ANALISIS KETERBATASAN PENGATURAN PASAL 21 UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI DALAM MENGATASI PELANGGARAN PRIVASI PADA PRAKTIK PENAGIHAN PINJAMAN ONLINE

Bintang Pradisa[1] dan Vita Mahardhika[2]

[1]Fakultas Hukum, Universitas Negeri Surabaya, Surabaya, Indonesia,bintang.22283@mhs.unesa.ac.id , https://orcid.org/0000-0001-9744-588X [2]Fakultas Hukum, Universitas Negeri Surabaya, Surabaya, Indonesia, vitamahardhika@unesa.ac.id,https://orcid.org/0000-0001-9744-588X

Abstrak

The rapid growth of online lending services has intensified personal data processing, particularly in debt collection practices that raise privacy concerns. This study analyzes the regulation of personal data processing purposes under Indonesia's Personal Data Protection Law (Law Number 27 of 2022, with particular emphasis on Article 21, in relation to online lending services and examines the implications of its regulatory limitations for legal accountability in cases of personal data misuse during debt collection. This research employs a normative legal method using statutory, conceptual, comparative, and case approaches. Legal materials were analyzed prescriptively. The study yields two principal findings. First, Article 21 requires data controllers to notify data subjects of processing purposes but does not explicitly integrate this obligation with Articles 27 and 28, allowing formal compliance without ensuring adherence to the principle of purpose limitation. Second, this normative gap creates legal uncertainty in determining purpose limitation violations, potential moral hazard within the controller–processor accountability framework, and ineffective law enforcement due to the absence of implementing Government Regulations and the incomplete operationalization of the personal data protection supervisory authority. This study recommends integrating Articles 21, 27, and 28, issuing implementing regulations, and strengthening accountability mechanisms for controllers and processors in online lending debt collection.

Kata kunci*: Personal Data Protection, Article 21 of the Personal Data Protection Law, Privacy, Online Loan Collection, Online Lendi.*

A. PENDAHULUAN

Latar Belakang

Data Otoritas Jasa Keuangan (OJK) menunjukkan pertumbuhan yang signifikan dalam jumlah penyelenggara layanan pinjaman online yang terdaftar dan berizin. Hingga akhir tahun 2024, terdapat ratusan penyelenggara aktif dengan total nilai penyaluran pinjaman yang terus meningkat dari tahun ke tahun, mencerminkan tingginya permintaan masyarakat terhadap layanan pembiayaan digital ini. Fenomena ini sejalan dengan agenda nasional literasi dan inklusi keuangan yang dicanangkan oleh pemerintah, sekaligus merefleksikan pergeseran perilaku masyarakat dalam mengakses layanan keuangan di era transformasi digital.

Namun demikian, kemudahan akses yang ditawarkan oleh layanan pinjaman online tidak terlepas dari berbagai risiko, terutama yang berkaitan dengan perlindungan data pribadi pengguna. Dalam praktiknya, penyelenggara pinjaman online mensyaratkan akses terhadap berbagai data pribadi sebagai bagian dari proses verifikasi dan analisis kelayakan kredit. Data yang dikumpulkan tidak hanya terbatas pada identitas dasar seperti nama, alamat, dan nomor identitas, tetapi juga mencakup data yang bersifat lebih sensitif, seperti daftar kontak yang tersimpan di perangkat pengguna, data lokasi, foto, riwayat transaksi, serta akses terhadap berbagai fitur perangkat pengguna.

Kondisi demikian menunjukkan adanya potensi besar terhadap penyalahgunaan data pribadi apabila tidak disertai dengan mekanisme perlindungan yang memadai dari sisi hukum maupun teknis. Dalam penelitian atau kajian perlindungan data pribadi, terdapat prinsip-prinsip dasar yang menjadi landasan dalam setiap pemrosesan data, antara lain prinsip legalitas, transparansi, pembatasan tujuan, minimalisasi data, dan akuntabilitas. Prinsip minimalisasi data menekankan bahwa data yang dikumpulkan harus relevan dan tidak berlebihan sesuai dengan tujuan pemrosesan. Apabila dikaitkan

dengan praktik pinjaman online, permintaan akses terhadap seluruh kontak, galeri, dan data pribadi lainnya menunjukkan adanya ketidaksesuaian dengan prinsip tersebut, sehingga berpotensi melanggar ketentuan perlindungan data pribadi pengguna. Intensitas pengumpulan data dalam layanan pinjaman online melampaui kebutuhan yang sesungguhnya diperlukan untuk pelaksanaan perjanjian pinjam-meminjam, sehingga berpotensi melanggar prinsip minimalisasi data yang menjadi salah satu fondasi dalam sistem perlindungan data pribadi modern.

Dalam sistem perlindungan data pribadi, terdapat prinsip fundamental yang dikenal sebagai *purpose limitation* atau pembatasan tujuan. Prinsip ini menegaskan bahwa data pribadi yang dikumpulkan untuk suatu tujuan tertentu tidak boleh digunakan untuk tujuan lain yang berbeda atau tidak sesuai dengan tujuan awal pemrosesan tersebut. Dengan kata lain, tujuan yang dinyatakan pada saat pengumpulan data merupakan batas hukum yang mengikat bagi pengendali data dalam seluruh rangkaian pemrosesan berikutnya. Prinsip ini dalam doktrin perlindungan data dikenal pula sebagai *purpose specification*, yang menegaskan bahwa data pribadi hanya boleh diproses untuk tujuan yang spesifik, eksplisit, dan sah sebagaimana dinyatakan sejak awal, serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut.

Sesuai dengan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dan peraturan terkait lainnya, pemrosesan data pribadi harus dilakukan dengan persetujuan dari subjek data, dan hanya untuk tujuan yang telah disetujui sebelumnya. Hal ini sejalan dengan Pasal 16 dalam Undang-Undang Perlindungan Data Pribadi yang menegaskan bahwa persetujuan harus diberikan secara sukarela, tanpa paksaan, serta dapat dicabut kapan saja oleh pemilik data. Namun, dalam praktiknya, banyak penyelenggara pinjaman online yang mencantumkan klausul kebijakan privasi

yang tidak jelas atau berpotensi menyesatkan. Sebagai hasilnya, persetujuan yang diberikan oleh nasabah sering kali tidak bersifat spesifik dan jelas, tidak sepenuhnya disadari, dan lebih cenderung menjadi prosedur administratif belaka.

Persoalan pelanggaran *purpose limitation* paling sering terjadi dalam praktik penagihan pinjaman online. Penyelenggara layanan umumnya menyatakan bahwa tujuan pengumpulan data pribadi adalah untuk keperluan verifikasi identitas dan analisis kelayakan kredit pengguna. Namun dalam kenyataannya, data yang sama — khususnya daftar kontak pada perangkat pengguna — kemudian digunakan untuk keperluan penagihan dengan cara menghubungi pihak-pihak yang tidak memiliki hubungan hukum apa pun dengan perjanjian pinjaman yang bersangkutan. Hal ini secara substantif melampaui tujuan awal yang dinyatakan dan seharusnya tidak diperkenankan dalam kerangka hukum perlindungan data pribadi.

Lebih lanjut, Pasal 21 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (selanjutnya disebut UU PDP) mengatur bahwa pemrosesan data pribadi wajib dilakukan secara terbatas dan spesifik sesuai dengan tujuan yang ditetapkan. Pasal 21 ayat (1) UU PDP mewajibkan pengendali data pribadi untuk menyampaikan tujuh jenis informasi kepada subjek data pribadi, yaitu: (a) legalitas dari pemrosesan data pribadi; (b) tujuan pemrosesan data pribadi; (c) jenis dan relevansi data pribadi yang akan diproses; (d) jangka waktu retensi dokumen yang memuat data pribadi; (e) rincian mengenai informasi yang dikumpulkan; (f) jangka waktu pemrosesan data pribadi; dan (g) hak subjek data pribadi.

