Binamulia Hukum, Volume 13, Nomor 2, Desember 2024 (461-481) *ISSN Print 1410-0088*
DOI: 10.37893/jbh.v13i2.964 *ISSN Online 2656-856X*

Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah *Fintech Lending* di Indonesia

Fauzi Rifa, Maslihati Nur Hidayati*
Fakultas Hukum Universitas Al Azhar Indonesia, Jakarta
*email: imas@uai.ac.id

Abstrak

Meningkatnya penggunaan layanan *fintech lending* yang menawarkan kemudahan akses pembiayaan juga membawa risiko terhadap keamanan data pribadi nasabah. Meskipun sejumlah regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), dan Peraturan Otoritas Jasa Keuangan (POJK) telah diberlakukan, implementasi dan penegakan hukum masih menghadapi berbagai tantangan. Permasalahan utama yang dihadapi adalah sejauh mana efektivitas kebijakan penal dalam melindungi data pribadi nasabah, serta bagaimana regulasi yang ada dapat ditingkatkan untuk memberikan perlindungan yang lebih optimal. Penelitian ini menggunakan metode hukum normatif dengan pendekatan kepustakaan untuk menganalisis regulasi yang berlaku dan mengevaluasi efektivitasnya dalam praktik. Hasil penelitian menunjukkan bahwa meskipun kerangka hukum yang ada telah bersifat komprehensif, mengacu pada prinsip-prinsip perlindungan data internasional, dan mencakup perlindungan preventif maupun represif, efektivitasnya masih sangat bergantung pada implementasi dan pengawasan yang konsisten. Selain itu, efektivitas perlindungan hukum tidak seharusnya hanya berfokus pada penerapan sanksi administratif, tetapi juga memerlukan langkah-langkah penegakan hukum yang lebih tegas dan terintegrasi.

Kata Kunci: Fintech; Kebijakan Penal; Perlindungan Data Pribadi; Perlindungan Hukum.

Abstract

The increasing use of fintech lending services, which offer convenient access to financing, also poses risks to the security of customers' personal data. Although various regulations, such as the Personal Data Protection Act (PDP Act), the Electronic Information and Transactions Act (EIT Act), and the Financial Services Authority Regulation (POJK), have been enacted, their implementation and enforcement face significant challenges. The primary issue lies in assessing the effectiveness of penal policies in protecting customers' personal data and determining how existing regulations can be enhanced to provide more optimal protection. This study employs a normative legal method with a literature-based approach to analyze the current regulations and evaluate their effectiveness in practice. The findings indicate that, while the existing legal framework is comprehensive, adheres to internationally recognized data protection principles, and incorporates preventive as well as repressive measures, its effectiveness heavily depends on consistent implementation and supervision. Furthermore, the effectiveness of legal protection should not solely focus on administrative sanctions but must also include more robust and integrated enforcement measures.

Keywords: *Fintech; Legal Protection; Penal Policy; Personal Data Protection; Legal Protection.*

A. PENDAHULUAN

Fintech lending di Indonesia telah mengalami pertumbuhan yang signifikan dalam beberapa tahun terakhir. Berdasarkan data dari Otoritas Jasa Keuangan (OJK), total *outstanding* pembiayaan *fintech peer-to-peer (P2P) lending* mencapai Rp 66,79 triliun pada Juni 2024, mencerminkan pertumbuhan tahunan sebesar 26,73% (Saputra, 2024). Pertumbuhan ini menunjukkan meningkatnya kepercayaan masyarakat terhadap *fintech lending* sebagai alternatif pembiayaan yang mudah diakses dan efisien.

Salah satu faktor utama yang mendorong pertumbuhan ini adalah kemampuan *fintech lending* untuk menjangkau segmen pasar yang sebelumnya tidak terlayani oleh lembaga keuangan tradisional. Dengan teknologi yang menawarkan akses yang lebih luas dan proses yang lebih cepat, *fintech lending* telah menjadi solusi penting bagi individu dan usaha kecil yang membutuhkan pembiayaan.

Pada Maret 2024, nilai penyaluran pembiayaan *fintech lending* di Indonesia mencapai Rp 22,76 triliun, meningkat sebesar 8,89% dibandingkan bulan sebelumnya dan 15,35% dibandingkan periode yang sama tahun sebelumnya (Saputra, 2024). Penyaluran pinjaman tersebut tersebar ke 9,78 juta akun penerima, dengan 75% dari total peminjam berasal dari Pulau Jawa. Data ini menunjukkan bahwa meskipun *fintech lending* telah memperluas jangkauan ke berbagai daerah, konsentrasi pengguna masih tinggi di wilayah Jawa.

Sebagian besar penyaluran pinjaman *fintech lending*, sekitar 33,61%, disalurkan ke sektor produktif seperti perdagangan besar dan eceran, pertanian, kehutanan, dan perikanan (Muhamad, 2024). Data ini menunjukkan peran penting *fintech lending* dalam mendukung sektor-sektor ekonomi produktif serta berkontribusi pada pertumbuhan ekonomi nasional.

Namun, meskipun pertumbuhan *fintech lending* sangat pesat, industri ini juga menghadapi tantangan signifikan, terutama terkait risiko kredit dan perlindungan data pribadi. Berdasarkan data OJK, pada April 2024 terdapat 15 penyelenggara *fintech P2P lending* dengan tingkat wanprestasi lebih dari 90 hari (TWP90) di atas 5% (Saputra, 2024). Meskipun angka TWP90 ini telah menurun dibandingkan bulan sebelumnya, hal ini tetap menjadi perhatian serius bagi regulator dan pelaku industri.

Selain risiko kredit, perlindungan data pribadi juga menjadi isu yang krusial. Kasus-kasus pembocoran data pribadi oleh penyelenggara *fintech lending*, baik yang beroperasi secara legal maupun ilegal, semakin sering terjadi. Situasi ini memicu kekhawatiran masyarakat terkait keamanan dan privasi data pribadi mereka, yang dapat berdampak pada kepercayaan terhadap industri *fintech lending* secara keseluruhan.

Pembocoran data pribadi dalam industri *fintech lending* di Indonesia telah menjadi isu signifikan yang menimbulkan kekhawatiran di kalangan masyarakat dan regulator. Kasus-kasus ini tidak hanya melibatkan penyelenggara *fintech lending* yang beroperasi secara legal, tetapi juga yang ilegal. Salah satu contoh mencolok adalah kasus yang melibatkan aplikasi pinjaman *online* Dompet Kartu, yang dituduh melakukan persekusi digital terhadap nasabahnya.

Pembocoran data pribadi sering kali mencakup penyalahgunaan informasi sensitif milik nasabah, seperti nama, Nomor Induk Kependudukan (NIK), nomor telepon, dan alamat. Informasi ini kerap digunakan untuk tujuan yang tidak sah,

termasuk penagihan utang secara agresif atau bahkan tindakan penipuan. Dalam kasus Dompet Kartu, aplikasi ini dituduh melakukan penagihan dengan cara-cara yang meresahkan, seperti ancaman dan penyebaran data pribadi nasabah kepada publik. Tindakan tersebut melanggar Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan peraturan perlindungan data pribadi lainnya (Indotelko, 2018).

Untuk menghadapi meningkatnya insiden penyalahgunaan data, pemerintah Indonesia telah menyusun berbagai kebijakan penal guna memperkuat perlindungan data pribadi nasabah *fintech lending*. Salah satu regulasi utama adalah Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP), yang memberikan kerangka hukum komprehensif dalam perlindungan data pribadi. UU PDP mencakup berbagai aspek, termasuk asas, jenis data pribadi, hak subjek data, serta kewajiban pengendali dan prosesor data. UU ini juga menetapkan sanksi administratif dan pidana yang tegas untuk pelanggaran, termasuk denda yang signifikan dan hukuman penjara, sebagai upaya memberikan efek jera.

Selain UU PDP, Peraturan Otoritas Jasa Keuangan (POJK) juga berperan penting dalam melindungi data pribadi di sektor *fintech lending*. POJK No. 77/POJK.01/2016 mengatur layanan *fintech peer-to-peer (P2P) lending* dengan menekankan kewajiban penyelenggara untuk mendapatkan persetujuan dari pemilik data sebelum memprosesnya. Peraturan ini juga mengharuskan adanya mekanisme autentikasi, verifikasi, dan validasi, dengan sanksi administratif bagi pelanggaran, mulai dari peringatan hingga pencabutan izin usaha.

Selanjutnya, POJK No. 10/POJK.05/2022 memperkuat perlindungan konsumen di sektor jasa keuangan, termasuk *fintech lending*, dengan mengatur kewajiban serupa terkait pemrosesan data pribadi. Sementara itu, UU ITE berkontribusi dalam perlindungan data pribadi di sistem elektronik dengan menetapkan sanksi bagi akses ilegal dan penyalahgunaan data yang dapat merugikan pemiliknya.

