi, S. (2020). *Perlindungan konsumen di era digital: Isu dan tantangan* (hlm. 185–186). Jakarta: Penerbit Buku Kompas.
- Fauji, D. A., & Widodo, M. W. (2020). *Financial technology*. Kediri: Penerbit Fakultas Ekonomi Universitas Nusantara PGRI Kediri.
- Haris, H. (2023). *Perlindungan data pribadi dan implikasinya terhadap penyelenggara fintech di Indonesia* (hlm. 220–225). Bandung: Refika Aditama.
- Schwab, K. (2016). *The fourth industrial revolution*. Geneva: World Economic Forum.
- Sundari, R. (2019). *Tantangan implementasi UU PDP dalam sektor fintech di Indonesia* (hlm. 95–98). Yogyakarta: Gadjah Mada University Press.

### *Jurnal Ilmiah*

- Croys Diansyah A., dkk. (2023). Perlindungan data pribadi konsumen financial technology (fintech) berdasarkan Peraturan OJK No. 77/POJK.01/2016 dan Peraturan BI No. 22/20/PBI/2020. *Madani*, 1(5), 228–240.
- Fitriyani Pakpahan, E., Chandra, L. R., & Dewa, A. A. (2020). Perlindungan hukum terhadap data pribadi dalam industri financial technology. *Veritas et Justitia*, 6(2), 298–323.
- Rifa, F., & Hidayati, M. N. (2024). Perlindungan data pribadi dalam industri fintech Indonesia. *Jurnal Teknologi dan Keamanan Informasi*.
- Rifa, F., & Hidayati, M. N. (2024). Hukum perlindungan data pribadi dalam fintech di Indonesia. *Jurnal Hukum Indonesia*, 14(2), 132–136.
- Saputra, D. F. (2023). Literasi digital untuk perlindungan data pribadi. *Jurnal Ilmu Kepolisian*, 17(3), 1–8.
- Suwono, A. (2021). Kepercayaan konsumen dan keamanan data dalam industri fintech di Indonesia. *Jurnal Teknologi dan Bisnis*, 19, 63–68.
- Kominfo. (2020). Kebocoran data Bukalapak: Dampak dan pelajaran untuk industri fintech di Indonesia. *Jurnal Perlindungan Data Pribadi*.

### *Artikel / Paper / Laporan Ilmiah / Prosiding*

- Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? *University of New South Wales Law Research Series*, No. 2016-62. <https://ssrn.com/abstract=2676553>
- Hermann, M., Pentek, T., & Otto, B. (2016). *Design principles for Industrie 4.0 scenarios*. Institute of Information Management, University of St. Gallen.
- PwC. (2020). *Consumer data privacy: Global survey 2020*. PricewaterhouseCoopers International Limited. <https://doi.org/10.56211/rechtsnormen.v4i1.1153>

Bappenas. (2020). *Studi kasus kebocoran data dalam industri teknologi finansial: Tokopedia*. Jakarta: Kementerian Perencanaan Pembangunan Nasional.

Information Commissioner's Office (ICO). (2019). *British Airways fined £183 million for data breach under GDPR*. <https://ico.org.uk/>

### **Berita / Artikel Online**

Makarim, E. (2020, Juli 9). Pertanggungjawaban hukum terhadap kebocoran data pribadi. *Hukumonline.com*. <https://www.hukumonline.com/berita/a/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-lt5f067836b37ef/> (Diakses 15 Maret 2025)

Rizki, M. J. (2019, September 23). Perlindungan data konsumen harus jadi prioritas industri fintech. *Hukumonline.com*. <https://www.hukumonline.com/berita/a/perlindungan-data-konsumen-harus-jadi-prioritas-industri-fintech-lt5d887b1ba7f91/> (Diakses 15 Maret 2025)

### **Peraturan Perundang-undangan**

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Pasal 26.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), Pasal 59.

Peraturan Otoritas Jasa Keuangan (OJK) No. 6/POJK.07/2022 tentang Perlindungan Konsumen di Sektor Jasa Keuangan.