Dari ketujuh informasi wajib tersebut, informasi mengenai tujuan pemrosesan data pribadi merupakan unsur yang paling sentral sekaligus menjadi inti permasalahan dalam penelitian ini. Kewajiban menyampaikan tujuan pemrosesan bukan sekadar formalitas administratif, melainkan memiliki konsekuensi hukum yang mengikat, yakni

bahwa tujuan yang telah dinyatakan kepada subjek data pada saat pengumpulan data merupakan batas hukum yang tidak boleh dilampaui oleh pengendali data dalam seluruh rangkaian pemrosesan berikutnya. Keterbatasan mendasar dari Pasal 21 terletak pada sifatnya yang masih bersifat normatif umum tanpa disertai ketentuan teknis yang operasional, sehingga ruang lingkup "tujuan yang disetujui" dan "penggunaan yang sesuai" menjadi mudah ditafsirkan secara luas oleh pengendali data, termasuk penyelenggara pinjaman online, tanpa adanya parameter yang jelas dan terukur.

Kondisi keterbatasan norma tersebut tidak hanya berdampak pada aspek privasi, tetapi juga menimbulkan implikasi hukum yang luas. Dalam aspek pidana, tindakan penyebaran data tanpa hak dapat dikualifikasikan sebagai perbuatan melawan hukum yang dapat dikenakan sanksi pidana. Oleh karena itu, perlindungan terhadap data pribadi menjadi penting tidak hanya untuk melindungi hak individu, tetapi juga sebagai bagian dari penegakan hukum. Selain itu, maraknya pinjaman online ilegal semakin memperparah kondisi perlindungan data pribadi di Indonesia. Pinjol ilegal umumnya tidak tunduk pada ketentuan hukum yang berlaku serta tidak memiliki standar keamanan data yang memadai, sehingga data pribadi pengguna menjadi sangat rentan untuk disalahgunakan.

Penelitian ini beranjak dari suatu premis bahwa permasalahan perlindungan data pribadi dalam praktik penagihan pinjaman online bukan semata-mata disebabkan oleh ketiadaan norma hukum, melainkan oleh apa yang disebut sebagai keterbatasan arsitektur norma. Maksudnya adalah kondisi di mana norma-norma yang dibutuhkan sebenarnya sudah ada dalam suatu peraturan perundang-undangan, tetapi norma-norma tersebut tidak saling terintegrasi satu sama lain dalam suatu mekanisme operasional yang koheren, sehingga menciptakan celah hukum yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab.

Secara lebih konkret, norma *purpose limitation* dalam UU PDP telah dirumuskan dalam Pasal 27 (kewajiban spesifisitas tujuan) dan Pasal 28 (kewajiban pemrosesan sesuai tujuan). Namun, Pasal 21 sebagai ketentuan yang mengatur kewajiban operasional pengendali data — yakni kewajiban memberitahukan informasi kepada subjek data sebelum pemrosesan dilakukan — tidak secara eksplisit merujuk kepada Pasal 27 dan Pasal 28. Tidak adanya integrasi eksplisit ini menciptakan situasi di mana pengendali data dapat memenuhi kewajiban formalnya berdasarkan Pasal 21 (memberitahukan tujuan pemrosesan) tanpa harus tunduk pada standar spesifisitas dan pembatasan yang diatur dalam Pasal 27 dan Pasal 28. Hal inilah yang disebut sebagai keterbatasan arsitektur norma UU PDP, yang menjadi fokus utama analisis dalam penelitian ini.

Keterbatasan arsitektur norma ini diperparah oleh belum terbitnya peraturan pemerintah (PP) pelaksana yang diamanatkan oleh beberapa pasal dalam UU PDP. Ketentuan-ketentuan dalam UU PDP yang memerlukan PP pelaksana antara lain mencakup tata cara pemberian persetujuan, mekanisme pengenaan ganti rugi, serta mekanisme penilaian dampak perlindungan data pribadi. Seluruh PP pelaksana ini hingga saat penelitian dilakukan belum diterbitkan, sehingga menyebabkan keseluruhan ekosistem norma UU PDP beroperasi tanpa petunjuk teknis yang memadai. Kondisi ini secara langsung memperlemah efektivitas perlindungan data pribadi dalam praktik layanan pinjaman online.

Dalam perspektif hukum, data pribadi merupakan bagian dari hak asasi manusia yang harus dilindungi oleh negara. Perlindungan terhadap data pribadi berkaitan erat dengan hak atas privasi yang melekat pada setiap individu. Oleh karena itu, negara memiliki kewajiban untuk menghadirkan regulasi yang mampu memberikan perlindungan hukum secara komprehensif terhadap data pribadi masyarakat. Sebagai

bentuk perlindungan hukum tersebut, pemerintah Indonesia telah mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi yang mengatur pemrosesan data pribadi secara menyeluruh. Undang-undang ini menegaskan bahwa setiap pemrosesan data harus didasarkan pada persetujuan yang sah serta dilakukan untuk tujuan yang jelas dan terbatas.

Signifikansi dari penelitian ini semakin diperkuat oleh fakta bahwa pelanggaran privasi dalam praktik penagihan tidak hanya terjadi pada penyelenggara pinjaman online ilegal yang beroperasi di luar pengawasan regulator, melainkan juga terdokumentasi pada penyelenggara resmi yang telah terdaftar dan berada di bawah pengawasan OJK. Kondisi ini secara tegas menunjukkan bahwa permasalahan yang ada bukan sekadar soal ketidakpatuhan pelaku usaha secara individual, melainkan lebih mendasar pada ketidaklengkapan arsitektur norma UU PDP itu sendiri.

Meskipun banyak penelitian yang membahas perlindungan data pribadi dalam sektor fintech dan pinjaman online, sebagian besar fokus pada aspek keamanan data atau bagaimana data dikumpulkan dan digunakan. Namun, hanya sedikit penelitian yang membahas secara mendalam siapa yang seharusnya bertanggung jawab ketika terjadi penyalahgunaan data pribadi dalam praktik pinjaman online. Meskipun penyelenggara pinjol mengumpulkan dan memproses data pribadi nasabah, *debt collector* yang bekerja sama dengan pinjol juga turut serta dalam penggunaan data untuk penagihan, sering kali tanpa adanya izin yang jelas dari nasabah. Hal ini menimbulkan kebingungan mengenai pihak yang seharusnya bertanggung jawab secara hukum ketika data pribadi digunakan tanpa izin atau disebarluaskan kepada pihak ketiga. Oleh karena itu, *gap* penelitian yang ada adalah kurangnya kajian yang secara spesifik mengkaji tanggung jawab hukum penyelenggara pinjol dan *debt collector* dalam penyalahgunaan data pribadi.

Selain itu, dalam praktiknya ditemukan adanya penyebaran data pribadi debitur yang menyebabkan kerugian hukum, baik dalam bentuk tekanan sosial maupun pelanggaran privasi. Tindakan ini bahkan dapat berujung pada konsekuensi hukum berupa tanggung jawab pidana dan administratif bagi pelaku. Penyalahgunaan data pribadi dalam layanan pinjaman online juga sering digunakan sebagai alat intimidasi, termasuk dengan melibatkan pihak keluarga atau lingkungan sosial debitur. Hal ini menunjukkan bahwa pemrosesan data pribadi tidak hanya melampaui tujuan awal, tetapi juga berpotensi melanggar hak privasi individu secara lebih luas. Dampak sosial dan psikologis yang ditimbulkan, seperti rasa malu, tekanan mental, dan terganggunya kehidupan sosial, merupakan konsekuensi nyata dari lemahnya mekanisme perlindungan data dalam ekosistem pinjaman online.

Sebagai contoh konkret yang dapat dijadikan ilustrasi empiris, kondisi keterbatasan regulasi tersebut tidak hanya terjadi pada layanan pinjaman online ilegal, melainkan juga terdokumentasi pada penyelenggara resmi yang telah terdaftar dan diawasi oleh Otoritas Jasa Keuangan. Salah satu contoh yang dapat dijadikan ilustrasi adalah praktik penagihan yang dilakukan oleh *debt collector ShopeePay Later*, yang diselenggarakan oleh PT Commerce Finance selaku lembaga pembiayaan resmi di bawah pengawasan Otoritas Jasa Keuangan. Berdasarkan pengaduan konsumen yang terdokumentasi, pihak penagih *ShopeePay Later* menghubungi sejumlah nomor telepon yang tidak terdaftar sebagai kontak darurat pengguna, melainkan kontak-kontak lain yang tersimpan di perangkat pengguna tanpa persetujuan yang sah dari pemilik data maupun dari pihak yang dihubungi tersebut.

