

TINJAUAN HUKUM KEBOCORAN DATA PRIBADI TERHADAP KEPERCAYAAN KONSUMEN DI INDUSTRI FINANSIAL TEKNOLOGI (*FINTECH*)¹

Oleh :

Agnes Juliet Goni²

Christine J. J. G Goni³

Jolanda M. Korua⁴

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimana pengaturan hukum terhadap kebocoran data pribadi konsumen finansial teknologi (*fintech*) dan untuk mengetahui bagaimana perlindungan terhadap korban kebocoran data pribadi konsumen finansial teknologi (*fintech*). Metode yang digunakan adalah yuridis normatif, dengan kesimpulan yaitu: 1. Terdapat beberapa aturan sebagai bentuk perlindungan hukum bagi konsumen *fintech* di Indonesia seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Otoritas Jasa Keuangan (OJK) terkait keamanan data dalam layanan *fintech*, serta beberapa Peraturan Bank Indonesia mengenai *Fintech*. Lebih khusus mengenai kebocoran data pribadi konsumen *fintech*, diatur di dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) Pasal 57 dan Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 Tahun 2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi. 2. Bentuk perlindungan terhadap korban konsumen kebocoran data *fintech*, terdapat beberapa langkah hukum jika data pribadi disalahgunakan sesuai dengan peraturan perundang-undangan yang berlaku yang dalam hal ini adalah UU Perlindungan Data Pribadi (UU PDP) dan Peraturan OJK (POJK). Langkah-langkah hukum tersebut diantaranya, Melaporkan ke Lembaga Terkait, Menggugat Secara Perdata, Melaporkan Secara Pidana.

Kata Kunci : *kebocoran data pribadi, fintech*

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi yang sangat pesat telah mengubah pola hidup masyarakat Indonesia seperti dalam hal sistem keuangan, dimana masyarakat yang dulunya masih melakukan transaksi keuangan secara konvensional (misalnya pembayaran dengan uang tunai, dompet saku, atau melakukan pinjaman uang di bank) berkat perkembangan teknologi masyarakat melakukan transaksi uang secara digital (misalnya *e-wallet*, pinjaman online, dsb).

Sistem keuangan pada dasarnya adalah suatu kesatuan yang terdiri atas lembaga jasa keuangan, pasar keuangan, dan infrastruktur keuangan, termasuk sistem pembayaran, yang berinteraksi dalam memfasilitasi pengumpulan dana masyarakat dan pengalokasiannya untuk mendukung aktivitas perekonomian nasional, serta korporasi dan rumah tangga yang terhubung dengan lembaga jasa keuangan.

Sistem keuangan berfungsi sebagai fasilitator perdagangan domestik dan internasional, mobilisasi simpanan menjadi berbagai instrumen investasi dan menjadi perantara antara penabung dengan pemberi pinjaman. Stabilitas dan pengembangan sistem keuangan sangat penting agar masyarakat meyakini bahwa sistem keuangan Indonesia aman, stabil, dan dapat memenuhi kebutuhan pengguna jasa keuangan.⁵

Indonesia merupakan negara dengan penduduk terbanyak ke-4 di dunia dimana kurang lebih 79% penduduk Indonesia merupakan pengguna internet. Tentu dengan jumlah pengguna internet yang sebanyak itu maka kegiatan yang menggunakan internet akan sangat masif dan berlangsung setiap hari sehingga rentan terjadinya kebocoran data dari para pengguna tersebut.

Era digital telah membawa perubahan besar dalam cara informasi pribadi dikelola. Data pribadi menjadi aset yang sangat berharga bagi perusahaan karena dapat digunakan untuk menganalisis kebiasaan, preferensi, dan kebutuhan konsumen. Namun, dengan besarnya jumlah data yang dikelola, risiko pelanggaran keamanan semakin tinggi. Perlindungan data pribadi bukan hanya isu teknis, tetapi juga menyangkut hak privasi individu yang harus dijaga oleh perusahaan penyedia layanan digital, termasuk *fintech*.

Lembaga keuangan, sebagaimana halnya suatu lembaga atau institusi pada hakikatnya

¹ Artikel Skripsi

² Mahasiswa Fakultas Hukum Unsrat, NIM 210711010144

³ Dosen Fakultas Hukum Unsrat, Magister Ilmu Hukum

⁴ Dosen Fakultas Hukum Unsrat, Magister Ilmu Hukum

⁵ Djoni S. Gazali, Rachmadi Usman, *Hukum Perbankan*, Jakarta: Sinar Grafika, 2016, hlm. 41.

berada dan ada di tengah-tengah masyarakat. Lembaga yang merupakan organ masyarakat merupakan “sesuatu” yang keberadaannya adalah untuk memenuhi tugas sosial dan kebutuhan khusus bagi masyarakat. Berbagai jenis lembaga ada dan dikenal masyarakat yang masing-masing mempunyai maksud dan tujuan dari tiap lembaga yang bersangkutan.⁶

Salah satu produk dari perkembangan teknologi adalah *Fintech*, *fintech* sendiri adalah singkatan dari *financial technology*, yang berarti teknologi keuangan. *Fintech* merupakan inovasi yang menggabungkan teknologi dengan jasa keuangan, sehingga dapat mengubah cara nasabah mengakses layanan keuangan.

Jumlah perusahaan *fintech* di Indonesia pada tahun 2024 yang terdaftar Otoritas Jasa Keuangan (OJK) adalah 98 perusahaan penyelenggara *fintech lending* dan 97 perusahaan penyelenggara *fintech peer-to-peer lending*. Beberapa contoh *fintech* di Indonesia misalnya: Doku, Finansialku, Kudo, Cicil.co.id, Go Pay, Cermati.com, KoinWorks, Kredivo. Adapun P2PL merupakan pemanfaatan teknologi finansial yang ditujukan untuk peminjaman sejumlah dana dari kreditur kepada debitur.⁷

Kebocoran data pribadi adalah masalah serius yang dapat berdampak signifikan pada industri finansial teknologi (*fintech*). Dalam era digital, data pribadi menjadi salah satu aset yang sangat berharga. Kemajuan teknologi telah memungkinkan perusahaan untuk mengumpulkan, menyimpan, dan memanfaatkan data konsumen dalam jumlah besar untuk memberikan layanan yang lebih personal dan efisien. Namun, seiring dengan meningkatnya penggunaan data digital, risiko pelanggaran keamanan data juga semakin tinggi.

Perlindungan data pribadi menjadi sangat penting karena data ini dapat mencakup informasi sensitif seperti identitas, informasi keuangan, dan riwayat aktivitas online. Ketika data ini bocor atau disalahgunakan, dampaknya dapat sangat merugikan, baik bagi individu yang datanya tercemar maupun bagi perusahaan yang kehilangan kepercayaan konsumen. Keamanan data tidak hanya terkait dengan privasi, tetapi juga menyangkut stabilitas ekonomi dan kepercayaan masyarakat terhadap ekosistem digital.

Industri *fintech*, yang berbasis pada layanan digital dan memanfaatkan data pribadi konsumen

untuk berbagai layanan keuangan, menghadapi risiko yang besar apabila data-data tersebut tidak dilindungi dengan baik. Kebocoran data pribadi tidak hanya mengancam keamanan informasi konsumen, tetapi juga berpotensi merusak hubungan kepercayaan antara konsumen dan perusahaan *fintech*.