Kebijakan penal ini mencerminkan komitmen pemerintah dalam memberikan perlindungan hukum yang kuat terhadap data pribadi nasabah fintech, sekaligus menjaga kepercayaan masyarakat terhadap sektor ini (Siaran Pers Kominfo, 2018).

Meskipun pemerintah Indonesia telah menyusun berbagai kebijakan penal untuk melindungi data pribadi nasabah *fintech lending*, efektivitas kebijakan tersebut masih menghadapi berbagai tantangan. Salah satu kendala utama adalah terbatasnya tugas, fungsi, dan wewenang Lembaga Pengawas Perlindungan Data. Lembaga ini tidak memiliki kewenangan untuk menyelesaikan sengketa melalui mekanisme ajudikasi non-litigasi atau mengeluarkan putusan mediasi terkait ganti rugi.

Tantangan lain adalah ketentuan batas waktu (*timeline*) yang diatur secara kaku dalam Undang-Undang Pelindungan Data Pribadi (UU PDP) terkait pemenuhan hak subjek data oleh pengendali data. Ketentuan ini berlaku seragam untuk semua sektor, meskipun corak dan model bisnis di setiap sektor berbeda-beda. Misalnya, pengendali data dari sektor publik mungkin menghadapi kesulitan dalam mematuhi persyaratan waktu yang ditentukan oleh UU PDP (Pakpahan dkk., 2020).

Efektivitas kebijakan penal ini sangat bergantung pada implementasi yang konsisten, pengawasan yang ketat oleh pihak berwenang, dan edukasi kepada masyarakat tentang pentingnya menjaga data pribadi.

Penelitian sebelumnya mengenai kebijakan penal perlindungan hukum data pribadi nasabah *fintech lending* di Indonesia telah membahas berbagai aspek

penting dari isu ini. Salah satu penelitian signifikan dilakukan oleh Elvira Fitriyani Pakpahan dan rekan-rekannya, yang mengungkap bahwa meskipun terdapat sistem regulasi yang mengatur industri fintech di Indonesia, perlindungan data pribadi konsumen masih belum memadai.

Penelitian tersebut menyoroti bahwa sanksi administratif, pidana, dan perdata yang ada saat ini belum cukup kuat untuk mencegah penyalahgunaan data pribadi. Untuk itu, penelitian ini merekomendasikan pembentukan undang-undang khusus tentang perlindungan data pribadi serta pendirian lembaga pengawas dengan wewenang yang lebih luas untuk memastikan implementasi kebijakan yang efektif (Pakpahan dkk., 2020).

Penelitian yang dilakukan oleh Husni Kurniawati dan Yunanto Yunanto menyoroti bahwa perlindungan hukum terhadap data pribadi nasabah *fintech P2P lending* di Indonesia telah dijamin dalam kerangka hukum nasional. Namun, implementasinya masih menghadapi berbagai tantangan. Mereka mengklasifikasikan perlindungan data pribadi ke dalam dua kategori, yaitu perlindungan umum dan spesifik. Data pribadi yang bersifat spesifik memerlukan perlindungan yang lebih ketat karena sifatnya yang sensitif. Penelitian ini juga menggarisbawahi pentingnya keberadaan regulasi yang lebih mendetail untuk mengatasi potensi penyalahgunaan data dalam konteks fintech (Kurniawati dan Yunanto, 2022).

Sementara itu, penelitian yang dilakukan oleh Siti Nasikhatuddini menekankan pentingnya peran hukum pidana dalam melindungi nasabah *fintech lending*. Ia mengungkapkan bahwa pelanggaran terhadap nasabah sering kali hanya dikenakan sanksi administratif, yang dinilai kurang memberikan rasa keadilan bagi korban. Oleh karena itu, ia menekankan perlunya penerapan sanksi pidana yang lebih tegas, khususnya untuk pelanggaran seperti penyebaran data pribadi, ancaman dalam proses penagihan, serta tindakan penipuan (Nasikhatuddini, 2021).

Penelitian-penelitian ini menunjukkan bahwa meskipun upaya regulasi telah dilakukan, perlindungan hukum terhadap data pribadi nasabah *fintech lending* di Indonesia masih membutuhkan peningkatan signifikan. Sanksi yang ada saat ini sering kali dianggap belum cukup kuat untuk mencegah terjadinya pelanggaran. Selain itu, terdapat kebutuhan mendesak untuk penyusunan regulasi yang lebih spesifik dan keberadaan lembaga pengawas yang efektif. Penelitian-penelitian ini juga menekankan pentingnya meningkatkan kesadaran dan pemahaman, baik di kalangan penyelenggara fintech maupun masyarakat, terkait urgensi perlindungan data pribadi.

Meskipun banyak penelitian telah membahas regulasi yang mengatur perlindungan data pribadi, seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), dan POJK, efektivitas implementasi regulasi tersebut masih belum dikaji secara mendalam. Penelitian sebelumnya cenderung berfokus pada keberadaan regulasi tanpa mengevaluasi sejauh mana regulasi tersebut diimplementasikan dan dipatuhi oleh penyedia layanan pinjaman *online* (pinjol). Kajian ini penting untuk mengidentifikasi celah dalam penegakan hukum dan merumuskan solusi yang lebih efektif.

Penelitian terdahulu juga telah membahas keberadaan sanksi administratif dan pidana untuk pelanggaran data pribadi. Namun, efektivitas sanksi tersebut dalam mencegah terjadinya pelanggaran belum banyak dievaluasi. Penelitian ini perlu

mengkaji apakah sanksi yang diterapkan saat ini sudah cukup tegas dan memberikan efek jera kepada pelanggar. Analisis ini mencakup evaluasi terhadap kasus-kasus pelanggaran yang telah ditindaklanjuti serta hasil akhir dari proses penegakan hukumnya.

Berdasarkan latar belakang yang telah disampaikan, permasalahan yang dirumuskan dalam penelitian ini adalah: *Pertama*, bagaimana kebijakan penal dalam memberikan perlindungan hukum terhadap privasi dan data pribadi konsumen pengguna aplikasi *fintech lending*? *Kedua*, sejauh mana efektivitas regulasi yang ada dalam melindungi data pribadi nasabah *fintech lending*?

Untuk mengisi celah dalam penelitian sebelumnya, fokus utama penelitian ini adalah pada analisis kebijakan penal perlindungan hukum data pribadi nasabah *fintech lending* di Indonesia. Penulis akan memusatkan kajian pada identifikasi, analisis efektivitas, implementasi, dan penegakan hukum.

Dalam kerangka teoritis, penelitian ini akan mengintegrasikan teori perlindungan hukum dari Philipus M. Hadjon dan teori kepastian hukum dari Satjipto Rahardjo. Pendekatan ini bertujuan untuk menghasilkan analisis yang mendalam dan komprehensif terkait perlindungan hukum data pribadi dalam konteks *fintech lending* di Indonesia.

B. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode hukum normatif. Penelitian ini mencakup kajian terhadap norma-norma hukum yang terdapat dalam peraturan perundang-undangan, putusan pengadilan, serta norma-norma hukum yang berlaku saat ini. Metode hukum normatif merupakan metode pengumpulan data yang berfokus pada penelitian kepustakaan, dengan data yang digunakan berupa data sekunder, yaitu data yang diperoleh dari dokumen-dokumen kepustakaan.

Jenis data yang digunakan dalam penelitian ini meliputi:

a) Dokumen dasar hukum. Dokumen ini mencakup data yang memuat aturan hukum yang mengikat, seperti undang-undang, perkara, dan peraturan lain yang relevan dan masih berlaku. Dalam penelitian ini, data yang digunakan mencakup Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Otoritas Jasa Keuangan (POJK), serta peraturan perundang-undangan lain yang terkait.
b) Dokumen hukum sekunder. Dokumen ini mencakup bahan hukum yang menjelaskan atau mendukung dokumen hukum dasar, seperti buku, laporan penelitian hukum, artikel ilmiah, serta dokumen lain yang berkaitan dengan pelaksanaan dan implementasi hukum.

Penelitian ini dianalisis secara kualitatif dengan menggunakan pendekatan hukum baku. Oleh karena itu, teknik pengumpulan data yang digunakan adalah penelitian kepustakaan (*library study*). Penelitian ini meliputi analisis terhadap peraturan perundang-undangan, buku-buku hukum, artikel ilmiah, serta dokumen lain yang relevan dengan topik penelitian.

C. HASIL PENELITIAN DAN PEMBAHASAN

1. Kebijakan Penal dalam Perlindungan Data Pribadi pada *Fintech Lending* di Indonesia

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016, merupakan payung hukum utama dalam pengaturan perlindungan data pribadi elektronik di Indonesia. UU ITE mengadopsi prinsip-prinsip perlindungan data pribadi yang diakui secara internasional. Namun, pengaturannya masih bersifat umum dan belum komprehensif (Martaon, 2023).