Pelanggaran privasi dalam praktik penagihan pinjaman online semakin menunjukkan perkembangan yang mengkhawatirkan. Salah satu contoh kasus yang diberitakan oleh kanal resmi seperti IDN Times mengungkap adanya praktik penagihan

yang dilakukan dengan cara menghubungi seluruh kontak yang ada di perangkat nasabah. Kontak ini meliputi keluarga, teman, hingga rekan kerja, yang sebenarnya tidak memiliki hubungan hukum dengan perjanjian pinjaman nasabah. Selain itu, dalam beberapa kasus, pihak penagih juga diketahui menggunakan aplikasi pesan instan untuk membuat grup komunikasi yang melibatkan sejumlah kontak nasabah dengan tujuan memberikan tekanan sosial agar nasabah segera memenuhi kewajiban pembayaran. Fakta bahwa pelanggaran serupa terjadi pada penyelenggara yang beroperasi secara legal semakin menegaskan bahwa permasalahan ini bukan semata-mata soal kepatuhan pelaku usaha, melainkan lebih mendasar pada ketidaklengkapan rumusan Pasal 21 Undang-Undang Perlindungan Data Pribadi.

Bertolak dari uraian latar belakang di atas, penelitian ini berupaya memberikan kontribusi akademik berupa rekonstruksi argumen dari perspektif "ketiadaan norma" menuju "keterbatasan arsitektur norma" sebagai kerangka analitis yang lebih akurat dalam menggambarkan persoalan perlindungan data pribadi dalam konteks pinjaman online di Indonesia. Hal ini menunjukkan bahwa penyalahgunaan data pribadi dalam pinjaman online merupakan masalah yang nyata dan terjadi secara luas di masyarakat. Meskipun sudah ada berbagai regulasi yang mengatur, pelanggaran tetap sering terjadi. Ini mencerminkan adanya kesenjangan antara norma hukum yang ada dan implementasinya di lapangan, yang disebabkan oleh lemahnya pengawasan, penegakan hukum yang kurang efektif, serta rendahnya kesadaran masyarakat.

Berdasarkan latar belakang diatas, dalam penelitian ini terdapat rumusan masalah yang muncul yakni, Bagaimana pengaturan tujuan pemrosesan data pribadi dalam pasal 21 Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi terhadap penggunaan data pribadi pada layanan pinjam online, dan Bagaimana keterbatasan pengaturan tujuan pemrosesan data pribadi dalam pasal 21 undang-undang

Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi berimplikasi terhadap pertanggungjawaban hukum atas penyalahgunaan data pribadi dalam praktik pinjaman online.

Berdasarkan penelitian terdahulu yakni pertama Nur Alfiana Alfitri (2025) dnegan judul Perlindungan terrhadap data pribadi di era digital berdasarkan UU No. 27 Tahun 2022 tentang perlindngan data pribadi, yang ke dua Muhamad Adri Rinjani dan Ricky Firmansayh (2025) dengan judul Hambatan Implementasi UU No. 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia, dan yang terakhir Dewi Wahyu Aprilia (2024) Perlindungan Hukum Data Konsumen yang Disebarkan Pinjaman Online. Berbagai penelitian terdahulu umumnya membahas perlindungan data pribadi dari aspek implementasi Undang-Undang Perlindungan Data Pribadi, perlindungan hukum terhadap korban penyalahgunaan data, atau efektivitas pengawasan dalam layanan pinjaman online. Namun, masih terbatas penelitian yang secara khusus mengkaji keterbatasan pengaturan tujuan pemrosesan data pribadi dalam Pasal 21 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi serta keterkaitannya dengan Pasal 27, Pasal 28, dan Pasal 51 dalam menentukan pertanggungjawaban hukum atas penyalahgunaan data pribadi. Oleh karena itu, penelitian ini menawarkan kebaruan melalui analisis terhadap keterbatasan arsitektur norma Pasal 21 beserta implikasinya terhadap pertanggungjawaban hukum dalam praktik penagihan pinjaman online

B. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif, dengan pendekatan penelitian yang digunakan yakni, pendekatan perundang-undangan (*statute approach),* pendekatan perbandingan *comparative approach),* pendekatan konseptual (*conceptual approach),* serta pendekatan kasus (*case approach).* Jenis dan sumber bahan hukum

yang digunakan yakni Bahan hukum primer ada Undang-undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, khususnya Pasal 21, yang mengatur kewajiban pengendali data untuk memberikan pemberitahuan kepada subjek data sebelum data pribadi mereka diproses, GDPR atau *General Data Protection Regulation* tentang Perlindungan Data Umum, dan peraturan lainnya yang terkait dengan keamanan data pribadi dna haka subjek data dalam konteks penagihan pinjaman online. Bahan hukum sekunder yang digunakan yakni buku yang terkait, jurnal yang menguraikan prinsip dasar dalam perlindungan data pribadi, termasuk transparansi dalam pengolahan data dan hak subjek data, dan doktrin hukum mengenai pemrosesan data pribadi dalam sektor pinjaman online, serta penerapan pasal 21 UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam regulasi perbankan atau fintech. Bahan hukum tersier yang digunakan yakni Kamus hukum, serta referensi daring untuk mendalami lebih dalam tentang pemrosesan data pribadi, dan juga peraturan internasional yang relevan, seperti GDPR yang juga mengatur kewajiban pemberitahuan. Penelitian dalam pengumpuan bahan hukum dengan melalui studi Pustaka (library research), yaitu melalui penelusuran dan analisis literatur yang berkaitan dengan Pasal 21 Undang-Undang Perlindungan Data Pribadi dan praktik penagihan pinjaman online. Penulis akan menelaah berbagai referensi, hasil penelitian terdahulu, jurnal ilmiah, dan dokumen perundang-undangan terkait. Selain itu, pendekatan komparatif digunakan untuk menginventarisasi peraturan perundang-undangan dan instrumen hukum internasional yang terkait dengan perlindungan data pribadi pada sektor keuangan. Penelitian ini dalam analisis bahan hukum dengan menggunakan metode penelitian hukum normatif, dengan sifat analisis preskriptif yang bertujuan untuk menghasilkan argumentasi hukum terkait dengan keterbatasan Pasal 21 dalam mengatasi masalah penyalahgunaan data pribadi dalam praktik penagihan pinjaman. Setelah studi pustaka,

penulis akan melakukan analisis mendalam mengenai efektivitas Pasal 21 dalam menangani pelanggaran privasi, serta mengidentifikasi tantangan yang ada.

C. HASIL DAN PEMBAHASAN

1. Peraturan Pasal 21 UU PDP terhadap Penggunaan data pribadi dalam layanan pinjaman online

   Perlindungan data pribadi merupakan respons hukum atas meningkatnya intensitas pengumpulan, pengolahan, dan distribusi data pribadi di era digital, yang dalam sektor keuangan berbasis teknologi telah mencapai skala yang sangat masif. Penyelenggara layanan pinjaman online merupakan salah satu pihak yang paling intensif dalam memproses data pribadi penggunanya, mulai dari tahap registrasi akun, verifikasi identitas, analisis kelayakan kredit, pencairan dana, hingga proses penagihan. Dalam setiap tahapan tersebut, penyelenggara memproses berbagai jenis data pribadi yang memiliki nilai ekonomi dan sosial yang tinggi, sehingga potensi penyalahgunaannya pun sangat besar apabila tidak disertai mekanisme perlindungan yang memadai.

   Sebelum menganalisis pengaturan tujuan pemrosesan data pribadi, perlu terlebih dahulu ditetapkan kedudukan hukum masing-masing pihak yang terlibat dalam proses layanan pinjaman online, karena kedudukan tersebut menentukan jenis kewajiban dan tanggung jawab yang berlaku. UU PDP membedakan tiga kedudukan utama: subjek data pribadi, pengendali data pribadi, dan prosesor data pribadi.