Kebocoran data pribadi adalah masalah serius yang dapat berdampak signifikan pada industri finansial teknologi (*fintech*). Ketika data pribadi konsumen, seperti informasi keuangan, identitas, dan riwayat transaksi, bocor atau disalahgunakan, hal ini dapat merusak kepercayaan konsumen terhadap perusahaan *fintech*. Kebocoran data pribadi menyebabkan konsumen merasa tidak aman menggunakan layanan *fintech*.

Ketika konsumen merasa data pribadi mereka tidak terlindungi, kepercayaan terhadap kemampuan perusahaan *fintech* dalam menjaga privasi dan keamanan data menurun. Reputasi perusahaan *fintech* yang mengalami kebocoran data dapat terpengaruh secara negatif. Media dan opini publik seringkali memperbesar dampak insiden tersebut, mengakibatkan persepsi negatif yang dapat bertahan lama dan mempengaruhi keberlanjutan bisnis perusahaan tersebut.

Secara keseluruhan, kebocoran data pribadi memiliki dampak yang merugikan terhadap kepercayaan konsumen dalam industri *fintech*. Oleh karena itu, penting bagi perusahaan *fintech* untuk mengimplementasikan langkah-langkah keamanan data yang ketat, transparan dalam penanganan data, dan cepat menanggapi insiden kebocoran data untuk memulihkan kepercayaan konsumen dan menjaga reputasi mereka.

Beberapa dampak kebocoran data konsumen *fintech*, seperti: hilangnya kepercayaan konsumen, kerugian finansial konsumen, gangguan privasi konsumen, dampak psikologis pada konsumen. Selain memiliki dampak terhadap konsumen, kebocoran data pribadi konsumen juga berdampak pada perusahaan *fintech* seperti: kerugian finansial dan reputasi bagi perusahaan *fintech*, serta terganggunya ekosistem *fintech*.

Indonesia mencatatkan namanya sebagai salah satu dari 10 besar negara dengan tingkat kebocoran data tertinggi di dunia. Data ini diungkapkan oleh Kepala Eksekutif Pengawas Perasuransian, Penjaminan, dan Dana Pensiun Otoritas Jasa Keuangan (OJK), Ogi Prastomiyono, dalam acara Risk and Governance Summit 2024. Kebocoran data ini tidak hanya berdampak pada privasi, tetapi juga memberikan kerugian finansial yang besar. Berdasarkan data tahun 2023, lebih dari 350 juta serangan siber terjadi, dengan total

⁶ Neni Sri Imaniyati, *Pengantar Hukum Perbankan di Indonesia*, Reika Aditama, Bandung, 2010, hlm. 2.

⁷ Diah Ayu Septi Fauji dan Moch. Wahyu Widodo, *Financial Technology*, Kediri: Fakultas Ekonomi, Universitas Nusantara PGRI Kediri, 2020, hlm.. 24

kerugian mencapai minimal 1 juta dolar AS atau sekitar Rp15,9 miliar.⁸

Beberapa contoh kasus kebocoran data pribadi di industri fintech, misalnya:

1. Bank Indonesia, Pada Januari 2022, Bank Indonesia mengalami serangan siber dari grup ransomware bernama Conti. Grup itu diduga mencuri 228 gigabyte (GB) data dari 513 komputer. Pada awalnya, Conti hanya mengunggah 487 MB data yang diklaim dicuri dari BI, tetapi kemudian terus bertambah hingga 228 GB. Sebelumnya pada Desember 2021 Bank Indonesia juga sudah mengakui bahwa pihaknya mengalami serangan ransomware. Peretasan itu sudah dilaporkan ke Badan Siber dan Sandi Negara (BSSN) dan aparat kepolisian.
2. Bank Jatim, Pada Oktober 2021, beredar informasi database Bank Jatim (BJTM) bocor. Dilansir Antara, database Bank Jatim dijual di forum pengumpul data hasil kebocoran database RaidForums. Database tersebut dijual dengan harga US\$250.000 sebesar 378 GB yang berisi data seperti data nasabah, data karyawan, data keuangan pribadi, dan lainnya. Penjelasan manajemen Bank Jatim kala itu menyebutkan dari hasil penelusuran awal pelaku kejahatan siber melakukan instruksi pada sistem aplikasi pendukung dan bukan pada core system. Dengan demikian, data nasabah disebut tetap terjaga dan nasabah bisa melakukan transaksi keuangan dengan aman.
3. Fintech Cermati Cermati.com menjadi salah satu korban yang datanya diretas oleh hacker global. Bersamaan dengan Cermati, terdapat 16 perusahaan yang juga dibobol oleh hacker dengan total 34 juta akun database. Dari foto yang diperlihatkan Bleepingcomputer Total sekitar 2,9 juta akun Cermati.com diretas oleh hacker tersebut. Data yang dicuri antara lain email, alamat, nomor telepon, pendapatan, id, pekerjaan, nama perusahaan, dan nama ibu.⁹

Hukum perlindungan data pribadi menjadi landasan utama dalam mengatasi tantangan ini, mengingat perlunya menyeimbangkan kemajuan teknologi dengan hak-hak individu untuk menjaga privasi mereka. Konsep perlindungan data pribadi

menyoroti hak setiap individu untuk mengatur nasib informasi mereka, termasuk kebebasan memilih apakah akan berbagi data atau tidak dan menetapkan syarat tertentu jika memilih untuk berbagi dalam komunitas. Informasi seperti nama, email, akun media sosial, dan nomor rekening yang sering diminta oleh aplikasi untuk berbagai tujuan, termasuk verifikasi kebenaran data, bisa berisiko disalahgunakan. Misalnya, penipuan lewat telepon, peretasan rekening bank, atau perampokan yang diarahkan pada pemilik data berdasarkan informasi pribadi mereka.¹⁰

Di Indonesia sendiri terdapat beberapa aturan hukum yang mengatur tentang perlindungan data pribadi seperti:

1. Undang-Undang (UU) Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP);
2. Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.
3. Peraturan Otoritas Jasa Keuangan (OJK) terkait keamanan data dalam layanan fintech;
4. Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;
5. Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial (PBI Tekfin);
6. Peraturan Bank Indonesia No 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia.

B. Rumusan Masalah

1. Bagaimana pengaturan hukum terhadap kebocoran data pribadi konsumen finansial teknologi (*fintech*)?
2. Bagaimana perlindungan terhadap korban kebocoran data pribadi konsumen finansial teknologi (*fintech*)?

C. Metode Penelitian

Penelitian ini adalah penelitian yuridis-normatif.

PEMBAHASAN

A. Konsumen Yang Pengaturan Hukum Terhadap Penyalahgunaan Data Pribadi Konsumen Teknologi Finansial (*Fintech*).

Pada perkembangan *fintech* di Indonesia sejumlah permasalahan pun bermunculan.

⁸ Rita Puspita Sari, *RI Masuk 10 Besar Kebocoran Data, Hampir 100 Juta Akun Bocor*, <https://csirt.or.id/berita/ri-masuk-10-besar-kebocoran-data>, (diakses tanggal 7 Februari 2025).