Perlindungan data pribadi dalam UU ITE diatur secara khusus pada Pasal 26. Pasal ini menegaskan bahwa penggunaan informasi melalui media elektronik yang menyangkut data pribadi seseorang harus didasarkan pada persetujuan dari individu yang bersangkutan. Ketentuan ini mencerminkan prinsip persetujuan (*consent*), yang merupakan salah satu prinsip fundamental dalam perlindungan data pribadi. Prinsip ini mengharuskan adanya persetujuan yang jelas dan tegas dari pemilik data sebelum data pribadinya dapat digunakan atau diproses oleh pihak lain (Oktavira, 2020).

Selain itu, Pasal 26 ayat (2) memberikan hak kepada individu yang merasa haknya dilanggar untuk mengajukan gugatan atas kerugian yang ditimbulkan. Ketentuan ini menjadi landasan hukum bagi individu untuk menuntut ganti rugi atas pelanggaran terhadap data pribadinya. Namun, mekanisme pengajuan gugatan ini masih bersifat umum, karena belum ada pengaturan khusus yang mengatur secara rinci tata cara pengajuan gugatan terkait pelanggaran data pribadi (Oktavira, 2020).

Selain itu, UU ITE juga mengatur kewajiban penyelenggara sistem elektronik untuk menghapus informasi elektronik yang tidak relevan yang berada di bawah kendalinya atas permintaan individu yang bersangkutan berdasarkan penetapan pengadilan. Ketentuan ini mencerminkan prinsip hak untuk dilupakan (*right to be forgotten*) yang telah diakui dalam regulasi perlindungan data di berbagai negara. Namun, implementasi hak ini masih memerlukan penetapan pengadilan, yang dapat menjadi hambatan bagi individu dalam mengakses haknya secara efektif (Martaon, 2023).

Salah satu kelemahan utama dalam pengaturan perlindungan data pribadi dalam UU ITE adalah ketiadaan definisi yang jelas mengenai apa yang dimaksud dengan data pribadi. UU ini tidak memberikan batasan atau kriteria spesifik terkait jenis informasi yang termasuk dalam kategori data pribadi. Ketidakjelasan ini dapat menimbulkan ketidakpastian hukum dan membuka ruang untuk perbedaan interpretasi dalam penerapannya.

Selain itu, UU ITE juga tidak mengatur secara rinci kewajiban-kewajiban spesifik bagi pengelola data pribadi (*data controller*) maupun pemroses data pribadi (*data processor*). Tidak terdapat ketentuan yang mengatur prinsip-prinsip pemrosesan data yang adil dan sah, pembatasan tujuan pengumpulan data, minimalisasi data, akurasi data, pembatasan penyimpanan, integritas dan kerahasiaan, serta akuntabilitas. Prinsip-prinsip ini merupakan elemen penting dalam regulasi perlindungan data modern, seperti yang diatur dalam General Data Protection Regulation (GDPR) Uni Eropa. Ketiadaan pengaturan ini mencerminkan kesenjangan signifikan dalam kerangka perlindungan data pribadi yang diadopsi oleh UU ITE (Tsamara, 2021).

UU ITE belum mengatur secara komprehensif hak-hak subjek data, seperti hak untuk mengakses data, hak untuk mengoreksi data, hak untuk membatasi pemrosesan data, hak untuk menolak pemrosesan data, dan hak atas portabilitas data. Ketiadaan pengaturan yang jelas mengenai hak-hak ini membatasi kemampuan individu untuk mengontrol data pribadinya secara efektif.

Dalam hal pengawasan dan penegakan hukum, UU ITE juga belum menetapkan otoritas pengawas independen yang bertanggung jawab untuk mengawasi implementasi perlindungan data pribadi. Tidak terdapat ketentuan yang mengatur kewenangan investigasi, audit, pemberian sanksi administratif, maupun penyelesaian pengaduan terkait pelanggaran data pribadi. Ketiadaan pengaturan ini menyulitkan upaya penegakan hukum yang efektif terhadap pelanggaran data pribadi.

Selain itu, UU ITE belum memberikan pengaturan khusus mengenai transfer data pribadi lintas batas (*cross-border data transfer*). Dalam era globalisasi dan ekonomi digital, arus data lintas batas adalah fenomena yang umum terjadi. Namun, ketiadaan regulasi yang jelas terkait hal ini dapat menimbulkan risiko terhadap perlindungan data pribadi warga negara Indonesia yang ditransfer ke luar negeri. Risiko ini mencakup kemungkinan data diproses atau disimpan di yurisdiksi yang tidak memiliki tingkat perlindungan data yang memadai (Yusuf, 2020).

Undang-Undang Perlindungan Data Pribadi (UU PDP) mendefinisikan data pribadi sebagai informasi tentang seseorang yang dapat diidentifikasi secara langsung atau tidak langsung, baik melalui sistem elektronik maupun non-elektronik, baik secara tersendiri maupun dalam kombinasi dengan informasi lain. Definisi ini mencakup spektrum luas dari informasi yang dapat mengidentifikasi individu (Farisa, 2022).

Salah satu aspek penting dalam UU PDP adalah pengelompokan data pribadi menjadi dua kategori, yaitu data pribadi umum dan data pribadi spesifik. Data pribadi umum mencakup informasi seperti nama lengkap, jenis kelamin, kewarganegaraan, agama, dan status perkawinan. Sementara itu, data pribadi spesifik meliputi data kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, serta data lain yang ditentukan dalam peraturan perundang-undangan. Pembagian ini memberikan dasar bagi tingkat perlindungan yang berbeda sesuai dengan tingkat sensitivitas data (Wahyuni, 2022).

UU PDP juga menetapkan prinsip-prinsip dasar yang harus dipatuhi oleh semua pihak yang terlibat dalam pemrosesan data pribadi. Prinsip-prinsip ini meliputi: Pengumpulan data pribadi yang terbatas dan spesifik, pemrosesan data yang sah, adil, dan transparan, jaminan keamanan data pribadi, pembatasan periode penyimpanan data, keakuratan data pribadi, akuntabilitas pengendali data.

Prinsip-prinsip ini sejalan dengan standar internasional perlindungan data pribadi, seperti yang diatur dalam GDPR Uni Eropa. Penyesuaian ini menunjukkan komitmen UU PDP untuk mengadopsi praktik terbaik global dalam melindungi data pribadi (Tsamara, 2021).

Salah satu aspek krusial dalam UU PDP adalah pengaturan mengenai hak-hak subjek data. UU ini memberikan sejumlah hak kepada individu terkait data pribadinya, antara lain: Hak untuk mengakses data pribadi, hak untuk memperbarui dan memperbaiki data pribadi, hak untuk menghapus atau memusnahkan data pribadi, hak untuk membatasi pemrosesan data pribadi, hak untuk memperoleh data pribadi dalam format yang terstruktur dan dapat dibaca secara elektronik

(*portabilitas data*), hak untuk mengajukan keberatan terhadap pemrosesan data pribadi.

Pengakuan atas hak-hak ini memberikan kontrol yang lebih besar kepada individu atas data pribadinya, sehingga memperkuat perlindungan privasi (Undang-Undang Nomor 27 Tahun 2022, Pasal 6–10).

UU PDP juga menetapkan kewajiban-kewajiban bagi pengendali data dan prosesor data. Pengendali data diwajibkan untuk: Melakukan penilaian dampak perlindungan data pribadi sebelum memproses data yang berisiko tinggi dan menerapkan langkah-langkah teknis dan organisasi yang memadai untuk memastikan tingkat keamanan sesuai dengan risiko yang dihadapi.

Sementara itu, prosesor data harus memproses data pribadi sesuai dengan instruksi dari pengendali data serta menjaga kerahasiaan data pribadi yang diproses. Ketentuan ini bertujuan untuk memastikan bahwa setiap pemrosesan data dilakukan secara aman dan bertanggung jawab (Undang-Undang Nomor 27 Tahun 2022, Pasal 53).

Aspek penting lainnya dalam UU PDP adalah pengaturan mengenai transfer data pribadi lintas negara. UU ini menetapkan bahwa transfer data pribadi ke luar wilayah Indonesia hanya dapat dilakukan jika negara atau organisasi internasional tujuan memiliki tingkat perlindungan data pribadi yang setara atau lebih tinggi dari ketentuan UU PDP. Apabila tingkat perlindungan di negara tujuan tidak setara, transfer data tetap dimungkinkan dengan syarat adanya perjanjian yang mengikat secara hukum antara pengendali data di Indonesia dan pihak penerima di luar negeri. Ketentuan ini dirancang untuk menjaga keamanan dan kerahasiaan data pribadi dalam konteks global (Undang-Undang Nomor 27 Tahun 2022, Pasal 56).

UU PDP mengatur pemberian sanksi administratif dan pidana bagi pelanggaran terhadap ketentuan undang-undang ini. Sanksi administratif meliputi peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, hingga pengenaan denda administratif. Di sisi lain, sanksi pidana dijatuhkan untuk pelanggaran serius, seperti memperoleh atau mengumpulkan data pribadi secara melawan hukum, mengungkapkan data pribadi tanpa izin, atau menggunakan data pribadi di luar tujuan yang telah disepakati (Undang-Undang Nomor 27 Tahun 2022).