   Pengguna layanan pinjaman online berkedudukan sebagai *subjek data pribadi*, yaitu orang perseorangan yang pada dirinya melekat data pribadi yang menjadi objek pemrosesan. Dalam kedudukan tersebut, pengguna memiliki sejumlah hak yang dilindungi oleh UU PDP, antara lain hak untuk mengetahui informasi

mengenai kejelasan identitas pengendali, dasar kepentingan hukum pemrosesan, tujuan permintaan dan penggunaan data, serta hak untuk mengakhiri persetujuan pemrosesan data pribadi kapan saja sesuai Pasal 5 UU PDP. Hak-hak tersebut menempatkan subjek data bukan sekadar sebagai objek pasif, melainkan sebagai subjek aktif yang memiliki kendali atas data pribadinya sendiri, sejalan dengan konsep *informational self-determination* yang berkembang dalam doktrin perlindungan data modern.

Penyelenggara layanan pinjaman online berkedudukan sebagai *pengendali data pribadi* (*data controller*). Berdasarkan Pasal 1 angka 4 UU PDP, pengendali data pribadi adalah setiap orang, badan publik, dan organisasi internasional yang bertindak sendiri-sendiri atau bersama-sama dalam menentukan tujuan dan melakukan kendali pemrosesan data pribadi. Kedudukan pengendali data pribadi ini menempatkan penyelenggara pinjaman online pada posisi yang paling sentral dalam ekosistem perlindungan data, karena merekalah yang menentukan mengapa, bagaimana, dan untuk apa data dikumpulkan dan diproses. Konsekuensinya, kewajiban hukum yang paling berat dalam UU PDP dibebankan kepada pengendali data.

Adapun *debt collector* atau pihak ketiga yang ditugaskan oleh penyelenggara untuk melaksanakan kegiatan penagihan berkedudukan sebagai *prosesor data pribadi* (*data processor*). Berdasarkan Pasal 1 angka 5 UU PDP, prosesor data pribadi adalah setiap orang, badan publik, atau organisasi internasional yang memproses data pribadi atas nama pengendali data pribadi. Perbedaan mendasar antara pengendali dan prosesor terletak pada otoritas penentuan tujuan: pengendali menentukan tujuan pemrosesan, sedangkan prosesor hanya melaksanakan pemrosesan berdasarkan perintah dan dalam batas yang ditetapkan oleh pengendali.

Prosesor tidak memiliki kewenangan untuk menetapkan tujuan pemrosesan secara mandiri.

Relasi hukum antara pengendali dan prosesor ini diatur dalam Pasal 51 UU PDP. Berdasarkan Pasal 51 ayat (1), prosesor data pribadi wajib melakukan pemrosesan data pribadi berdasarkan perintah pengendali data pribadi. Pasal 51 ayat (3) menegaskan bahwa pemrosesan yang dilakukan oleh prosesor termasuk dalam tanggung jawab pengendali data pribadi. Dengan demikian, penggunaan *debt collector* oleh penyelenggara pinjaman online tidak menghilangkan tanggung jawab penyelenggara selaku pengendali data atas penggunaan data yang dilakukan oleh *debt collector* tersebut.Namun demikian, terdapat satu ketentuan penting yang berkaitan dengan penentuan batas tanggung jawab. Pasal 51 ayat (6) UU PDP mengatur bahwa apabila prosesor data pribadi melakukan pemrosesan data di luar perintah dan tujuan yang ditetapkan oleh pengendali, maka pemrosesan tersebut menjadi tanggung jawab prosesor data pribadi sendiri. Ketentuan ini mengandung ambivalensi yang penting untuk dicermati: di satu sisi ia melindungi pengendali data dari tanggung jawab atas tindakan prosesor yang menyimpang; namun di sisi lain, ketentuan ini membuka potensi *moral hazard* di mana pengendali data dapat berargumen bahwa tindakan *debt collector* yang melanggar privasi pengguna adalah tindakan yang dilakukan di luar perintah, sehingga tanggung jawab seluruhnya beralih ke *debt collector*. Persoalan ini akan dianalisis lebih lanjut dalam sub-bab 4.2.2.

UU PDP membedakan data pribadi menjadi dua kategori utama berdasarkan tingkat sensitivitasnya. Berdasarkan Pasal 4 UU PDP, data pribadi yang bersifat spesifik meliputi data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi, dan data lainnya sesuai

ketentuan peraturan perundang-undangan. Sementara itu, data pribadi yang bersifat umum meliputi nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan kombinasi data yang dapat mengidentifikasi seseorang. Dalam praktik layanan pinjaman online, penyelenggara mengumpulkan kedua jenis data tersebut secara bersamaan. Data umum yang dikumpulkan mencakup nama lengkap, nomor identitas (KTP/SIM), nomor telepon, alamat, dan informasi pekerjaan. Data spesifik yang dikumpulkan mencakup data keuangan pribadi seperti rekening bank, riwayat transaksi, dan jumlah pendapatan. Selain itu, banyak penyelenggara pinjaman online yang mensyaratkan akses terhadap data-data yang bersifat lebih sensitif dari perspektif privasi, seperti daftar kontak pada perangkat pengguna, data lokasi, dan akses terhadap galeri foto. Pengumpulan data ini melampaui kebutuhan verifikasi identitas dan analisis kredit yang merupakan tujuan awal yang dinyatakan, sehingga mengindikasikan adanya ketidaksesuaian dengan prinsip minimalisasi data (*data minimization*) sejak tahap pengumpulan.

Pengumpulan data kontak pada perangkat pengguna merupakan kategori data yang paling relevan dengan permasalahan yang dikaji dalam penelitian ini. Data kontak bukan merupakan data pribadi pengguna semata, melainkan juga merupakan data pribadi pihak-pihak lain yang nomor teleponnya tersimpan dalam perangkat pengguna. Pengumpulan dan penggunaan data tersebut oleh penyelenggara pinjaman online untuk kepentingan penagihan kepada pihak yang bersangkutan menimbulkan persoalan hukum ganda: pertama, pelanggaran terhadap tujuan pemrosesan yang dinyatakan kepada pengguna sebagai subjek data; dan kedua, pemrosesan data pribadi pihak ketiga tanpa persetujuan dari pihak tersebut.

Undang-Undang Perlindungan Data Pribadi pada dasarnya tidak hanya mengatur bagaimana pemrosesan data harus dilakukan sejak awal, melainkan juga

menentukan batas-batas penggunaan data pribadi sepanjang siklus pemrosesannya. Pemrosesan data pribadi tidak dapat dilakukan secara bebas oleh pengendali data pribadi tanpa memperhatikan landasan tujuan yang sah dan telah dikomunikasikan kepada subjek data. Dalam kerangka ini, Pasal 21 UU PDP memainkan peran yang sangat sentral. Pasal 21 ayat (1) UU PDP mewajibkan pengendali data pribadi untuk menyampaikan tujuh informasi kepada subjek data pribadi sebelum pemrosesan dilakukan, meliputi: legalitas dari pemrosesan data pribadi, tujuan pemrosesan data pribadi, jenis dan relevansi data pribadi yang akan diproses, jangka waktu retensi dokumen yang memuat data pribadi, rincian mengenai informasi yang dikumpulkan, jangka waktu pemrosesan data pribadi, dan hak subjek data pribadi.

Pengendali data pribadi berkewajiban memberikan seluruh informasi tersebut kepada subjek data pribadi sebagai bentuk perlindungan terhadap hak privasi dan hak atas informasi. Di antara ketujuh kewajiban informasi tersebut, kewajiban menyampaikan tujuan pemrosesan data pribadi merupakan elemen yang paling menentukan dalam konteks penelitian ini. Hal ini dikarenakan tujuan pemrosesan itulah yang kemudian berfungsi sebagai batas hukum penggunaan data dalam seluruh rangkaian pemrosesan berikutnya. Kewajiban ini menunjukkan bahwa penggunaan data pribadi harus didasarkan pada tujuan yang jelas dan harus diketahui oleh subjek data pribadi sejak awal.