⁹ Annisa Sulisty Rini, *Daftar Kasus Kebocoran Data Sektor Finansial RI Selain BSI (BRIS)*, <https://finansial.bisnis.com/read/20230516/90/1656438/daf-tar-kasus-kebocoran-data-sektor-finansial-ri-selain-bsi-bris>, (diakses tanggal 8 Februari 2025)

¹⁰ Jefri Arnolius Pasaribu, *Perlindungan Data Pribadi: Tantangan Hukum di Era Digital*, K Law (General), 2023, hlm.4.

Misalnya yang berkaitan dengan perusahaan fintech dan konsumen yang menggunakan layanan *fintech* tersebut. Salah satu permasalahan hukum yang muncul pada industri *fintech* ini adalah tentang bagaimana perlindungan terhadap data pribadi konsumen. Hal ini sangat penting mengingat dalam industri *fintech* khususnya pada peer to peer lending, banyak terjadi data pribadi konsumen yang disalahgunakan, seperti akses terhadap kontak telepon milik konsumen. Kontak telepon itu sejatinya digunakan untuk memastikan bahwa peminjam uang benar-benar orang yang namanya tercantum dalam form. Beberapa kasus akses kontak digunakan untuk melakukan penagihan. Penggunaan data pribadi dalam penyedia layanan *fintech* tidak jarang disalahgunakan dan diakses untuk keperluan diluar transaksi yang disediakan penyedia *fintech*. Pada kasus lain, terdapat perusahaan *fintech* yang menyebarluaskan dan memperjualbelikan data konsumen tanpa seizin bersangkutan. Dengan adanya kebocoran data yang diperjualbelikan secara illegal tersebut, bukan saja merugikan pengguna (konsumen) tetapi juga merugikan kredibilitas dari pelaku usaha tersebut.¹¹

Kepercayaan merupakan fondasi penting dalam hubungan antara konsumen dan penyedia layanan, termasuk platform *fintech*. Kepercayaan ini didasarkan pada ekspektasi konsumen bahwa informasi pribadi yang mereka berikan akan dijaga kerahasiaannya dan dilindungi dari akses atau penggunaan yang tidak sah. Insiden kebocoran data secara langsung merusak ekspektasi ini dan mengakibatkan erosi kepercayaan yang mendalam.

Persepsi konsumen terhadap keamanan data pribadi di platform *fintech* telah mengalami perubahan signifikan, terutama setelah berbagai insiden kebocoran data yang marak terjadi dalam beberapa tahun terakhir. Banyak konsumen kini merasa ragu dan was-was terhadap keamanan informasi pribadi mereka, terutama data sensitif seperti nomor KTP, rekening bank, data penghasilan, dan informasi kontak darurat. Terdapat beberapa faktor yang dinilai memperburuk persepsi konsumen terhadap *fintech* pascakebocoran data, faktor tersebut meliputi:

1. Transparansi yang Rendah: Banyak perusahaan *fintech* tidak memberikan

informasi jelas tentang langkah mitigasi pascakebocoran.

2. Respons Lambat: Penanganan insiden yang tidak cepat memperparah ketidakpercayaan.
3. Minimnya Edukasi: Konsumen sering tidak paham hak-hak hukum mereka terkait perlindungan data.

Hukum harus menempatkan secara individu sebagai pusatnya, yang memastikan data pribadi harus di lindungi, terlepas dimana mereka harus di dalam atau luar wilayahnya. Dalam hukum data pribadi ini kana meninjau dari suatu hak privai seseorang juga, baik dari privasi merupakan suatu konsep yang bersifat universal dan dikenal di berbagai negara baik tertulis maupun tidak tertulis, dalam bentuk Undang-Undang maupun tidak tertulis dalam bentuk aturan moral¹²

Kebocoran data pribadi di industri *fintech* tidak hanya menimbulkan kerugian materiil tetapi juga mengikis kepercayaan konsumen. Persepsi negatif ini muncul karena data finansial (seperti riwayat transaksi, pinjaman, dan informasi rekening) bersifat sangat sensitif dan rentan disalahgunakan untuk tindak pidana seperti penipuan, pemalsuan identitas, atau pemerasan.

Secara yuridis, persepsi negatif ini menunjukkan bahwa prinsip *transparency* dan *accountability* sebagaimana diamanatkan dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) belum diimplementasikan secara maksimal. Padahal, Pasal 20 ayat (1) UU PDP mewajibkan pengendali data untuk memberikan pemberitahuan secara tertulis kepada pemilik data apabila terjadi kebocoran data, sesuatu yang kerap tidak dilakukan oleh perusahaan *fintech*.

Kepercayaan konsumen merupakan elemen krusial yang dilindungi oleh Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK). Pasal 4 UUPK menjamin hak konsumen atas kenyamanan, keamanan, dan privasi. Jika *fintech* gagal memenuhi kewajiban ini, mereka dapat dikategorikan melanggar prinsip itikad baik dalam perjanjian (Pasal 1338 KUHPerdata).

Insiden kebocoran data menimbulkan kekhawatiran terhadap bagaimana data pribadi mereka dikelola, disimpan, dan digunakan. Banyak konsumen merasa tidak memperoleh informasi yang memadai terkait pengelolaan data oleh penyelenggara *fintech*, serta tidak memiliki kendali terhadap data yang telah diberikan dalam

¹¹ Croy 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: Jurnal Ilmiah Multidisiplin, Vol. 1 No. 5, 2023, hlm. 231.

¹² Sinta Dewi Rosadi, *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Bandung: Widya Padjajaran, 2009, hlm. 45.

rangka pengajuan pinjaman online. Hal ini menyebabkan penurunan tingkat kepercayaan terhadap platform fintech secara umum.

Ketentuan Pasal 26 ayat (1) UU Informasi dan Transaksi Elektronik dinyatakan yaitu, “kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan”. Berdasarkan ketentuan tersebut, korelasi antara penerapan teknologi informasi dengan privasi rights dapat diartikan sebagai: a. Hak individu dalam rangka menikmati privasinya secara bebas serta jauh dari berbagai ancaman/gangguan dari pihak manapun; b. Hak individu untuk menjalin komunikasi/hubungan relasi dengan semua orang tanpa kecuali dengan terbebas dari kegiatan “spionase”; dan c. Hak individu melakukan pengawasan terhadap informasi-informasi berkenaan dengan privasi orang lain.¹³

Mega Lois Aprilia (2020) pada penelitian ilmiah Perlindungan Konsumen *Financial Technology Peer To Peer Lending* Di Indonesia Terhadap Kerugian Akibat Tindakan Doxing menemukan kebocoran data dikarenakan penyalahgunaan yang dilakukan oleh pihak jasa keuangan dengan cara menyebarkan informasi soal peminjaman dan data pribadi konsumen dengan cara membuat Grup WhatsApp yang isinya daftar kontak telepon peminjam disertai dengan kalimat bahwa orang tersebut telah meminjam uang dengan jumlah tertentu bahkan pihak jasa keuangan juga melakukan nada intimidasi dan berupa kekerasan fisik ditempat umum jika tidak melunasi hutang maka data pribadinya akan disebar luaskan, M. Olifiansyah (2021) menemukan bahwa data konsumen pihak jasa keuangan memberikan data kepada pihak ketiga sebagai debt collector untuk melakukan penagihan yang tidak sesuai aturan.¹⁴

Kebocoran data di sektor fintech, seperti pada aplikasi pinjaman online (pinjol), telah menunjukkan celah besar dalam sistem keamanan siber dan kepatuhan terhadap regulasi perlindungan data. Konsumen yang sebelumnya merasa percaya kepada layanan digital karena

kemudahan dan kecepatan proses, kini menjadi lebih skeptis terhadap jaminan keamanan data yang diberikan oleh penyedia layanan.