UU PDP menetapkan sejumlah ketentuan pidana yang bertujuan untuk memberikan efek jera dan mencegah pelanggaran terhadap perlindungan data pribadi. Ketentuan ini melengkapi perlindungan hukum yang bersifat preventif melalui mekanisme administratif dengan memberikan perlindungan hukum yang bersifat represif bagi pelanggaran serius (Ali dan Andika, 2023).

Pasal 67 UU PDP secara khusus mengatur sanksi pidana untuk pelanggaran perlindungan data pribadi:

(1) "Bahwa setiap orang yang dengan sengaja dan melawan hukum memperoleh atau mengumpulkan data pribadi yang bukan miliknya dengan maksud untuk menguntungkan diri sendiri atau orang lain, yang mengakibatkan kerugian bagi subjek data pribadi sebagaimana dimaksud dalam Pasal 65 ayat (1), dapat dipidana dengan penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah)."

(2) "Bahwa setiap orang yang dengan sengaja dan melawan hukum

> mengungkapkan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (2), dapat dipidana dengan penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah)."

Ketentuan ini bertujuan untuk mencegah tindakan penyebaran atau pengungkapan data pribadi tanpa izin, yang dapat melanggar privasi dan menimbulkan kerugian signifikan bagi subjek data. Dengan mengatur sanksi pidana yang tegas, UU PDP memperkuat perlindungan hukum bagi individu dan menekankan pentingnya kepatuhan terhadap pengelolaan data pribadi yang sesuai dengan peraturan.

Selanjutnya, Pasal 67 ayat (3) UU PDP mengatur bahwa setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya sebagaimana dimaksud dalam Pasal 65 ayat (3) dapat dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau pidana denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Ketentuan ini bertujuan untuk mencegah penyalahgunaan data pribadi oleh pihak yang tidak berwenang, yang dapat menimbulkan berbagai bentuk kerugian bagi subjek data.

Ketentuan pidana dalam UU PDP tidak hanya berlaku bagi individu, tetapi juga mencakup tindak pidana yang dilakukan oleh korporasi. Pasal 68 UU PDP menyebutkan bahwa apabila tindak pidana sebagaimana dimaksud dalam Pasal 67 dilakukan oleh korporasi, maka pidana pokok yang dijatuhkan adalah pidana denda dengan pemberatan sebesar 3 (tiga) kali dari pidana denda sebagaimana diatur dalam Pasal 67. Ketentuan ini menunjukkan bahwa UU PDP memberikan perhatian khusus terhadap potensi pelanggaran yang dilakukan oleh entitas bisnis atau organisasi yang mengelola data pribadi dalam skala besar.

Selain pidana pokok, UU PDP juga mengatur pidana tambahan yang dapat dijatuhkan terhadap korporasi. Pasal 68 ayat (2) menetapkan bahwa, selain pidana denda, korporasi dapat dikenai pidana tambahan berupa:

a) Pengumuman putusan hakim.
b) Pembekuan sebagian atau seluruh kegiatan usaha korporasi.
c) Pencabutan izin usaha.
d) Pembubaran korporasi.

Ketentuan ini memberikan fleksibilitas kepada hakim dalam menentukan sanksi yang lebih komprehensif dan efektif. Dengan demikian, sanksi tambahan ini tidak hanya bertujuan untuk menghukum pelanggaran, tetapi juga untuk mencegah terulangnya pelanggaran serupa di masa depan.

Kebijakan penal dalam UU PDP mencakup aspek pertanggungjawaban pidana korporasi. Pasal 69 mengatur bahwa apabila tindak pidana sebagaimana dimaksud dalam Pasal 67 dilakukan oleh korporasi, maka tuntutan dan penjatuhan pidana dapat dilakukan terhadap korporasi sebagai entitas hukum dan/atau pengurusnya. Ketentuan ini memberikan landasan bagi penegak hukum untuk menuntut tidak hanya korporasi, tetapi juga individu yang bertanggung jawab atas pengambilan keputusan di dalam korporasi tersebut.

Lebih lanjut, Pasal 69 ayat (2) menegaskan bahwa tindak pidana dianggap dilakukan oleh korporasi apabila dilakukan oleh seseorang yang, berdasarkan hubungan kerja atau hubungan lain, bertindak dalam lingkup korporasi tersebut, baik secara individu maupun bersama-sama. Ketentuan ini memperluas cakupan

pertanggungjawaban pidana korporasi, sehingga mencakup tindakan yang dilakukan oleh karyawan, pengurus, atau pihak lain yang bertindak atas nama atau demi kepentingan korporasi.

UU PDP juga mengadopsi pendekatan yang komprehensif dengan melibatkan berbagai pihak dalam penegakan hukum. Pasal 70 mengatur bahwa penyidikan terhadap tindak pidana dalam undang-undang ini dilakukan oleh:

a) Penyidik Pegawai Negeri Sipil (PPNS) di lingkungan pemerintah yang menyelenggarakan urusan di bidang komunikasi dan informatika.
b) PPNS di lingkungan lembaga pemerintah nonkementerian yang melaksanakan tugas di bidang statistik.
c) Penyidik Kepolisian Negara Republik Indonesia.

Pasal 70 ayat (2) menetapkan kewenangan PPNS dalam melakukan penyidikan, antara lain:

a) Memeriksa laporan atau keterangan terkait tindak pidana di bidang perlindungan data pribadi.
b) Memeriksa orang dan/atau badan usaha yang diduga melakukan tindak pidana di bidang perlindungan data pribadi.
c) Memanggil orang untuk diperiksa sebagai saksi atau tersangka.
d) Memeriksa pembukuan, catatan, dan dokumen lain terkait tindak pidana perlindungan data pribadi.
e) Melakukan pemeriksaan di tempat yang diduga menyimpan barang bukti serta melakukan penyitaan terhadap barang atau dokumen terkait tindak pidana.
f) Meminta bantuan ahli untuk mendukung pelaksanaan penyidikan.
g) Menghentikan penyidikan apabila dianggap perlu.
h) Melakukan tindakan lain yang sesuai dengan hukum yang berlaku.

Ketentuan ini menunjukkan bahwa UU PDP memberikan kewenangan luas kepada PPNS dan penegak hukum untuk memastikan penegakan hukum terhadap pelanggaran data pribadi berjalan secara efektif. Pendekatan ini juga memungkinkan koordinasi yang lebih baik antara berbagai instansi dalam menangani tindak pidana terkait perlindungan data pribadi.

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi merupakan langkah strategis dalam mengatur dan mengawasi perkembangan industri *financial technology (fintech)* di Indonesia, khususnya dalam sektor *peer-to-peer lending* (*P2P lending*). Regulasi ini dirancang sebagai respons terhadap pertumbuhan signifikan layanan pinjam meminjam uang berbasis teknologi informasi, yang memerlukan kerangka hukum yang jelas guna melindungi kepentingan seluruh pihak yang terlibat, termasuk konsumen. Salah satu aspek penting yang diatur dalam peraturan ini adalah perlindungan terhadap data pribadi konsumen (Fitriana dkk., 2021).

POJK No. 77/POJK.01/2016 secara komprehensif mencakup berbagai aspek penyelenggaraan layanan pinjam meminjam uang berbasis teknologi informasi. Ketentuan dalam regulasi ini, meskipun tidak secara eksplisit menggunakan istilah "kebijakan penal," mengandung aturan yang bersifat mengikat dan dapat diinterpretasikan sebagai bentuk kebijakan penal dalam konteks perlindungan data pribadi pada sektor *fintech lending*. Dengan demikian, regulasi ini tidak hanya

bertujuan mengatur tata kelola operasional penyelenggara *P2P lending*, tetapi juga memastikan perlindungan hak-hak konsumen.

Selain itu, peraturan ini memberikan kewenangan penuh kepada OJK untuk melakukan pengawasan dan penegakan hukum terhadap penyelenggara layanan *P2P lending*. Sebagaimana diatur dalam Pasal 47, OJK memiliki otoritas untuk mengawasi operasional penyelenggara, termasuk mengenakan sanksi administratif apabila terjadi pelanggaran terhadap ketentuan yang berlaku. Sanksi yang dapat dikenakan mencakup peringatan tertulis, denda, pembatasan kegiatan usaha, hingga pencabutan izin operasional. Langkah ini mencerminkan komitmen OJK dalam memastikan keberlangsungan dan keamanan sektor *fintech lending* di Indonesia (Saly dkk., 2024).

Meskipun sanksi yang diatur dalam POJK No. 77/POJK.01/2016 bersifat administratif, ketentuan tersebut dapat dipandang sebagai bentuk kebijakan penal dalam arti luas. Pendekatan ini mencerminkan paradigma modern dalam penegakan hukum di sektor keuangan, di mana sanksi administratif sering dianggap lebih efektif dan proporsional dibandingkan dengan sanksi pidana konvensional. Hal ini terutama relevan dalam menangani pelanggaran di sektor fintech, yang bersifat sangat teknis dan dinamis (Kristian, 2022).