Tujuan pemrosesan data pribadi dapat dipahami sebagai alasan atau kepentingan tertentu yang menjadi dasar dilakukannya pengumpulan, penyimpanan, penggunaan, pengungkapan, maupun penghapusan data pribadi. Keberadaan tujuan pemrosesan data pribadi memiliki fungsi sebagai batas hukum yang menentukan ruang lingkup penggunaan data pribadi oleh pengendali data pribadi. Tujuan pemrosesan data pribadi juga berkaitan erat dengan prinsip *purpose limitation*, yaitu

prinsip yang menghendaki agar data pribadi digunakan secara terbatas sesuai dengan tujuan yang telah ditentukan sebelumnya. Oleh karena itu, data pribadi pada prinsipnya hanya boleh digunakan untuk tujuan yang telah ditetapkan dan diberitahukan kepada subjek data pribadi saat pemrosesan dilakukan. Transparansi mengenai tujuan pemrosesan data memiliki fungsi penting untuk mencegah penggunaan data pribadi secara sewenang-wenang oleh pihak yang mengendalikan data tersebut. Kejelasan tujuan pemrosesan data pribadi memungkinkan pengguna mengetahui ruang lingkup batas-batas penggunaan data pribadi yang mereka berikan kepada penyelenggara layanan. Sebaliknya, apabila tujuan pemrosesan dirumuskan secara terlalu umum atau tidak memberikan batas yang jelas terhadap penggunaan data pribadi, maka potensi terjadinya penyalahgunaan data pribadi akan semakin besar. Penggunaan data di luar tujuan yang dinyatakan merupakan pelanggaran privasi dalam kategori *information use* sebagaimana dikategorikan dalam taksonomi privasi Solove, yang berbeda dari kategori *information collection* dan *information dissemination*. Perbedaan kategorisasi ini penting karena masing-masing kategori memerlukan mekanisme perlindungan yang berbeda.

Pemahaman yang tepat terhadap peran Pasal 21 dalam UU PDP mensyaratkan pembacaan yang sistemik, bukan parsial. Dalam ekosistem UU PDP, terdapat setidaknya enam pasal yang secara langsung membentuk kerangka normatif perlindungan tujuan pemrosesan data, yaitu Pasal 16, Pasal 20, Pasal 21, Pasal 22, Pasal 27, dan Pasal 28. Keenam pasal ini beroperasi pada tahapan yang berbeda dalam siklus pemrosesan data, namun semuanya bermuara pada satu prinsip dasar yang sama: bahwa data pribadi hanya boleh diproses untuk tujuan yang sah, jelas, dan sesuai dengan apa yang telah disepakati bersama subjek data. Pertama, Pasal 16 ayat (2) UU PDP menetapkan bahwa pengumpulan data pribadi dilakukan secara

terbatas dan spesifik, sah secara hukum, dan transparan. Ketentuan ini menempatkan standar spesifisitas sejak tahap pengumpulan, sebelum data bahkan diproses lebih lanjut. Artinya, penyelenggara layanan tidak hanya wajib menyampaikan tujuan pemrosesan kepada pengguna, tetapi juga wajib membatasi pengumpulan data hanya pada data yang relevan dan diperlukan untuk tujuan yang dinyatakan tersebut.

Kedua, Pasal 20 UU PDP mengatur dasar-dasar legalitas pemrosesan data pribadi. Pemrosesan data pribadi harus didasarkan pada salah satu dari enam dasar yang diakui, yaitu: (a) persetujuan yang eksplisit dari subjek data; (b) pelaksanaan perjanjian; (c) pemenuhan kewajiban hukum; (d) perlindungan kepentingan vital subjek data; (e) pelaksanaan tugas dalam kepentingan umum; atau (f) kepentingan yang sah dari pengendali data. Dalam konteks pinjaman online, dasar legalitas yang paling umum digunakan adalah persetujuan (huruf a) dan pelaksanaan perjanjian (huruf b). Relevansinya terhadap isu tujuan pemrosesan adalah bahwa masing-masing dasar legalitas ini memiliki implikasi yang berbeda terhadap ruang lingkup penggunaan data yang diizinkan.

Ketiga, Pasal 21 ayat (1) UU PDP mewajibkan pengendali data untuk menyampaikan tujuh informasi kepada subjek data sebelum pemrosesan dilakukan: (a) legalitas dari pemrosesan data pribadi; (b) tujuan pemrosesan data pribadi; (c) jenis dan relevansi data pribadi yang akan diproses; (d) jangka waktu retensi dokumen yang memuat data pribadi; (e) rincian mengenai informasi yang dikumpulkan; (f) jangka waktu pemrosesan data pribadi; dan (g) hak subjek data pribadi. Dari ketujuh informasi tersebut, kewajiban menyampaikan tujuan pemrosesan (huruf b) merupakan elemen yang paling menentukan dalam konteks

penelitian ini, karena tujuan pemrosesan itulah yang nantinya berfungsi sebagai batas hukum penggunaan data dalam seluruh rangkaian pemrosesan berikutnya.

Keempat, Pasal 22 ayat (4) UU PDP mengatur bahwa apabila persetujuan memuat tujuan lain selain tujuan utama, permintaan persetujuan harus memenuhi tiga syarat: (a) dapat dibedakan secara jelas dengan hal lainnya; (b) dibuat dengan format yang dapat dipahami dan mudah diakses; dan (c) menggunakan bahasa yang sederhana dan jelas. Pasal 22 ayat (5) mempertegas bahwa persetujuan yang tidak memenuhi syarat tersebut dinyatakan batal demi hukum. Ketentuan ini sangat relevan dengan praktik penyelenggara pinjaman online yang lazimnya menggabungkan berbagai tujuan pemrosesan data dalam satu klausul syarat dan ketentuan yang panjang, tanpa memberikan kesempatan kepada pengguna untuk menyetujui sebagian tujuan dan menolak tujuan lainnya secara terpisah.

Kelima, Pasal 27 UU PDP secara tegas mewajibkan pengendali data untuk melakukan pemrosesan data secara terbatas dan spesifik, sah secara hukum, dan transparan. Pasal ini merupakan norma *purpose specification* dalam UU PDP: ia tidak sekadar mewajibkan pemberitahuan tujuan, tetapi mensyaratkan bahwa tujuan yang ditetapkan harus memiliki kualitas tertentu, yaitu terbatas dan spesifik. Kewajiban "spesifik" ini berarti bahwa tujuan pemrosesan tidak dapat dirumuskan secara umum atau kabur, melainkan harus menggambarkan secara konkret untuk kepentingan apa data akan digunakan.

Keenam dan yang paling krusial, Pasal 28 UU PDP mewajibkan pengendali data untuk melakukan pemrosesan data sesuai dengan tujuan pemrosesan data pribadi yang telah ditetapkan. Pasal 28 merupakan norma *purpose limitation* yang paling eksplisit dalam UU PDP: ia secara implisit melarang penggunaan data di luar tujuan yang telah ditetapkan dan disampaikan kepada subjek data. Dengan

demikian, Pasal 28 sejatinya telah memberikan dasar normatif yang cukup kuat untuk menyatakan bahwa penggunaan data kontak pengguna untuk menghubungi pihak ketiga dalam proses penagihan, yang jelas melampaui tujuan awal verifikasi identitas dan analisis kredit yang merupakan pelanggaran hukum.