Peningkatan kekhawatiran ini secara langsung memengaruhi perilaku konsumen. Mereka menjadi lebih hati-hati dalam memberikan informasi pribadi saat menggunakan platform fintech, cenderung mengurangi frekuensi penggunaan layanan, atau bahkan beralih ke platform lain yang dianggap memiliki reputasi keamanan yang lebih baik. Dari perspektif hukum, sikap kehati-hatian konsumen ini merupakan respons yang wajar terhadap potensi risiko yang timbul akibat kelalaian platform dalam menjaga keamanan data.

Faktor lain yang memperburuk persepsi konsumen adalah kurangnya penegakan hukum terhadap pelaku kebocoran data dan lemahnya sanksi terhadap pelanggaran yang dilakukan oleh perusahaan fintech. Ketika insiden kebocoran data terjadi, tidak ada mekanisme yang jelas dan transparan mengenai penyelesaian sengketa atau ganti rugi terhadap korban.

Insiden kebocoran data di platform *fintech* dapat secara signifikan memengaruhi persepsi konsumen terhadap keamanan data pribadi mereka:

1. Penurunan Kepercayaan: Kebocoran data sering kali mengakibatkan penurunan drastis kepercayaan konsumen terhadap platform fintech yang bersangkutan. Mereka merasa bahwa platform tersebut tidak mampu menjaga informasi sensitif mereka dengan baik. Kepercayaan yang hilang ini sulit untuk dipulihkan.
2. Peningkatan Kekhawatiran: Konsumen menjadi lebih khawatir tentang potensi penyalahgunaan data pribadi mereka setelah insiden kebocoran. Kekhawatiran ini meliputi risiko penipuan finansial, pencurian identitas, dan penggunaan data untuk tujuan yang tidak sah lainnya.
3. Sikap Lebih Hati-hati: Setelah mengalami atau mendengar tentang kebocoran data, konsumen cenderung lebih berhati-hati dalam menggunakan platform fintech. Mereka mungkin menjadi enggan untuk memberikan informasi pribadi baru, mengurangi frekuensi penggunaan aplikasi, atau bahkan beralih ke platform lain yang dianggap lebih aman.
4. Tuntutan Transparansi dan Akuntabilitas: Konsumen menuntut transparansi yang lebih besar dari platform fintech terkait langkah-langkah keamanan yang mereka terapkan dan bagaimana mereka menanggapi insiden kebocoran data. Mereka juga mengharapkan

¹³ Ni Nyoman Ratna Dewi, Ayu Putu Laksmi Danyathi, *Perlindungan Hukum Bagi Pengguna Situs Pinjaman Dana Online Dari Tindakan Penyalahgunaan Data Pribadi*, ojs.unud.ac.id, 2022, Hlm.81.

¹⁴ Andri Soemitra, Adlina Hasan, *Perlindungan Konsumen Terhadap Kebocoran Data Pada Jasa Keuangan Di Indonesia*, Juripol (Jurnal Institusi Polgan), Vol. 5 No. 1, 2022, hlm. 294.

adanya akuntabilitas dan kompensasi yang jelas jika data mereka disalahgunakan akibat kelalaian platform.

Perlindungan hukum atas data/informasi mencakup langkah-langkah untuk melindungi keamanan data pribadi dan ketentuan terkait penggunaan data pribadi. Secara umum, perlindungan hukum adalah cara untuk mewujudkan hak individu dan memberikan rasa aman kepada individu, salah satunya tampak ditujukan bagi pihak yang dirugikan atas adanya kejahatan yang bentuk perlindungan hukumnya dapat berupa ganti rugi maupun bentuk-bentuk lainnya.¹⁵

Pelaksanaan pelindungan data pribadi di Indonesia memiliki suatu landasan filosofis. Landasan filosofisnya ialah Pancasila dan Undang-Undang Dasar NKRI Tahun 1945 Hasil Amandemen ke-IV (UUD 1945). Dalam Pasal 28G ayat (1) UUD 1945 terdapat amanat mengenai hak setiap individu untuk dilindungi terhadap segala aspek yang berkaitan dengan dirinya, baik itu perlindungan atas diri pribadinya, keluarganya, martabat dan kehormatannya, maupun harta benda yang berada di bawah kekuasaannya. Selain itu, setiap individu juga memiliki hak untuk merasa aman dan dilindungi dari segala ancaman ketakutan yang dapat mempengaruhi hak asasinya. (UUD 1945, Ps. 28G ayat (1)) Oleh karenanya, masyarakat perlu memiliki pemahaman dan kesadaran hukum akan kemanusiaan dalam konteks pelindungan privasi dan data dirinya.¹⁶

UUPK memiliki tiga prinsip dasar, yaitu hak untuk mendapatkan dan membeli barang dan jasa dengan harga yang sesuai dengan harga pasar (wajar), hak untuk melindungi konsumen dari kerugian, dan hak untuk menyelesaikan sengketa perlindungan konsumen. Penting bagi masyarakat untuk menyadari bahwa konsumen perlu dilindungi secara hukum. Administrasi Jasa Keuangan menetapkan peraturan berikut untuk mengatur pinjaman online:¹⁷

- 1) Peraturan POJK Nomor 1/POJK.07/2013 tentang "Perlindungan Konsumen Sektor Jasa Keuangan" sebagai berikut:
 - a. Transparan;
 - b. Adil terhadap konsumen;
 - c. Berpengalaman dan dapat diandalkan;
 - d. Menjaga data pelanggan aman dan rahasia
 - e. Menerima pengaduan pelanggan dan menyelesaikan masalah dengan cara yang mudah, jelas, cepat, dan murah.
 - 2) Pengaturan Pinjam Meminjam Uang Berbasis Teknologi Informasi (PJOK) NOMOR 77/PJOK.01/2016 tentang Layanan.
 - 3) Surat Edsaran Otoritas Jasa Keuangan Nomor 18/SEOJK.02/2017. Setelah berlakunya POJK Nomor 77/POJK.01/2016 tentang "Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi", Otoritas Jasa Keuangan telah menetapkan persyaratan untuk menerapkan tata kelola dan manajemen risiko teknologi informasi pada sistem pinjam meminjam uang berbasis teknologi.
 - 4) Surat Edaran Otoritas Jasa Keuangan No.014/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data Konsumen
- Perlindungan hukum terhadap penyalahgunaan data pribadi terhadap *financial technology* di Indonesia diatur oleh beberapa peraturan perundang-undangan, yang diantaranya:
1. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP): UU PDP merupakan landasan hukum utama yang mengatur seluruh aspek perlindungan data pribadi, termasuk dalam konteks perjanjian pinjaman online. Beberapa poin penting dalam UU PDP terkait hal ini:
 - a) Prinsip Pemrosesan Data Pribadi: Pemrosesan data pribadi harus dilakukan secara sah, adil, transparan, terbatas, dan akurat. Persetujuan eksplisit dari pemilik data menjadi salah satu dasar sah pemrosesan.
 - b) Hak Pemilik Data Pribadi: Konsumen sebagai pemilik data pribadi memiliki berbagai hak, termasuk hak untuk mengakses, memperbaiki, menghapus, menarik persetujuan, dan mengajukan keberatan terhadap pemrosesan data mereka.
 - c) Kewajiban Pengendali Data Pribadi (Platform Fintech): Platform fintech sebagai pengendali data pribadi memiliki kewajiban untuk menerapkan langkah-langkah keamanan yang memadai, memberitahukan pemilik data jika terjadi kebocoran data, dan bertanggung jawab

¹⁵ Dewi, Sinta. *Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia*. Yustisia Jurnal Hukum 5, no. 1, 2016, hlm. 35-53.