Selain pengaturan mengenai sanksi, POJK No. 77/POJK.01/2016 juga menetapkan kewajiban bagi penyelenggara layanan fintech untuk memiliki dan menerapkan prosedur serta mekanisme perlindungan terhadap kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, serta data keuangan yang mereka kelola. Sebagaimana diatur dalam Pasal 28, penyelenggara diwajibkan untuk memiliki sistem pengamanan yang andal dan aman, serta prosedur pencegahan yang efektif guna menghindari gangguan, kegagalan, atau kerugian. Ketentuan ini dapat dianggap sebagai bentuk kebijakan penal preventif yang bertujuan mencegah terjadinya pelanggaran terhadap data pribadi sebelum insiden tersebut terjadi (Kurniawati dan Yunanto, 2022).

Lebih lanjut, POJK No. 77/POJK.01/2016 beserta peraturan turunannya memberikan kewenangan kepada OJK untuk melakukan pemeriksaan terhadap penyelenggara, baik secara berkala maupun sewaktu-waktu. Pemeriksaan ini mencakup aspek kepatuhan terhadap ketentuan perlindungan data pribadi yang telah ditetapkan. Jika ditemukan pelanggaran, OJK memiliki kewenangan untuk menjatuhkan sanksi administratif sebagaimana diatur dalam Pasal 47 POJK No. 77/POJK.01/2016. Langkah ini menunjukkan komitmen OJK dalam memastikan kepatuhan penyelenggara terhadap regulasi dan perlindungan konsumen di sektor fintech.

POJK Nomor 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi merupakan langkah strategis dalam mengatur dan mengawasi perkembangan industri fintech di Indonesia, khususnya di sektor *peer-to-peer lending* (*P2P lending*). Regulasi ini dirumuskan sebagai respons terhadap pertumbuhan signifikan layanan pendanaan berbasis teknologi informasi yang memerlukan kerangka hukum yang jelas guna melindungi kepentingan seluruh pihak yang terlibat, termasuk perlindungan data pribadi konsumen.

POJK Nomor 10/POJK.05/2022 secara komprehensif mengatur berbagai aspek penyelenggaraan layanan pendanaan berbasis teknologi informasi, salah satunya adalah perlindungan data pribadi pengguna. Meskipun tidak secara eksplisit menggunakan istilah "kebijakan penal," ketentuan dalam peraturan ini mengandung

elemen yang bersifat mengikat, sehingga dapat diinterpretasikan sebagai bentuk kebijakan penal dalam konteks perlindungan data pribadi di sektor *fintech lending* (Noor dkk., 2023).

Salah satu aspek penting yang diatur dalam peraturan ini adalah kewajiban penyelenggara untuk menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi pengguna. Pasal 30 secara tegas menyatakan bahwa penyelenggara wajib menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, serta data keuangan yang dikelola sejak data diperoleh hingga data dimusnahkan. Ketentuan ini mencerminkan prinsip keamanan data (*data security principle*), yang diakui sebagai salah satu standar internasional dalam perlindungan data pribadi (Nursantih dan Ratnawati, 2023).

Lebih lanjut, POJK Nomor 10/POJK.05/2022 juga mengatur kewajiban penyelenggara untuk memperoleh persetujuan dari pemilik data pribadi sebelum memproses data tersebut. Pasal 31 ayat (1) menegaskan bahwa penggunaan data dan informasi pengguna yang diperoleh penyelenggara harus berdasarkan persetujuan pengguna dan digunakan sesuai dengan keperluan serta tujuan yang disampaikan saat pembukaan akun. Ketentuan ini mencerminkan prinsip persetujuan (*consent principle*), yang merupakan salah satu elemen fundamental dalam perlindungan data pribadi.

POJK Nomor 10/POJK.05/2022 memberikan kewenangan kepada Otoritas Jasa Keuangan (OJK) untuk mengawasi dan menegakkan hukum terhadap penyelenggara layanan pendanaan bersama berbasis teknologi informasi. Berdasarkan Pasal 51, OJK berwenang melakukan pengawasan terhadap penyelenggara, termasuk memberikan sanksi administratif jika terjadi pelanggaran terhadap ketentuan yang diatur dalam peraturan ini. Sanksi administratif tersebut meliputi peringatan tertulis, pembatasan kegiatan usaha, pembekuan kegiatan usaha, hingga pencabutan izin usaha.

Meskipun sanksi yang diatur dalam POJK Nomor 10/POJK.05/2022 bersifat administratif, ketentuan ini dapat dianggap sebagai bentuk kebijakan penal dalam arti luas. Pendekatan ini mencerminkan paradigma modern dalam penegakan hukum di sektor keuangan, di mana sanksi administratif sering dianggap lebih efektif dan proporsional dibandingkan dengan sanksi pidana konvensional. Hal ini sangat relevan dalam mengatur sektor fintech yang bersifat teknis dan dinamis. (Isnani dkk., 2024)

Selain pengaturan mengenai sanksi, POJK Nomor 10/POJK.05/2022 juga menetapkan kewajiban bagi penyelenggara untuk memiliki dan menerapkan prosedur serta mekanisme perlindungan data. Pasal 33 mengatur bahwa penyelenggara wajib menjaga kerahasiaan, keutuhan, dan ketersediaan data pribadi, data transaksi, dan data keuangan yang mereka kelola. Untuk itu, penyelenggara diwajibkan memiliki sistem pengamanan yang andal dan aman serta prosedur untuk mencegah gangguan, kegagalan, dan potensi kerugian. Ketentuan ini dapat diinterpretasikan sebagai bentuk kebijakan penal preventif yang bertujuan mencegah pelanggaran data pribadi sebelum insiden terjadi.

Lebih lanjut, POJK Nomor 10/POJK.05/2022 dan peraturan turunannya memberikan kewenangan kepada OJK untuk melakukan pemeriksaan terhadap penyelenggara, baik secara berkala maupun sewaktu-waktu. Pemeriksaan ini mencakup aspek kepatuhan terhadap ketentuan perlindungan data pribadi yang telah ditetapkan. Apabila ditemukan pelanggaran, OJK memiliki wewenang untuk

menjatuhkan sanksi administratif sesuai dengan ketentuan dalam Pasal 51 POJK Nomor 10/POJK.05/2022.

2. Studi Kasus Pelanggaran Data Pribadi oleh *Fintech Lending* dan Dampaknya terhadap Konsumen: Tinjauan atas Putusan Nomor 438/Pid.Sus/2020/PN.Jkt.Utr

Putusan Nomor 438/Pid.Sus/2020/PN.JKT.Utr mengungkap kasus penyalahgunaan data pribadi dan pelanggaran hukum dalam industri pinjaman *online* (*fintech lending*) di Indonesia. Kasus ini melibatkan terdakwa Dede Supardi, seorang *desk collection staff* di PT Barracuda Fintech Indonesia. Perusahaan ini merupakan penyedia layanan pinjaman *online* yang bekerja sama dengan PT Vega Data Indonesia sebagai penyedia aplikasi dan pusat layanan (*call center*).

Dalam menjalankan tugas sebagai penagih utang, terdakwa terbukti melakukan tindakan-tindakan yang melanggar hukum dan norma etika. Terdakwa secara rutin melakukan penagihan dengan menggunakan ancaman dan pemerasan melalui telepon dan pesan WhatsApp. Praktik ilegal ini tidak hanya merupakan inisiatif pribadi terdakwa, tetapi juga diketahui dan diizinkan oleh pimpinan perusahaan. Manajemen PT Barracuda Fintech Indonesia memberikan keleluasaan kepada para *desk collection staff* untuk menggunakan berbagai cara dalam menagih utang, asalkan penagihan tersebut berhasil.

Data nasabah yang digunakan untuk penagihan diperoleh melalui PT Vega Data Indonesia. Praktik ini menunjukkan adanya berbagi data pribadi secara ilegal (*private data sharing*) antar perusahaan tanpa persetujuan pemilik data. Hal ini merupakan pelanggaran serius terhadap prinsip-prinsip perlindungan data pribadi yang diakui secara hukum.

Tindakan terdakwa dalam menagih utang dengan cara mengancam dan memeras nasabah jelas melanggar berbagai ketentuan hukum. Pertama, tindakan tersebut melanggar Pasal 27 ayat (4) UU ITE, yang melarang distribusi atau pembuatan informasi elektronik yang berisi pemerasan dan/atau ancaman. Kedua, tindakan ini juga bertentangan dengan ketentuan POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, khususnya terkait larangan penggunaan data pribadi untuk kepentingan yang tidak disepakati.

Dalam putusannya, majelis hakim mempertimbangkan berbagai aspek hukum dan fakta yang terungkap selama persidangan. Hakim menyimpulkan bahwa unsur-unsur tindak pidana sebagaimana didakwakan telah terpenuhi. Terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana:

> "Dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman" sebagaimana diatur dalam Pasal 27 ayat (4) jo Pasal 45 ayat (4) UU ITE.