Pemetaan terhadap keenam pasal tersebut menghasilkan suatu gambaran yang penting: prinsip *purpose limitation* dalam UU PDP bukan tidak ada, melainkan sudah ada dalam Pasal 27 dan Pasal 28. Ini merupakan koreksi mendasar terhadap argumen yang selama ini beredar dalam beberapa penelitian terdahulu yang menyatakan bahwa UU PDP tidak mengatur *purpose limitation* secara memadai. Argumen tersebut tidak tepat secara normatif. Yang sesungguhnya terjadi adalah bahwa Pasal 21 sebagai ketentuan operasional yang paling langsung bersentuhan dengan hubungan pengendali-subjek data tidak secara eksplisit mengintegrasikan kewajiban Pasal 27 dan Pasal 28 ke dalam mekanisme pemberitahuan. Ketidakintegrasian inilah yang menciptakan celah arsitektur norma. Dalam konteks ekosistem norma yang telah dipetakan, Pasal 21 UU PDP berkedudukan sebagai ketentuan operasional yang paling langsung mengatur hubungan informasional antara pengendali data dan subjek data sebelum pemrosesan dimulai. Fungsi Pasal 21 dapat dianalogikan sebagai *front gate*: ia merupakan gerbang pertama yang harus dilalui oleh pengendali data sebelum dapat memproses data pribadi pengguna secara sah. Dalam doktrin perlindungan data, kewajiban pemberitahuan pra-pemrosesan (*pre-processing notification obligation*) seperti yang diatur dalam Pasal 21 merupakan salah satu instrumen perlindungan yang paling fundamental. Menurut Daniel J. Solove, perlindungan privasi di era informasi tidak dapat direduksi hanya pada pencegahan akses tidak sah terhadap data, melainkan harus mencakup juga pengaturan mengenai bagaimana data digunakan setelah diperoleh

secara sah. Dalam kerangka taksonomi privasi yang dikembangkan Solove, penggunaan data di luar tujuan yang dinyatakan merupakan pelanggaran privasi dalam kategori *information use*, yang berbeda dari *information collection* dan *information dissemination*. Perbedaan kategorisasi ini penting karena masing-masing kategori memerlukan mekanisme perlindungan yang berbeda pula.

Pasal 21 ayat (2) UU PDP juga mengatur kewajiban pengendali data untuk memberitahukan perubahan informasi kepada subjek data sebelum perubahan tersebut terjadi. Kewajiban ini relevan dalam konteks layanan pinjaman online karena berimplikasi bahwa apabila penyelenggara ingin mengubah atau memperluas tujuan pemrosesan data — misalnya dari sekadar verifikasi kredit menjadi juga penagihan melalui kontak pengguna — penyelenggara wajib terlebih dahulu memberitahukan perubahan tersebut dan memperoleh persetujuan ulang dari pengguna. Dalam praktiknya, kewajiban ini hampir tidak pernah dipatuhi oleh penyelenggara pinjaman online. Secara konseptual, keterbatasan utama Pasal 21 bukan terletak pada apa yang diaturnya, melainkan pada apa yang tidak diaturnya secara tegas dan pada kegagalannya untuk menghubungkan diri dengan pasal-pasal lain yang relevan. Pasal 21 mewajibkan pemberitahuan tujuan, tetapi tidak mensyaratkan bahwa tujuan tersebut harus memenuhi standar spesifisitas yang ditetapkan Pasal 27. Pasal 21 mewajibkan pemberitahuan, tetapi tidak menyediakan mekanisme verifikasi bahwa penggunaan data selanjutnya tetap berada dalam batas tujuan yang diberitahukan sebagaimana diwajibkan Pasal 28. Pasal 21 mengatur hubungan pengendali-subjek data, tetapi tidak mengatur bagaimana tujuan yang diberitahukan tersebut mengikat pihak ketiga yang terlibat dalam penagihan sebagaimana dimaksud Pasal 37.

Inilah yang dimaksud dengan keterbatasan arsitektur norma: Pasal 21 beroperasi sebagai pulau yang terpisah dalam ekosistem norma UU PDP, tanpa jembatan yang secara eksplisit menghubungkannya dengan Pasal 27, 28, dan 37. Akibatnya, kepatuhan formal terhadap Pasal 21 — dengan sekadar mencantumkan tujuan pemrosesan dalam klausul syarat dan ketentuan — tidak secara otomatis menjamin kepatuhan substantif terhadap Pasal 28, yang mewajibkan penggunaan data sesuai dengan tujuan tersebut. Di sinilah celah hukum yang dimanfaatkan oleh penyelenggara pinjaman online terbuka.

Penerapan Pasal 21 UU PDP dalam kegiatan penagihan pinjaman online memiliki implikasi yang sangat konkret. Kegiatan penagihan pada dasarnya merupakan bagian dari pelaksanaan perjanjian pinjaman antara penyelenggara layanan pinjaman online dengan pengguna. Oleh karena itu, penggunaan data pribadi untuk menghubungi debitur dalam rangka penagihan dapat dilakukan sepanjang penggunaan tersebut masih sesuai dengan tujuan pemrosesan data pribadi yang telah diberitahukan kepada pengguna sebelumnya. Penerapan Pasal 21 UU PDP dalam kegiatan penagihan tidak hanya menuntut adanya pemberitahuan mengenai tujuan pemrosesan data pribadi, tetapi juga menuntut agar penggunaan data pribadi tetap berada dalam batas tujuan yang telah ditetapkan tersebut.

Kejelasan tujuan ini menjadi penting karena memberikan kepastian mengenai ruang lingkup penggunaan data pribadi oleh penyelenggara layanan pinjaman online. Dengan adanya tujuan yang jelas, pengguna dapat mengetahui sejauh mana dan untuk kepentingan apa data pribadinya digunakan serta dapat menilai apakah penggunaan data tersebut tetap sesuai dengan koridor tujuan awal pemrosesan data. Selain sebagai pemenuhan kewajiban pengendali data pribadi, kejelasan tujuan pemrosesan data pribadi juga berkaitan langsung dengan perlindungan privasi

pengguna. Penyalahgunaan data pribadi berpotensi menimbulkan gangguan terhadap privasi individu karena membuka kemungkinan penggunaan data untuk kepentingan lain yang tidak diketahui atau diharapkan oleh pemilik data.

Pasal 21 ayat (2) UU PDP juga mengatur kewajiban pengendali data untuk memberitahukan perubahan informasi kepada subjek data sebelum perubahan tersebut terjadi. Dalam konteks layanan pinjaman online, hal ini berarti bahwa apabila penyelenggara ingin mengubah atau memperluas tujuan pemrosesan data, misalnya dari sekadar verifikasi kredit menjadi juga penagihan melalui kontak pengguna, penyelenggara wajib terlebih dahulu memberitahukan perubahan tersebut dan memperoleh persetujuan ulang dari pengguna. Siklus pemrosesan data dalam layanan pinjaman online mencakup setidaknya lima tahap yang berbeda: registrasi, verifikasi identitas, analisis kelayakan kredit, pencairan dana, dan penagihan. Pada setiap tahap, terjadi pemrosesan data dengan intensitas dan jenis yang berbeda. Pasal 21 UU PDP, dengan kewajiban pemberitahuan tujuan yang dipersyaratkannya, idealnya harus mampu mencakup dan membatasi penggunaan data di seluruh tahapan tersebut. Pada tahap registrasi, pengguna memberikan data identitas dasar dan menyetujui syarat dan ketentuan layanan. Di sinilah kewajiban Pasal 21 pertama kali berlaku: penyelenggara wajib menyampaikan tujuan pemrosesan data secara jelas sebelum pengguna memberikan persetujuannya. Namun dalam praktiknya, tujuan pemrosesan yang dicantumkan dalam klausul persetujuan sering kali dirumuskan secara sangat luas, seperti "untuk keperluan layanan keuangan kami" atau "untuk memenuhi kewajiban hukum dan peraturan yang berlaku." Rumusan demikian secara formal memenuhi kewajiban Pasal 21 karena tujuan disebutkan, namun secara substantif tidak memenuhi standar Pasal 27 karena tujuan tidak dirumuskan secara terbatas dan spesifik. Pada tahap verifikasi

identitas, penyelenggara memproses data identitas yang telah diberikan untuk memastikan keaslian identitas pengguna. Pada tahap ini, penggunaan data masih relatif sesuai dengan tujuan yang dinyatakan. Persoalan mulai muncul pada tahap analisis kelayakan kredit, di mana beberapa penyelenggara mengakses data yang melampaui kebutuhan analisis kredit yang sebenarnya, termasuk data kontak, data lokasi, dan akses perangkat.