¹⁶ Gita Theresa, *Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintech di Indonesia*, Jurnal Darma Agung, Vol. 32 No.3, 2024, hlm. 357

¹⁷ Shafa Rosedila, *Analisis Perlindungan Konsumen Terhadap Pelanggaran Hak Informasi Pribadi Pada Pinjaman Berbasis Online*, Vol. 17, 2024, hlm. 128-129.

atas kerugian yang timbul akibat penyalahgunaan data karena kelalaian mereka.

- d) Sanksi Pelanggaran: UU PDP mengatur sanksi administratif (peringatan tertulis, denda administratif, penghentian sementara kegiatan pemrosesan data pribadi) dan sanksi pidana (pidana penjara dan/atau denda) bagi pelanggaran ketentuan perlindungan data pribadi.
2. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK): Meskipun fokus utamanya bukan pada data pribadi, UUPK juga relevan dalam konteks perjanjian pinjaman online. Konsumen memiliki hak atas informasi yang benar, jelas, dan jujur mengenai produk dan layanan, termasuk bagaimana data pribadi mereka akan digunakan dan dilindungi. Pelaku usaha (platform fintech) memiliki kewajiban untuk memberikan informasi tersebut.
3. Peraturan Otoritas Jasa Keuangan (POJK): OJK sebagai regulator sektor keuangan juga mengeluarkan berbagai peraturan yang mengatur penyelenggaraan layanan pinjaman online, termasuk aspek perlindungan data konsumen. POJK dapat mengatur standar keamanan data, kewajiban penyedia pinjaman untuk menjaga kerahasiaan data, dan mekanisme penanganan pengaduan terkait penyalahgunaan data.
4. Kitab Undang-Undang Hukum Perdata (KUHPerdata): Asas itikad baik dalam perjanjian juga relevan. Platform fintech diharapkan bertindak dengan itikad baik dalam mengelola data pribadi konsumen dan tidak menyalahgunakannya.

Melalui aturan BI Nomor 19/12/PBI/2017 dapat diketahui ruang lingkup kegiatan dari *financial technology*, sebagai berikut:

- a) Skema pembayaran/digital payment;
- b) Pendukung pasar;
- c) Manajemen investasi serta resiko;
- d) Kredit/pinjaman, pembiayaan serta penyediaan modal; dan
- e) Jasa finansial lainnya.

Kedudukan OJK di sini untuk menjalankan sistem pengawasan secara menyeluruh aspek jasa keuangan, dengan demikian *financial technology* ini pun juga menjadi yurisdiksi pengawasan OJK. Dalam hal perlindungan konsumen (termasuk konsumen *financial technology*), OJK mengeluarkan beberapa kebijakan, seperti POJK Nomor 01/POJK.07/2013 dalam Pasal 2, yang mana pada pokoknya konsumen (termasuk konsumen *financial technology*) dilindungi

berdasarkan beberapa prinsip yakni adil, transparansi, keandalan, penyelesaian pengaduan dan sengketa yang cepat sederhana yang berbiaya ringan, serta jaminan keamanan data pribadi. Adapun secara spesifik diatur mengenai batasan yang tidak boleh dilakukan oleh POJK terhadap data pribadi pengguna layanan dapat dilihat pada pada Pasal 31.¹⁸

Perusahaan *e-commerce* mempunyai kewajiban untuk mencegah kebocoran data pribadi dengan melindungi keamanan data pribadi dari pengaksesan, pengungkapan, pengubahan yang tidak sah, penyalahgunaan, kerusakan dan penghilangan data pribadi. Jika terjadi kebocoran data pribadi, maka perusahaan *e-commerce* yang bersangkutan wajib menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada penggunanya dan lembaga yang menyelenggarakan data pribadi. Pemberitahuan tersebut harus memuat data pribadi yang terungkap, kapan dan bagaimana data pribadi tersebut bocor, serta upaya penanganan serta pemulihan kebocoran data pribadi. Jika kebocoran data pribadi tersebut hingga mengganggu pelayanan publik dan/atau berdampak serius terhadap kepentingan masyarakat, maka perusahaan *e-commerce* harus mengumumkan kebocoran tersebut kepada masyarakat.¹⁹

Berdasarkan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) Pasal 57, pengendali data pribadi yang tidak mengumumkan kebocoran data pribadi yang telah terjadi, dapat dikenai sanksi administratif berupa:

- a. peringatan tertulis;
- b. penghentian sementara semua kegiatan pemrosesan data pribadi;
- c. penghapusan atau pemusnahan data pribadi; dan/atau
- d. denda administratif.

Terdapat beberapa kewajiban Penyelenggara terkait pemrosesan data pribadi yang diatur dalam POJK 10/22 antara lain sebagai berikut: (POJK 10/22, Ps. 44 ayat (1))

1. untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang dikelola oleh Penyelenggara dari tahap perolehan hingga pemusnahan;

¹⁸ Ni Nyoman Ratna Dewi, Ayu Putu Laksmi Danyathi, *Op. Cit.*, hlm. 77-78.

¹⁹ Nafiatul Munawaroh, *Tanggung Jawab E-Commerce atas Kebocoran Data Pribadi*, <https://www.hukumonline.com/klinik/a/tanggung-jawab-ie-commerce-i-atas-kebocoran-data-pribadi-lt63638331d18f0/>, (diakses pada tanggal 8 Mei 2025).

2. untuk memastikan dilakukannya tahapan autentikasi, verifikasi, dan validasi dalam rangka mendukung keabsahan tindakannya untuk mengakses, memroses, serta mengeksekusi data pribadi, data transaksi, dan data keuangan yang dalam pengelolaannya;
3. untuk memastikan mengenai penggunaan dan pengungkapan data pribadi, data transaksi, dan data keuangan dalam pengelolaan Penyelenggara yang didasarkan pada persetujuan pemiliknya, kecuali ada ketentuan lain dalam hukum yang berlaku; dan
4. apabila terjadi kegagalan ataupun pelanggaran dari pihak Penyelenggara dalam menjaga dan melindungi kerahasiaan data pribadi, data transaksi, dan data keuangan yang dikelolanya maka pemilik data harus mendapatkan pemberitahuan secara tertulis dari Penyelenggara perihal kegagalan tersebut.²⁰