Dalam menjatuhkan putusan, majelis hakim mempertimbangkan berbagai faktor yang memberatkan dan meringankan terdakwa. Faktor yang memberatkan adalah perbuatan terdakwa telah menimbulkan keresahan di masyarakat dan merugikan pihak lain. Sementara itu, faktor yang meringankan meliputi sikap terdakwa yang sopan selama persidangan, pengakuan dan penyesalan atas perbuatannya, serta fakta bahwa terdakwa belum pernah dihukum sebelumnya.

Berdasarkan pertimbangan tersebut, majelis hakim menjatuhkan pidana penjara selama 1 (satu) tahun dan denda sebesar Rp70.000.000 (tujuh puluh juta

rupiah), dengan ketentuan apabila denda tidak dibayar maka diganti dengan pidana kurungan selama 2 (dua) bulan. Putusan ini dinilai relatif ringan jika dibandingkan dengan ancaman maksimal yang diatur dalam Pasal 45 ayat (4) UU ITE, yaitu pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000 (satu miliar rupiah).

Perspektif pertama berkaitan dengan lemahnya pengawasan terhadap perusahaan pinjaman *online*, baik dalam hal perizinan maupun praktik operasional mereka. PT Barracuda Fintech Indonesia, perusahaan tempat terdakwa bekerja, diketahui tidak memiliki izin resmi dari Otoritas Jasa Keuangan (OJK). Fakta ini mengungkap masih adanya celah dalam sistem pengawasan, yang memungkinkan perusahaan ilegal beroperasi tanpa pengawasan yang memadai. Hal ini menjadi ancaman serius bagi perlindungan konsumen dan stabilitas industri (Sudirman dan Disemadi, 2022).

Perspektif kedua adalah pengungkapan praktik berbagi dan penyalahgunaan data pribadi yang meluas di industri ini. Dalam kasus ini, data nasabah dengan mudah dibagikan antar perusahaan tanpa persetujuan pemilik data. Fenomena ini menunjukkan rendahnya kesadaran dan implementasi prinsip-prinsip perlindungan data pribadi di kalangan pelaku industri pinjaman *online*. Kejadian seperti ini menggarisbawahi pentingnya penguatan regulasi dan penegakan hukum terkait perlindungan data pribadi (Admiral dan Pauck, 2023).

Perspektif ketiga adalah lemahnya perlindungan konsumen dalam menghadapi praktik penagihan utang yang agresif dan melanggar hukum. Kasus ini mencerminkan pola yang sering terjadi, di mana konsumen menjadi korban intimidasi, ancaman, dan pemerasan dalam proses penagihan utang oleh perusahaan pinjaman *online*. Kondisi ini menunjukkan perlunya mekanisme perlindungan konsumen yang lebih kuat dan pengawasan yang lebih ketat terhadap metode penagihan yang digunakan oleh penyelenggara layanan (Rahmayani, 2018).

Putusan ini juga memperlihatkan potensi UU ITE sebagai instrumen efektif dalam menangani kejahatan siber, termasuk dalam konteks fintech. Namun, penerapan UU ITE dalam kasus seperti ini harus disertai dengan pemahaman mendalam tentang karakteristik dan dinamika industri fintech. Langkah ini penting untuk memastikan bahwa hukum yang diterapkan tidak hanya bersifat represif, tetapi juga mampu mendukung pengembangan industri yang berkelanjutan.

Putusan ini menyoroti pentingnya prinsip pertanggungjawaban korporasi dalam tindak pidana yang melibatkan perusahaan. Meskipun dalam kasus ini yang dihukum adalah seorang karyawan individual, tindakan tersebut dilakukan dalam konteks kebijakan dan operasional perusahaan. Fakta ini menunjukkan adanya celah dalam penerapan prinsip pertanggungjawaban korporasi. Ke depan, penerapan prinsip ini perlu diperkuat untuk mencegah perusahaan berlindung di balik tindakan karyawannya ketika terjadi pelanggaran hukum (Wahyono, 2021).

Penulis menilai bahwa putusan pengadilan telah tepat dalam menjatuhkan hukuman kepada terdakwa. Namun, langkah ini belum cukup untuk mengatasi akar permasalahan di industri *fintech lending*. Kasus ini mencerminkan hanya puncak gunung es dari berbagai praktik ilegal dan tidak etis yang terjadi di industri ini.

Diperlukan pendekatan yang lebih holistik dan sistemik untuk menangani permasalahan ini. Pendekatan tersebut dapat mencakup:

a) Penguatan Regulasi dan Pengawasan. Regulasi dan pengawasan terhadap perusahaan pinjaman *online* perlu diperkuat, mencakup aspek perizinan,

praktik operasional, dan perlindungan data pribadi. Otoritas Jasa Keuangan (OJK) dan regulator terkait harus meningkatkan kapasitas serta sumber daya mereka untuk menghadapi tantangan pengawasan di industri yang berkembang pesat ini (Khoirunisa dkk., 2023).

b) Edukasi Masyarakat. Diperlukan edukasi yang intensif kepada masyarakat mengenai risiko dan tanggung jawab dalam menggunakan layanan *fintech lending*. Banyak konsumen yang terjebak dalam utang akibat kurangnya pemahaman tentang konsekuensi finansial dari pinjaman *online*. Edukasi ini dapat mendorong pengambilan keputusan yang lebih bijaksana oleh konsumen.

c) Mendorong Praktik Bisnis yang Etis dan Bertanggung Jawab. Industri *fintech lending* perlu diarahkan untuk mengadopsi praktik bisnis yang lebih etis dan bertanggung jawab. Langkah ini dapat dilakukan melalui kombinasi regulasi yang lebih ketat, insentif bagi perusahaan yang menerapkan praktik terbaik, dan dorongan untuk menerapkan *self-regulation* di kalangan pelaku industri.

Kasus ini juga menggarisbawahi pentingnya perlindungan data pribadi di Indonesia. Penyalahgunaan data pribadi yang terungkap menunjukkan betapa mudahnya data konsumen disalahgunakan. Dengan telah disahkannya UU PDP, pemerintah harus segera mengimplementasikan dan menegakkan aturan ini secara efektif.

Kasus ini harus menjadi *wake-up call* bagi semua pemangku kepentingan, termasuk pemerintah, regulator, pelaku industri, dan masyarakat. Semua pihak harus bekerja sama untuk menciptakan ekosistem pinjaman *online* yang sehat, aman, dan bermanfaat bagi semua pihak. Pendekatan kolaboratif yang mengedepankan regulasi, edukasi, dan inovasi yang bertanggung jawab menjadi kunci untuk mengatasi tantangan di sektor ini.

3. Analisis Kebijakan Penal dalam Perlindungan Hukum terhadap Data Pribadi Nasabah *Fintech Lending* di Indonesia

Undang-Undang Perlindungan Data Pribadi (UU PDP), yang disahkan pada tahun 2022, merupakan langkah signifikan dalam melindungi data pribadi warga negara Indonesia. UU ini mengadopsi prinsip-prinsip perlindungan data yang diakui secara internasional, seperti prinsip persetujuan (*consent principle*), pembatasan penggunaan (*purpose limitation*), dan keamanan data (*data security*). Dari perspektif teori perlindungan hukum yang dikemukakan oleh Philipus M. Hadjon, UU PDP memberikan perlindungan hukum yang bersifat preventif dan represif.

Perlindungan hukum preventif tercermin dari ketentuan yang mewajibkan pengendali dan prosesor data untuk:

a) Menerapkan langkah-langkah keamanan yang memadai.

b) Melakukan penilaian dampak perlindungan data (*data protection impact assessment*).

c) Memperoleh persetujuan dari pemilik data sebelum memproses data pribadi.

Sementara itu, perlindungan represif diwujudkan melalui ketentuan sanksi administratif dan pidana bagi pihak yang melanggar UU PDP. Pendekatan ini menunjukkan adanya upaya komprehensif untuk mencegah dan menindak pelanggaran dalam pemrosesan data pribadi (Fauzi dan Radika Shandy, 2022).

Meskipun UU PDP memberikan kerangka hukum yang kuat, efektivitasnya masih harus diuji dalam tahap implementasi. Salah satu tantangan utama adalah pembentukan dan operasionalisasi lembaga pengawas perlindungan data pribadi, yang berfungsi untuk mengawasi kepatuhan terhadap UU PDP dan menangani pengaduan terkait pelanggaran data pribadi.

Keterlambatan dalam pembentukan lembaga ini dapat mengurangi efektivitas perlindungan yang dijanjikan oleh UU PDP. Hal ini menjadi perhatian utama karena lembaga pengawas memiliki peran krusial dalam memastikan pelaksanaan prinsip-prinsip perlindungan data secara konsisten (Yolanda dan Hutabarat, 2023).