Persoalan paling serius terjadi pada tahap penagihan. Pada tahap ini, data kontak yang semula dikumpulkan dalam rangka registrasi dan verifikasi digunakan untuk tujuan yang berbeda, yaitu menghubungi pihak-pihak yang nomor teleponnya tersimpan dalam perangkat pengguna. Penggunaan data untuk tujuan ini jelas melampaui tujuan awal pemrosesan, dan oleh karena itu bertentangan dengan kewajiban Pasal 28 UU PDP yang mewajibkan pemrosesan sesuai tujuan. Namun karena Pasal 21 tidak mengintegrasikan secara eksplisit kewajiban Pasal 28 ke dalam mekanisme pemberitahuan, penyelenggara dapat berargumen bahwa klausul tujuan yang luas dalam syarat dan ketentuan mereka mencakup juga penggunaan data kontak untuk penagihan.

Kondisi ini menggambarkan dengan jelas mengapa celah arsitektur norma dalam Pasal 21 bukan persoalan yang bersifat teoritis semata, melainkan memiliki konsekuensi hukum yang nyata dalam kehidupan pengguna layanan pinjaman online. Tanpa mekanisme yang secara eksplisit menghubungkan kewajiban pemberitahuan Pasal 21 dengan standar spesifisitas Pasal 27 dan larangan penggunaan di luar tujuan dalam Pasal 28, prinsip *purpose limitation* yang secara normatif sudah ada dalam UU PDP tidak dapat berfungsi secara efektif sebagai pelindung privasi pengguna dalam praktik penagihan.

2. Keterbatasan pengaturan Pasal 21 UU PDP dan Implikasinya terhadap Pertanggungjawaban Hukum atas Penyalahgunaan Data Pribadi dalam Praktik Pinjaman Online

Berdasarkan pemetaan ekosistem norma yang telah dilakukan dalam sub-bab 4.1, penelitian ini mengidentifikasi empat keterbatasan arsitektur norma Pasal 21 UU PDP yang saling berkaitan secara kausal dan bersama-sama membentuk celah implementasi yang signifikan. Keempat keterbatasan ini tidak berdiri sendiri-sendiri, melainkan membentuk sebuah rantai: keterbatasan pertama memungkinkan terjadinya keterbatasan kedua, yang kemudian diperparah oleh keterbatasan ketiga, dan seluruhnya dibiarkan tanpa jangkar sanksi yang spesifik karena keterbatasan keempat. Pemahaman terhadap kausalitas ini penting agar solusi yang ditawarkan dalam saran penelitian dapat bersifat sistemik, bukan parsial.

Pertama, Tidak Ada Pengintegrasian Eksplisit antara Kewajiban Pemberitahuan Tujuan (Pasal 21) dan Kewajiban Spesifisitas Tujuan (Pasal 27). Keterbatasan pertama dan yang paling mendasar dari arsitektur norma Pasal 21 UU PDP adalah ketiadaan pengintegrasian eksplisit antara kewajiban pemberitahuan tujuan yang diatur dalam Pasal 21 dengan kewajiban spesifisitas tujuan yang diatur dalam Pasal 27. Kedua pasal ini beroperasi secara paralel tanpa saling merujuk, sehingga menciptakan situasi di mana pengendali data dapat memenuhi kewajiban Pasal 21 secara formal tanpa harus memenuhi standar substantif Pasal 27. Untuk memahami keterbatasan ini secara lebih mendalam, perlu terlebih dahulu dipahami perbedaan antara *purpose notification* dan *purpose specification* dalam doktrin perlindungan data. *Purpose notification* adalah kewajiban untuk memberitahukan tujuan pemrosesan kepada subjek data. Hal ini yang diatur Pasal 21. *Purpose specification* adalah kewajiban untuk merumuskan tujuan tersebut secara spesifik,

eksplisit, dan konkret. Hal ini yang diatur Pasal 27. Dalam sistem perlindungan data yang efektif, keduanya harus berjalan bersamaan: pemberitahuan tujuan yang tidak spesifik tidak memiliki nilai perlindungan karena subjek data tidak dapat memahami secara nyata apa yang akan dilakukan dengan datanya. Sebaliknya, spesifisitas tujuan yang tidak diberitahukan kepada subjek data pun tidak bermanfaat karena tidak memberikan kesempatan bagi subjek data untuk memberikan persetujuan yang sungguh-sungguh berdasarkan informasi yang memadai (*informed consent*).

General Data Protection Regulation (GDPR) Uni Eropa menunjukkan bagaimana kedua kewajiban ini dapat diintegrasikan secara efektif. Pasal 5 ayat (1) huruf b GDPR menetapkan dalam satu ketentuan yang terintegrasi bahwa data pribadi harus dikumpulkan untuk tujuan yang spesifik, eksplisit, dan sah, serta tidak boleh diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut. Artinya, dalam GDPR, kewajiban spesifisitas tujuan dan larangan penggunaan di luar tujuan tergabung dalam satu pasal yang sama. Pengendali data tidak dapat memenuhi Pasal 5 GDPR hanya dengan menyebutkan tujuan secara umum — tujuan tersebut harus spesifik, eksplisit, dan sah sekaligus. Standar demikian tidak terdapat dalam satu pasal yang terintegrasi dalam UU PDP.

Dalam konteks perbandingan yang lebih luas, Pasal 18 ayat (1) huruf b Personal Data Protection Act (PDPA) Thailand 2019 juga mengatur bahwa pengendali data wajib memberitahukan tujuan pemrosesan dengan cara yang jelas dan dapat dipahami sebelum atau pada saat pengumpulan data, dengan spesifikasi yang cukup agar subjek data dapat memahami jenis pemrosesan yang akan dilakukan. Standar "spesifikasi yang cukup" ini secara inheren menghubungkan

kewajiban pemberitahuan dengan standar kualitas tujuan yang diberitahukan — suatu hubungan yang tidak secara eksplisit ada dalam Pasal 21 UU PDP.

Perwujudan nyata dari keterbatasan pertama ini dapat ditemukan dalam praktik layanan *ShopeePay Later* yang diselenggarakan oleh PT Commerce Finance. Klausul persetujuan dalam aplikasi *ShopeePay Later* mencantumkan berbagai tujuan penggunaan data dalam satu paket persetujuan yang komprehensif. Pengguna dihadapkan pada pilihan biner: menyetujui seluruh tujuan pemrosesan yang tercantum atau tidak dapat menggunakan layanan sama sekali. Tidak tersedia mekanisme bagi pengguna untuk menyetujui sebagian tujuan — misalnya menyetujui penggunaan data untuk analisis kredit tetapi menolak penggunaan data kontak untuk penagihan kepada pihak ketiga. Praktik demikian sebenarnya telah bermasalah dari perspektif Pasal 22 ayat (4) dan ayat (5) UU PDP yang mensyaratkan bahwa apabila persetujuan memuat tujuan lain, persetujuan harus dapat dibedakan secara jelas, dan ketidakpatuhan terhadap syarat ini mengakibatkan persetujuan batal demi hukum. Namun persoalannya adalah bahwa tidak ada mekanisme verifikasi yang konkret untuk menentukan apakah klausul persetujuan tertentu telah memenuhi standar Pasal 22 ayat (4). Pertanyaan "apakah tujuan-tujuan pemrosesan telah dapat dibedakan secara jelas" memerlukan penilaian subjektif yang tidak memiliki parameter objektif dalam UU PDP maupun dalam Peraturan Pemerintah pelaksana — yang hingga saat ini belum diterbitkan.

Paul Schwartz dan Karl-Nikolaus Peifer dalam kajian komparatif mereka mengenai hukum privasi menemukan bahwa efektivitas ketentuan *purpose limitation* sangat bergantung pada ketersediaan mekanisme operasional yang menghubungkan norma-norma yang tersebar menjadi satu sistem yang koheren dan dapat ditegakkan. Tanpa mekanisme demikian, norma-norma yang baik pun akan

kehilangan daya tegaknya karena tidak ada instrumen yang memungkinkan penentuan secara objektif apakah suatu tindakan pengendali data telah memenuhi atau melanggar norma tersebut.