B. Perlindungan Terhadap Korban Kebocoran Data Pribadi Konsumen Teknologi Finansial (*Fintech*)

Perusahaan *Fintech* pada umumnya mengumpulkan berbagai jenis Data Pribadi pengguna untuk berbagai keperluan. Seiring dengan meningkatnya penggunaan *Fintech*, muncul kekhawatiran tentang keamanan Data Pribadi dan privasi pengguna. Perusahaan *Fintech* berpotensi menjadi target serangan siber yang mengincar kumpulan Data Pribadi yang sangat bernilai tinggi. Kekhawatiran publik juga meningkat karena insiden seperti penagihan pinjaman tidak etis dan kebocoran data. Kepatuhan terhadap aturan Perlindungan Data Pribadi tidak hanya diperlukan untuk memenuhi kewajiban hukum, tetapi juga untuk meningkatkan kepercayaan pengguna karena mereka merasa Data Pribadi mereka aman. Selain itu, perusahaan yang patuh pada Perlindungan Data Pribadi pada umumnya memiliki reputasi yang lebih baik, menarik perhatian investor dan mitra bisnis, serta mengurangi risiko hukum. Bagi Perusahaan *Fintech*, kepatuhan terhadap Perlindungan Data Pribadi sangat penting untuk menjaga kelangsungan bisnis dan mendukung terciptanya ekosistem keuangan yang aman dan terpercaya.²¹

Perlindungan merupakan hak dari setiap masyarakat. Maka dari itu, keambiguan dalam perumusan kebijakan terkait perlindungan akan melahirkan ketidakpastian hukum. Kepastian merupakan keadaan yang pasti, dalam hal pemberian pengaturan. Hukum diamanatkan untuk bersikap adil melalui pemberian kepastian. Dalam segi kacamata hukum, kepastian dalam hukum adalah sesuatu yang hanya dapat dijawab secara normatif, bukan sosiologi.²²

Kebocoran data pribadi tidak memengaruhi semua konsumen dalam industri *fintech* secara seragam. Faktor demografis seperti usia, jenis kelamin, dan tingkat pendidikan dapat memengaruhi persepsi, respons, serta tingkat kepercayaan konsumen setelah terjadinya pelanggaran data.

Terdapat beberapa permasalahan yang kerap ditemukan berdasarkan temuan yang dikaitkan dengan fenomena kebocoran data pribadi yang muncul di lapangan, beberapa permasalahan tersebut antara lain:²³

1. Penambahan Regulasi Tidak Menjamin Optimalnya Perlindungan
Berkaca pada preseden beberapa tahun terakhir, sekalipun sudah ada UITE, PPPSTE, Permen Kominfo PDPSE serta beberapa regulasi inti lainnya, pelanggaran data pribadi masih marak terjadi. Bahkan, sebagian besar bersumber dari kebocoran sistem milik penyelenggara sistem elektronik yang merupakan badan publik. Anomali ini membawapada keyakinan bahwa sesempurna apapun materi muatannya dibuat, implementasinya akan sangat bergantung pada kemampuan otoritas untuk tidak hanya melakukan pengawasan tetapi juga melakukan penegakan hukum.
2. Terlalu Banyak Otoritas Menimbulkan Kecenderungan Saling Lempar TanggungJawab
Selama ini ada beberapa otoritas berbeda yang saling beririsan dalam konteks PDP, semisal Kemkominfo untuk urusan tata kelola informasi dan sistem elektronik, Badan Sani dan Siber Negara (BSSN) untuk urusan keamanan jaringan, dan Otoritas

3.amazonaws.com/aftech/knowledgeHub/48ef934f-96b4-475c-8b71-2a1603b9e9e5.pdf, 2024, hlm. 10

²² Dominikus Rato, *Filsafat Hukum Mencari: Memahami dan Memahami Hukum*, Yogyakarta: Laksbang Pressindo, 2010, hlm. 59

²³ Olisias Gultom, Auditya Firza Saputra, Muhammad Faiz Aziz, *Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital*, Laporan Penelitian, Indonesia for Global Justice, 2022, hlm. 118-121

²⁰ Gita Theresa, *Op. Cit.*, Hlm. 361-362

²¹ *Pedoman Perlindungan Data Pribadi di Industri Fintech*, fintechid-bucket.s3.ap-southeast-

Jasa Keuangan (OJK) untuk pengaturan PDP konsumen jasa keuangan dan bidang perbankan. Di satu sisi, banyaknya otoritas bisa jadi sebuah hal positif manakala fungsinya teroptimisasi sesuai porsi yang didesain. Namun, realitasnya di sisi lain menunjukkan bahwa terlalu banyak otoritas cenderung membuat pembagian kewenangan tidak jelas dan pada gilirannya memunculkan anomali seperti kecenderungan saling lempar tanggung jawab, terutama manakala terjadi kegagalan perlindungan data pribadi.

3. Keterbatasan Pemahaman Sumber Daya Manusia

Pelindungan data pribadi merupakan isu multidimensi yang membutuhkan atensi setiap pemangku kepentingan. Masalah pada dimensi sumber daya manusia (SDM) muncul karena adanya gap pengetahuan teknis antara pelaksana di bidang IT, regulator dan pelaksana. Mulai dari persoalan peristilahan hingga perbedaan logika berpikir disipliner. Misalnya, pelaksana pada bagian IT pada suatu departemen bisa saja memahami teknisi tata kelola sistem dan pemrosesan data, tapi di sisi lain tidak begitu paham tentang aspek hukum atau filosofi privasi. Ada perbedaan naluri pada logika berpikir eksakta dan sosial: mayoritas pelaku IT beranggapan pengumpulan data sebanyak mungkin dibutuhkan karena informasi yang padat akan jadi bekal sempurna bagi pemrosesan. Prinsipnya, *the more (data) the merrier*. Tapi, di sisi lain logika eksakta itu berseberangan dengan konstruksi berpikir konsep privasi yang secara naluri menghendaki pengumpulan data seminimal dan relevan mungkin karena ada risiko-risiko sosial di dalamnya.

4. Banyak Laporan Pelanggaran Data Pribadi Tidak Diterima/Ditindaklanjuti Kepolisian

Salah satu problem struktural yang terlihat adalah ketidakmampuan kepolisian untuk menindak lanjuti laporan perihal pelanggaran data pribadi. Ini berkaitan erat dengan masalah yang disebut sebelumnya. Dilansir oleh Kompas, sepanjang 2020 ada tujuh kasus kebocoran data pribadi yang dilaporkan, yaitu kasus Tokopedia (sejumlah 91 juta data pribadi pengguna), bhineka.com (sejumlah 1,2 juta data pengguna), kebocoran data KPU tentang data pemilih tetap (sejumlah 190 juta data pemilih), Kredit Plus (sejumlah 890 ribu data nasabah), ShopBack (data kartu kredit pengguna), Red Doorz (5,8 juta data pengguna), dan Cermati (sejumlah

2,9 juta data pengguna).³⁶⁶ Jumlah yang fantastis sebelumnya belum menghitung laporan yang datang dari orang-perorang yang diduga berjumlah jutaan. Persoalannya, meski merupakan sebuah tindak pidana dalam banyak undang-undang, banyak laporan dari masyarakat yang kemudian dimentahkan oleh unit cyber crime di kantor-kantor kepolisian. Menurut informasi yang didapat dari wawancara dengan sejumlah informan (identitas sengaja dirahasiakan), beberapa alasan yang kerap diangkat petugas administrasi kepolisian antara lain: (1) jumlah kerugian tidak bisa dipastikan (atau terlalu kecil); (2) Polsek atau Polres tidak memiliki unit sendiri sehingga pelapor diminta untuk mengadu ke Polda; (3) Pengadu diminta menghubungi perusahaan penyedia platform terlebih dahulu; (4) Belum timbul kerugian dari kejahatan (walaupun data sudah berpindah tangan secara ilegal); (5) tidak ada bukti telah terjadi kejahatan.