Dari sudut pandang teori kepastian hukum yang dikemukakan oleh Satjipto Rahardjo, UU PDP memberikan kerangka hukum yang lebih jelas dan komprehensif dibandingkan regulasi sebelumnya. UU ini secara tegas mendefinisikan apa yang dimaksud dengan data pribadi, hak-hak subjek data, dan kewajiban pengendali dan prosesor data.

Kejelasan ini diharapkan dapat meningkatkan kepastian hukum bagi semua pihak yang terlibat dalam pemrosesan data pribadi, sekaligus mendorong kepatuhan terhadap aturan yang berlaku (Julyano dan Sulistyawan, 2019).

Meskipun UU PDP telah memberikan kerangka hukum yang lebih jelas, masih terdapat beberapa area yang memerlukan klarifikasi untuk meningkatkan kepastian hukum. Salah satu area tersebut adalah mekanisme persetujuan yang dianggap valid dalam konteks digital, yang hingga kini memerlukan panduan lebih rinci. Selain itu, kriteria untuk menentukan "kepentingan yang sah" sebagai dasar hukum pemrosesan data pribadi juga perlu dijabarkan lebih detail untuk menghindari penafsiran yang terlalu luas dan potensial disalahgunakan (Jannah, 2022).

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) juga memiliki peran penting dalam perlindungan data pribadi di Indonesia. Dari perspektif teori perlindungan hukum, UU ITE memberikan perlindungan preventif dengan mewajibkan penyelenggara sistem elektronik untuk menjaga kerahasiaan data pribadi pengguna. Perlindungan represif diwujudkan melalui sanksi pidana bagi pihak yang melanggar ketentuan perlindungan data pribadi (Jannah, 2022).

Namun, dari sudut pandang teori kepastian hukum, UU ITE memberikan kerangka hukum yang cukup jelas untuk transaksi elektronik secara umum tetapi kurang memberikan kepastian dalam konteks perlindungan data pribadi. Dibandingkan dengan UU PDP, UU ITE lebih bersifat umum sehingga memerlukan harmonisasi untuk memastikan perlindungan data pribadi yang lebih komprehensif di era digital (Jannah, 2022).

Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 dan POJK Nomor 10/POJK.05/2022 memberikan kerangka regulasi yang lebih spesifik terkait perlindungan data pribadi dalam konteks *fintech lending*. Dari perspektif teori perlindungan hukum, kedua POJK ini memberikan perlindungan preventif melalui kewajiban penyelenggara *fintech lending* untuk menjaga kerahasiaan data pribadi nasabah dan memperoleh persetujuan nasabah sebelum menggunakan data pribadi untuk keperluan tertentu.

Perlindungan represif dalam Peraturan Otoritas Jasa Keuangan (POJK) terlihat dari adanya sanksi administratif bagi pelanggaran terhadap ketentuan perlindungan data pribadi. Namun, sanksi yang diatur dalam POJK ini terbatas pada sanksi administratif dan tidak mencakup sanksi pidana seperti yang diatur dalam

UU PDP dan UU ITE. Ketiadaan sanksi pidana dalam POJK dapat mengurangi efek jera bagi pelaku pelanggaran serius terhadap data pribadi nasabah (Ndruru dkk., 2023).

Dari sudut pandang teori kepastian hukum, POJK memberikan kerangka regulasi yang cukup jelas untuk perlindungan data pribadi dalam konteks *fintech lending*. Namun, terdapat beberapa area yang memerlukan klarifikasi lebih lanjut. Salah satunya adalah mekanisme persetujuan yang dianggap valid dalam konteks digital, yang hingga saat ini belum memiliki panduan teknis yang memadai. Selain itu, prosedur penanganan pelanggaran data pribadi juga memerlukan aturan yang lebih rinci untuk memastikan keadilan bagi semua pihak yang terlibat.

Salah satu kelebihan kebijakan penal perlindungan data pribadi di Indonesia adalah keberadaan kerangka hukum yang komprehensif yang mencakup berbagai sektor. UU PDP berfungsi sebagai kerangka umum yang mengatur prinsip-prinsip dasar perlindungan data pribadi, sementara UU ITE dan POJK memberikan regulasi yang lebih spesifik untuk sektor tertentu, seperti layanan teknologi informasi dan *fintech lending*. Kombinasi ini memungkinkan pendekatan yang lebih holistik dalam upaya melindungi data pribadi, sekaligus menyesuaikan regulasi dengan kebutuhan dan karakteristik masing-masing sektor.

Kebijakan penal yang ada telah memberikan perlindungan yang cukup komprehensif terhadap data pribadi nasabah. Namun, terdapat beberapa kelemahan yang memerlukan perhatian lebih lanjut. Mekanisme kompensasi bagi korban pelanggaran data pribadi belum diatur secara jelas. Ketidakjelasan ini dapat menghambat pemulihan hak korban dan mengurangi akuntabilitas bagi pelaku pelanggaran. Prosedur terkait penanganan pelanggaran data, termasuk kewajiban notifikasi kepada nasabah yang terdampak, memerlukan pengaturan yang lebih rinci. Hal ini penting untuk memastikan transparansi dan tanggung jawab dalam penanganan insiden pelanggaran.

Dengan sifat lintas batas dari aliran data di era digital, Indonesia perlu memperhatikan aspek interoperabilitas dengan rezim perlindungan data di negara lain. Interoperabilitas ini penting untuk mendukung aliran data internasional yang diperlukan dalam perdagangan global dan inovasi teknologi, tanpa mengabaikan standar perlindungan data yang tinggi. Upaya ini juga dapat memperkuat daya saing Indonesia dalam ekonomi digital global.

Praktik berbagi data antarperusahaan (*data sharing*) dalam industri *fintech lending* sering kali menimbulkan risiko pelanggaran privasi. Oleh karena itu, regulasi perlu menetapkan batasan dan persyaratan yang jelas terkait berbagi data, termasuk kewajiban untuk memperoleh persetujuan eksplisit dari nasabah sebelum data dibagikan dan penerapan standar keamanan yang memadai dalam proses transfer data untuk mencegah kebocoran atau penyalahgunaan data.

Industri *fintech lending* memiliki karakteristik khusus yang melibatkan data keuangan yang sensitif. Oleh karena itu, perlu diterapkan standar keamanan yang lebih tinggi, seperti:

a) Data keuangan nasabah harus dienkripsi secara menyeluruh (*end-to-end*) untuk melindungi kerahasiaan informasi selama proses penyimpanan dan transfer.
b) Perusahaan *fintech lending* wajib melakukan audit keamanan secara berkala untuk memastikan kepatuhan terhadap standar keamanan dan mengidentifikasi potensi kerentanan.

D. SIMPULAN

Meskipun telah ada regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta Peraturan Otoritas Jasa Keuangan (POJK), implementasi dan penegakan hukum perlindungan data pribadi di Indonesia masih menghadapi berbagai tantangan signifikan. Tantangan ini meliputi: Ketidakharmonisan antara berbagai peraturan membuat interpretasi dan penerapan hukum menjadi tidak konsisten, penegakan hukum sering kali terkendala oleh kurangnya kapasitas institusi pengawas dan prosedur hukum yang belum memadai, serta tingkat pemahaman masyarakat dan pelaku usaha mengenai hak dan kewajiban terkait perlindungan data pribadi masih rendah, yang menghambat upaya perlindungan secara menyeluruh.

Kebijakan penal yang ada saat ini memberikan kerangka hukum yang lebih komprehensif dibandingkan regulasi sebelumnya. UU PDP mengatur prinsip-prinsip dasar perlindungan data pribadi, seperti hak subjek data atas informasi, akses, dan penghapusan data pribadinya. Regulasi ini memberikan landasan hukum yang kuat, tetapi efektivitasnya sangat bergantung pada implementasi yang konsisten dan pengawasan yang ketat oleh pihak berwenang. UU ITE memberikan perlindungan preventif dan represif terhadap pelanggaran data pribadi. Namun, definisi data pribadi dan hak-hak subjek data dalam UU ini kurang spesifik dibandingkan UU PDP, sehingga menimbulkan ketidakpastian hukum dalam penerapannya. POJK memberikan kerangka regulasi yang spesifik untuk perlindungan data pribadi dalam konteks *fintech lending*. Regulasi ini mewajibkan penyelenggara untuk menjaga kerahasiaan data pribadi nasabah dan memperoleh persetujuan sebelum memproses data tersebut. Namun, sanksi yang diatur terbatas pada sanksi administratif, tanpa mencakup sanksi pidana, yang dapat mengurangi efek jera terhadap pelanggaran serius.

Kondisi ini menunjukkan perlunya harmonisasi antara UU PDP, UU ITE, dan POJK untuk meningkatkan kepastian hukum dan efektivitas perlindungan data pribadi. Harmonisasi ini dapat dilakukan dengan menyusun panduan teknis yang selaras untuk implementasi ketiga regulasi tersebut, memperjelas pembagian peran dan kewenangan antara lembaga terkait untuk menghindari tumpang tindih, serta memperkuat sanksi dalam POJK agar lebih mencakup pelanggaran serius dengan dampak signifikan terhadap nasabah.

DAFTAR PUSTAKA

Admiral, A., dan Pauck, M. A. (2023). Unveiling the Dark Side of Fintech: Challenges and Breaches in Protecting User Data in Indonesia's Online Loan Services. Lex Scientia Law Review, 7(2), 995–1048. https://doi.org/10.15294/lesrev.v7i2.77881

Ali, F., dan Andika, F. (2023). 4 Tindak Pidana Dalam UU PDP dan Sanksinya! sippn.menpan.go.id/. https://sippn.menpan.go.id/berita/59933/rumah-tahanan-negara-kelas-iib-pelaihari/4-tindak-pidana-dalam-uu-pdp-dan-sanksinya

Farisa, F. C. (2022). Jenis-jenis Data Pribadi Menurut UU PDP, Ini Rinciannya. Kompas.com. https://nasional.kompas.com/read/2022/09/20/13143351/jenis-jenis-data-pribadi-menurut-uu-pdp-ini-rinciannya

Fauzi, E., dan Radika Shandy, N. A. (2022). Hak Atas Privasi dan Politik Hukum

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Jurnal Lex Renaissance, 7(3), 445–461. https://doi.org/10.20885/JLR.vol7.iss3.art1

Fitriana, D., Rahman, N., dan Wahid, A. (2021). Analisa Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (LPMUBTI) Terhadap Penggunaan Financial Technology (Fintech) Pada Industri Jasa Perbankan di Wilayah III Cirebon. Mahkamah: Jurnal Kajian Hukum Islam, 6(1), 1. https://doi.org/10.24235/mahkamah.v6i1.7722

Indotelko. (2018). Fintech Lending Langgar Aturan Lakukan Persekusi Digital. Indotelko. https://www.indotelko.com/read/1532239943/fintech-lending-persekusi-digital

Isnani, A. M., Haditami, N., Kamil, M. I., dan Zain, I. I. (2024). Financial Services Authority Laws Against Non-Bank Financial Institutions Based on Outlaw Financial Technology. International Journal of Multicultural and Multireligious Understanding, 11(5), 210. https://doi.org/10.18415/ijmmu.v11i5.5701

Jannah, L. M. (2022). UU Perlindungan Data Pribadi dan Tantangan Implementasinya. fia.ui.ac.id. https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/

Julyano, M., dan Sulistyawan, A. Y. (2019). Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum. Crepido, 1(1), 13–22. https://doi.org/10.14710/crepido.1.1.13-22

Khoirunisa, D., Arifiani, N. D., Maulana, M. R., dan Panggiarti, E. K. (2023). Analisis Peran Otoritas Jasa Keuangan (OJK) dalam Mengawasi Pelayanan Pada Perusahaan Financial Technology (Fintech) di Indonesia. Inisiatif: Jurnal Ekonomi, Akuntansi dan Manajemen, 2(3), 127–132. https://doi.org/https://doi.org/10.30640/inisiatif.v2i3.1108

Kristian, O. Y. (2022). Perlindungan Hukum Pengguna Layanan Fintech P2P Lending dari Tindak Pidana Ekonomi dan Terhadap Penyedia Layanan Fintech P2P Lending Ilegal. Majalah Hukum Nasional, 52(2), 297–320. https://doi.org/https://doi.org/10.33331/mhn.v52i2.174

Kurniawati, H., dan Yunanto, Y. (2022). Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur Dalam Aktivitas Pinjaman Online. Jurnal Ius Constituendum, 7(1), 102. https://doi.org/10.26623/jic.v7i1.4290

Martaon, A. T. (2023, Februari 27). Kekurangan The Right to be Forgotten di UU ITE dan UU PDP. Medcom.id. https://www.medcom.id/nasional/politik/nbw045Bk-kekurangan-the-right-to-be-forgotten-di-uu-ite-dan-uu-pdp

Muhamad, N. (2024, Mei 14). Penyaluran Pinjol di Indonesia Naik Jadi Rp22,76 Triliun pada Maret 2024. databoks.katadata. https://databoks.katadata.co.id/datapublish/2024/05/14/penyaluran-pinjol-di-indonesia-naik-jadi-rp2276-triliun-pada-maret-2024

Nasikhatuddini, S. (2021). Perlindungan Hukum Pidana Terhadap Nasabah Dalam Pelaksanaan Pinjam Meminjam Uang Berbasis Teknologi Informasi (Fintech) Peer to Peer Lending. Jurnal Lex Renaissance, 6(3). https://doi.org/10.20885/JLR.vol6.iss3.art1

Ndruru, L., Herman, C. W., Ttistian, D. O., dan Widodo, S. (2023). Law Enforcement

on Misuse of Personal Data by Online Loan Business Actors. Indonesian Journal of Law and Islamic Law (IJLIL), 5(2), 40–49. https://doi.org/10.35719/ijlil.v5i2.317

Noor, A., Wulandari, D., dan Muhammad Afif, A.-S. (2023). Regulating Fintech Lending in Indonesia: A Study of Regulation of Financial Services Authority No. 10/POJK.05/2022. Qubahan Academic Journal, 3(4), 42–50. https://doi.org/10.48161/qaj.v3n4a156

Nursantih, N., dan Ratnawati, E. (2023). Pengawasan OJK Atas Data Pribadi Konsumen Pada Perusahaan Peer to Peer Lending. Unes Law Review, 5(4), 1564–1579. https://doi.org/https://doi.org/10.31933/unesrev.v5i4.453

Oktavira, B. A. (2020). Jerat Hukum Pelaku Cracking Menurut UU PDP dan UU ITE. Hukumonline. https://www.hukumonline.com/klinik/a/dasar-hukum-perlindungan-data-pribadi-pengguna-internet-lt4f235fec78736/

Pakpahan, E. F., Chandra, L. R., dan Dewa, A. A. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology. Veritas et Justitia, 6(2), 298–323. https://doi.org/https://doi.org/10.25123/vej.v6i2.3778

Rahmayani, N. (2018). Tinjauan Hukum Perlindungan Konsumen Terkait Pengawasan Perusahaan Berbasis Financial Technology di Indonesia. Pagaruyuang Law Journal, 2(1), 24–41. https://doi.org/https://doi.org/10.31869/plj.v2i1.887

Saly, J. N., Artamevia, H., Kheista, K., Gulo, B. J. S., Rhemrev, E. A., dan Christie, M. (2024). Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022. Jurnal Serina Sosial Humaniora, 1(3), 145–153. https://journal.untar.ac.id/index.php/JSSH/article/view/28615

Saputra, F. (2024). Per April 2024, Ada 15 Fintech Lending dengan TWP90 di Atas 5%. Kontan.co.id. https://keuangan.kontan.co.id/news/per-april-2024-ada-15-fintech-lending-dengan-twp90-di-atas-5

Saputra, F. (2024). Outstanding Pembiayaan Fintech P2P Lending Capai Rp 66,79 Triliun pada Juni 2024. Kontan.co.id. https://keuangan.kontan.co.id/news/outstanding-pembiayaan-fintech-p2p-lending-capai-rp-6679-triliun-pada-juni-2024

Siaran Pers Kominfo. (2018). Jamin Perlindungan Data Pribadi, Kominfo Beri Sanksi Terhadap Penyalahgunaan oleh Pihak Ketiga. kominfo.go.id. https://www.kominfo.go.id/content/detail/12865/siaran-pers-no-85hmkominfo042018-tentang-jamin-perlindungan-data-pribadi-kominfo-beri-sanksi-terhadap-penyalahgunaan-oleh-pihak-ketiga/0/siaran_pers

Sudirman, L., dan Disemadi, H. S. (2022). Titik Lemah Industri Keuangan Fintech di Indonesia: Kajian Perbandingan Hukum. Jurnal Pembangunan Hukum Indonesia, 4(3), 471–493. https://doi.org/10.14710/jphi.v4i3.471-493

Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. Jurnal Suara Hukum, 3(1), 53–84. https://doi.org/10.26740/jsh.v3n1.p53-84

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Wahyono, D. (2021). The Criminal Responsibility by Corporate. International Journal of Law Reconstruction, 5(1), 126. https://doi.org/10.26532/ijlr.v5i1.15587

Wahyuni, W. (2022). Dua Jenis Data Pribadi yang Perlu Dilindungi Menurut UU PDP. Hukumonline. https://www.hukumonline.com/berita/a/dua-jenis-data-pribadi-yang-perlu-dilindungi-menurut-uu-pdp-lt6349e2932bd09/

Yolanda, E., dan Hutabarat, R. R. (2023). Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif. Syntax Literate: Jurnal Ilmiah Indonesia, 8(6), 4166–4182. https://doi.org/10.36418/syntax-literate.v8i6.12583

Yusuf. (2020). Transfer Data Antarnegara Bisa Dilakukan jika Memiliki Aturan Setara UU PDP. Aptika.Kominfo. https://aptika.kominfo.go.id/2020/08/transfer-data-antarnegara-bisa-dilakukan-jika-memiliki-aturan-setara-uu-pdp/