Pangsa aktivitas fintech di Indonesia berdasarkan data statistik, pada tahun 2016 nilai transaksi fintech di Indonesia diperkirakan telah mencapai angka USD 14,5 Miliar. Pelaku fintech di Indonesia juga masih dominan berbisnis *payment* yaitu 42,22%, pinjaman sebesar 17,78% dan sisanya berbentuk *aggregator*, *financial planning* dan lain sebagainya.²⁴

Pengaruh kebocoran data pribadi terhadap kepercayaan konsumen dibedakan berdasarkan beberapa faktor demografis, faktor-faktor tersebut tentunya berpengaruh terhadap persepsi konsumen terhadap keamanan data pribadi. Faktor-faktor tersebut terdiri atas faktor usia, jenis kelamin, atau tingkat pendidikan.

Sebagai bentuk perlindungan terhadap korban konsumen kebocoran data *fintech*, terdapat beberapa langkah hukum jika data pribadi disalahgunakan sesuai dengan peraturan perundang-undangan yang berlaku yang dalam hal ini adalah UU Perlindungan Data Pribadi (UU PDP) dan Peraturan OJK (POJK). Langkah-langkah hukum tersebut diantaranya:²⁵

1. Melaporkan ke Lembaga Terkait

Penyelenggara *fintech* yang menggunakan atau memproses data pribadi tanpa persetujuan pemiliknya dapat dikenai sanksi

²⁴ Croys Diansyah A dkk, *Op. Cit.*, hlm. 229.

²⁵ Nafiatul Munawaroh, *Pelindungan Data Pribadi dalam Penyelenggaraan Fintech*, <https://www.hukumonline.com/klinik/a/pelindungan-data-pribadi-dalam-penyelenggaraan-ifintech-i-lt5c498fb94dc87/>, diakses pada tanggal 14 Mei 2025).

administratif berdasarkan UU PDP dan POJK 10/2022.

Korban dapat melaporkan kepada Otoritas Jasa Keuangan (“OJK”) jika tidak ada persetujuan pemrosesan data pribadi atau penyelenggara *fintech* tidak mematuhi prinsip-prinsip sebagaimana diatur di dalam Pasal 44 ayat (1) POJK 10/2022.

Adapun sanksi administratif bagi penyelenggara *fintech* tersebut dapat berupa peringatan tertulis yang dapat disertai dengan pemblokiran sistem elektronik penyelenggara, pembatasan kegiatan usaha dan/atau pencabutan izin yang akan dilakukan oleh OJK.

Sedangkan dalam UU PDP, Anda dapat melaporkan ke lembaga penyelenggaraan perlindungan data pribadi yang akan ditetapkan oleh presiden. Adapun sanksi administratif yang ditetapkan UU PDP adalah:

- a. peringatan tertulis;
 - b. penghentian sementara semua kegiatan pemrosesan data pribadi;
 - c. penghapusan atau pemusnahan data pribadi; dan/atau
 - d. denda administratif dikenakan paling tinggi 2% dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran.
2. Menggugat Secara Perdata
- Salah satu hak subjek data pribadi dalam UU PDP adalah menggugat pengendali data pribadi dan menerima ganti rugi atas pelanggaran pemrosesan data pribadi berdasarkan ketentuan peraturan perundang-undangan.
- Mengatur hal serupa, berdasarkan Pasal 26 ayat (1) UU 19/2016 berbunyi:
- “Kecuali ditentukan lain oleh peraturan perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan.”
- Maka, setiap orang yang dilanggar haknya tersebut dapat mengajukan gugatan atas kerugian yang ditimbulkan.
- Untuk mengajukan gugatan atas penyalahgunaan data pribadi, maka pihak yang dirugikan dapat mengajukan gugatan perbuatan melawan hukum dalam Pasal 1365 KUH Perdata.
3. Melaporkan Secara Pidana
- Berkaitan dengan contoh penyalahgunaan data pribadi berupa menggunakan data orang

lain untuk meminjam uang di *fintech* sebagaimana Anda tanyakan, Anda dapat membaca ulasan selengkapnya dalam artikel Jerat Pidana Menyalahgunakan KTP Orang Lain untuk Pinjol.

Adapun, berdasarkan UU PDP, apabila penyelenggara *fintech* melakukan penyalahgunaan data pribadi, maka dapat pula dilaporkan secara pidana.

Korporasi pada dasarnya dilarang memperoleh/mengumpulkan, mengungkapkan dan/atau menggunakan data pribadi yang bukan miliknya secara melawan hukum.

Jika hal tersebut dilanggar, maka akan dijera pidana berdasarkan Pasal 67 UU PDP berupa pidana penjara dan/atau pidana denda. Selain itu, dapat pula dijatuhi pidana tambahan berupa perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian.

Terhadap tindak pidana yang dilakukan korporasi, maka pidana dapat dijatuhkan kepada pengurus, pemegang kendali, pemberi perintah, pemilik manfaat dan/atau korporasi. Adapun untuk pidana denda yang dijatuhkan kepada korporasi maksimal 10 kali maksimal denda yang diancamkan.

PENUTUP

A. Kesimpulan

1. Landasan filosof tentang data pribadi ialah Pancasila dan Undang-Undang Dasar NKRI Tahun 1945 Hasil Amandemen ke-IV (UUD 1945). Dalam Pasal 28G ayat (1) UUD 1945. Terdapat beberapa aturan sebagai bentuk perlindungan hukum bagi konsumen *fintech* di Indonesia seperti UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, UU No. 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Otoritas Jasa Keuangan (OJK) terkait keamanan data dalam layanan *fintech*, serta beberapa Peraturan Bank Indonesia mengenai *Fintech*. Lebih khusus mengenai kebocoran data pribadi konsumen *fintech*, diatur di dalam Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) Pasal 57 dan Peraturan Otoritas Jasa Keuangan Nomor 10/POJK.05/2022 Tahun 2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi
2. Bentuk perlindungan terhadap korban konsumen kebocoran data *fintech*, terdapat

beberapa langkah hukum jika data pribadi disalahgunakan sesuai dengan peraturan perundang-undangan yang berlaku yang dalam hal ini adalah UU Perlindungan Data Pribadi (UU PDP) dan Peraturan OJK (POJK). Langkah-langkah hukum tersebut diantaranya, Melaporkan ke Lembaga Terkait, Menggugat Secara Perdata, Melaporkan Secara Pidana.

B. Saran

1. Sebaiknya aturan hukum yang mengatur mengenai kebocoran data konsumen dibuat lebih sederhana, Pemerintah serta Lembaga yang ada diharapkan memperkuat pengawasan dan implementasi regulasi yang telah ada, khususnya dalam hal pengamanan data pribadi konsumen oleh penyelenggara fintech. Peraturan yang telah ditetapkan perlu ditegakkan secara tegas dan pelanggaran harus dikenakan sanksi administratif maupun pidana sesuai ketentuan yang berlaku.
2. Sebaiknya Pemerintah perlu menyediakan mekanisme pengaduan dan pendampingan hukum bagi korban kebocoran data pribadi. Perusahaan fintech wajib segera memberi tahu korban dan memberikan ganti rugi yang layak. Edukasi tentang perlindungan data pribadi juga perlu ditingkatkan agar konsumen lebih waspada dan terlindungi.

DAFTAR PUSTAKA

Buku

- Ahmadi Miru, 2010. *Hukum Perlindungan Konsumen*, Jakarta: Rajawali Pers.
- Danrivanto Budhijanto, 2023. *Hukum Perlindungan Data Pribadi di Indonesia Cyberlaw & Cybersecurity*, Bandung: PT Refika Aditama.
- Fauji Diah Ayu Septi dan Widodo Moch. Wahyu, 2020, *Financial Technology*, Kediri: Fakultas Ekonomi, Universitas Nusantara PGRI Kediri.
- Gazali Djonis S, Rachmadi Usman, 2012, *Hukum Perbankan*, Jakarta: Sinar Grafika.
- Rato Dominikus, 2010, *Filsafat Hukum Mencari: Memahami dan Memahami Hukum*, Yogyakarta: Laksbang Pressindo..
- Sarwin Kiko, 2017. Dkk, Eds, *Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Perlindungan Konsumen Pada Fintech*, Jakarta: Departemen Perlindungan Konsumen OJK.
- Imaniyati Neni Sri, 2010, *Pengantar Hukum Perbankan di Indonesia*, Reika Aditama, Bandung.

Marzuki Peter Mahmud, 2005, *Penelitian Hukum*, Jakarta: Kencana Prenada Media.

Hadjon Philipus M, 1987, *Perlindungan Bagi Rakyat di Indonesia*, Surabaya: PT.Bina Ilmu.

Rahardjo Satjipto, 2004, *Hukum Indonesia*, Surakarta: Muhammadiyah University Press.

Raharjo Satjipto, 2000, *Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti.

Rosadi Sinta Dewi, 2009, *Perlindungan Privasi atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Bandung: Widya Padjajaran.

Soekanto Soerjono, 1998, *Penelitian Hukum Normatif*. Jakarta: Rajawali Press.

Wasiaturahma, dkk, 2019, *Fintech dan Prospek Bisnis Koperasi Syariah*, Surabaya: Scopindo Media Pustaka.

Shofie Yusuf, 2016, *Hukum Perlindungan Konsumen*, Jakarta: Kencana.

Peraturan Perundang-undangan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 28G Ayat 1

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

Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Otoritas Jasa Keuangan (OJK) terkait keamanan data dalam layanan fintech.

Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.

Peraturan Bank Indonesia Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial (PBI Tekfin).

Peraturan Bank Indonesia No 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia.

Jurnal/ Artikel Ilmiah

Alfi Fratiwi, *Tinjauan Yuridis Transaksi Financial Technology di Indonesia*, MEDIA OF LAW AND SHARIA, Vol. 2, No. 4, 2021.

Andri Soemitra, Adlina Hasan, *PERLINDUNGAN KONSUMEN TERHADAP KEBOCORAN DATA PADA JASA KEUANGAN DI*

- INDONESIA, Juripol (Jurnal Institusi Polgan), Vol. 5 No. 1, 2022.
- Aswirah dkk, *Perkembangan Dan Dampak Financial Technology Terhadap Inklusi Keuangan Di Indonesia: Studi Literatur*, Jurnal Ilmiah Bisnis & Keuangan JBK, Vol. 13, No. 2, 2024.
- 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: Jurnal Ilmiah Multidisiplin, Vol. 1 No. 5, 2023.
- Dewi, S, *Prinsip – Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya*, Sosiohumaniora, Vol.19 No. 3, 2017.
- Dewi, Sinta. *Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia*. Yustisia Jurnal Hukum, Vol. 5 No. 1, 2016.
- Ernama Santi, *Pengawasan Otoritas Jasa Keuangan terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016*, Diponegoro Law Journal, Vol. 6, No. 3, 2017.
- Fuad dkk, *Desain Perlindungan Hukum Bagi Konsumen Dan Data Pribadi Untuk Kegiatan Usaha Menggunakan Fintech Di Indonesia*, Jurnal Rectum, Vol. 7, No. 1, 2025.
- Gita Theresa, *Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintechp2plendingdi Indonesia*, Jurnal Darma Agung, Vol. 32 No.3, 2024.
- Husnul Khatimah, *Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Online Di Aplikasi Lazada Dan Shopee*, Lex LATA Jurnal Ilmiah Hukum, Vol. 4 No. 3, 2022.
- Jefri Arnolius Pasaribu, *Perlindungan Data Pribadi: Tantangan Hukum di Era Digital*, K Law (General), 2023.
- Kadek Rima Anggen Suari, I Made Sarjana, *Menjaga Privasi di Era Digital:Perlindungan DataPribadi di Indonesia*, Jurnal Analisis Hukum, Vol.6, No. 1, 2023.
- Miswan Ansori, *“Perkembangan Dan Dampak Financial Teknologi (Fintech) Terhadap Industry Keuangan Syariah Di Jawa Tengah”*, Wahana Islamika : Jurnal Study Keislaman, Vol 5. No 1, 2019.
- Ni Nyoman Ratna Dewi, Ayu Putu Laksmi Danyathi, *Perlindungan Hukum Bagi Pengguna Situs Pinjaman Dana Online Dari Tindakan Penyalahgunaan Data Pribadi*, ojs.unud.ac.id, 2022.
- Olisias Gultom, Auditya Firza Saputra, Muhammad Faiz Aziz, *Perlindungan Data Pribadi Di Indonesia Menyikapi Liberalisasi Ekonomi Digital*, Laporan Penelitian, Indonesia for Global Justice, 2022.
- Shafa Rosedila, *Analisis Perlindungan Konsumen Terhadap Pelanggaran Hak Informasi Pribadi Pada Pinjaman Berbasis Online*, Vol. 17, 2024.
- Sumber Lainnya**
- Annisa Sulisty Rini, *Daftar Kasus Kebocoran Data Sektor Finansial RI Selain BSI (BRIS)*, <https://finansial.bisnis.com/read/20230516/90/1656438/daftar-kasus-kebocoran-data-sektor-finansial-ri-selain-bsi-bris>, (diakses tanggal 8 Februari 2025).
- Kamsidah dan Alya Nur Hanifah, *Transformasi Keuangan melalui Fintech, Solusi Finansial bagi Masyarakat Indonesia*, <https://www.djkn.kemenkeu.go.id/kpknl-semarang/baca-artikel/16528/Transformasi-Kuangan-melalui-Fintech-Solusi-Finansial-bagi-Masyarakat-Indonesia.html>, (diakses pada tanggal 6 februari 2025).
- Nafiatul Munawaroh, *Tanggung Jawab E-Commerce atas Kebocoran Data Pribadi*, <https://www.hukumonline.com/klinik/a/tanggung-jawab-ie-commerce-i-atas-kebocoran-data-pribadi-lt63638331d18f0/>, (diakses pada tanggal 8 Mei 2025).
- Pedoman Perlindungan Data Pribadi di Industri Fintech*, fintechid-bucket.s3.ap-southeast-3.amazonaws.com/aftech/knowledgeHub/48ef934f-96b4-475c-8b71-2a1603b9e9e5.pdf, 2024
- Rita Puspita Sari, *RI Masuk 10 Besar Kebocoran Data, Hampir 100 Juta Akun Bocor*, <https://csirt.or.id/berita/ri-masuk-10-besar-kebocoran-data>, (diakses tanggal 7 Februari 2025).