Dalam konteks UU PDP, ketiadaan Peraturan Pemerintah pelaksana Pasal 16 ayat (3) yang seharusnya mengatur ketentuan lebih lanjut mengenai standar teknis pemrosesan data menjadikan keterbatasan pertama ini semakin sulit diatasi. Tanpa Peraturan Pemerintah yang menetapkan parameter objektif mengenai apa yang dimaksud dengan tujuan yang "terbatas dan spesifik" dalam Pasal 27, penyelenggara layanan memiliki diskresi yang sangat luas untuk mendefinisikan tujuan pemrosesan sesuai kepentingannya sendiri, asalkan masih dapat dianggap memenuhi syarat formal Pasal 21.

Kedua, Ketiadaan Instrumen Verifikasi Kepatuhan terhadap Kewajiban Pemrosesan Sesuai Tujuan (Pasal 28). Keterbatasan kedua merupakan konsekuensi langsung dari keterbatasan pertama. Karena Pasal 21 tidak mengintegrasikan standar spesifisitas Pasal 27, tujuan yang diberitahukan kepada pengguna sering kali dirumuskan secara terlalu luas untuk dapat dijadikan ukuran yang terukur dalam menilai kepatuhan terhadap Pasal 28. Namun terlepas dari persoalan spesifisitas tujuan tersebut, keterbatasan kedua adalah bahwa Pasal 21 tidak memuat instrumen apapun yang memungkinkan verifikasi terhadap apakah penggunaan data oleh pengendali telah tetap berada dalam batas tujuan yang diberitahukan. Dalam teori efektivitas hukum yang dikembangkan oleh Soerjono Soekanto, salah satu faktor penentu efektivitas suatu norma hukum adalah tersedianya sarana atau fasilitas yang memungkinkan pelaksanaan norma tersebut. Norma hukum yang tidak dilengkapi dengan mekanisme implementasi yang memadai cenderung tidak efektif bukan karena substansi normanya lemah,

melainkan karena tidak tersedia instrumen untuk memastikan kepatuhan terhadapnya. Keterbatasan kedua Pasal 21 adalah kegagalannya dalam menyediakan mekanisme implementasi yang menghubungkan kewajiban pemberitahuan tujuan dengan pengawasan kepatuhan terhadap tujuan tersebut sepanjang siklus pemrosesan data.

Dari perspektif aktif, Pasal 5 UU PDP memberikan hak kepada subjek data untuk mendapatkan informasi mengenai penggunaan data pribadinya. Namun hak ini bersifat pasif yang berarti subjek data dapat meminta informasi, tetapi tidak ada mekanisme yang secara otomatis memastikan bahwa informasi tersebut diberikan secara proaktif oleh pengendali data. Lebih jauh, tidak ada ketentuan yang mewajibkan pengendali data untuk memberikan laporan periodik kepada subjek data mengenai bagaimana datanya telah digunakan, apakah penggunaan tersebut masih sesuai dengan tujuan yang diberitahukan, dan apakah tujuan tersebut telah berubah.

Dari perspektif pasif, Pasal 31 UU PDP mewajibkan pengendali data untuk melakukan perekaman terhadap seluruh kegiatan pemrosesan data pribadi. Kewajiban ini pada prinsipnya menyediakan mekanisme pembuktian kepatuhan karena rekaman pemrosesan dapat digunakan untuk menunjukkan bahwa setiap penggunaan data memiliki dasar yang sah dan sesuai dengan tujuan yang ditetapkan. Namun, Pasal 31 tidak mewajibkan pengendali data untuk memberikan akses atas rekaman tersebut kepada subjek data, dan tidak mengatur mekanisme pemeriksaan rekaman pemrosesan oleh lembaga pengawas secara berkala. Rekaman pemrosesan berdasarkan Pasal 31 lebih berfungsi sebagai alat pembuktian yang baru dapat diminta ketika sudah terjadi sengketa, bukan sebagai instrumen preventif yang mencegah terjadinya pelanggaran tujuan pemrosesan.

Perbandingan dengan GDPR kembali relevan di sini. Dalam GDPR, Pasal 13 dan Pasal 14 mengatur kewajiban pengendali data untuk menyediakan informasi kepada subjek data mengenai tujuan dan dasar hukum pemrosesan, termasuk kepentingan yang sah yang digunakan sebagai dasar legalitas pemrosesan. Lebih penting lagi, GDPR mengatur prinsip *accountability* dalam Pasal 5 ayat (2) yang mewajibkan pengendali data untuk tidak hanya mematuhi prinsip-prinsip perlindungan data, tetapi juga mampu menunjukkan kepatuhannya. Prinsip demikian menetapkan beban pembuktian terbalik: bukan korban yang harus membuktikan bahwa pengendali telah melanggar, melainkan pengendali yang harus membuktikan bahwa ia telah mematuhi.

Ketiadaan prinsip serupa dalam Pasal 21 UU PDP berdampak langsung pada kemampuan subjek data untuk menuntut pertanggungjawaban pengendali data. Dalam kasus *ShopeePay Later*, pengadu yang melaporkan bahwa pihak penagih menghubungi nomor-nomor yang bukan kontak darurat terdaftar menghadapi kesulitan normatif yang sangat nyata: bagaimana membuktikan bahwa penggunaan data tersebut melampaui tujuan yang dinyatakan dalam klausul persetujuan, ketika tujuan tersebut dirumuskan secara sangat luas. Tanpa instrumen verifikasi kepatuhan yang konkret, korban berada dalam posisi yang sangat lemah untuk menuntut pertanggungjawaban pengendali data. Sinta Dewi Rosadi dalam karyanya mengenai aspek privasi dalam hukum siber menekankan bahwa efektivitas perlindungan privasi dalam era digital sangat bergantung pada ketersediaan mekanisme *accountability* yang konkret, tidak cukup hanya dengan adanya norma substantif yang baik. Mekanisme akuntabilitas yang dimaksud mencakup kewajiban pengendali data untuk mendokumentasikan dan dapat membuktikan kepatuhannya terhadap prinsip-prinsip perlindungan data, termasuk

prinsip *purpose limitation*, kapan saja diminta oleh subjek data maupun lembaga pengawas.

Ketiga, Pengaturan Penggunaan Data oleh Pihak Ketiga Tidak Diintegrasikan ke dalam Mekanisme Pasal 21. Keterbatasan ketiga berkaitan dengan peran pihak ketiga dalam ekosistem penagihan pinjaman online. Dalam praktiknya, kegiatan penagihan pada layanan pinjaman online tidak selalu dilakukan secara langsung oleh penyelenggara. Penagihan dapat dilakukan oleh unit penagihan internal, oleh agen *debt collector* yang merupakan karyawan penyelenggara, atau oleh *debt collector* pihak ketiga yang memperoleh akses terhadap data pribadi pengguna berdasarkan kontrak dengan penyelenggara.

Pasal 21 UU PDP secara eksplisit hanya mengatur kewajiban pengendali data terhadap subjek data: pengendali wajib menyampaikan informasi mengenai tujuan pemrosesan kepada subjek data. Pasal 21 tidak mengatur bagaimana tujuan yang telah diberitahukan kepada subjek data tersebut berlaku mengikat bagi pihak ketiga yang kemudian menggunakan data tersebut untuk kepentingan penagihan. Pertanyaan normatif yang tidak terjawab oleh Pasal 21 adalah: apakah tujuan pemrosesan yang disampaikan oleh pengendali data kepada subjek data secara otomatis menjadi batas penggunaan data yang mengikat *debt collector* sebagai pihak yang menggunakan data tersebut dalam kegiatan penagihan?

Pasal 37 UU PDP memberikan jawaban parsial terhadap pertanyaan ini. Pasal 37 mewajibkan pengendali data untuk melakukan pengawasan terhadap setiap pihak yang terlibat dalam pemrosesan data di bawah kendalinya. Kewajiban pengawasan ini secara implisit menunjukkan bahwa tanggung jawab pengendali data mencakup juga pemastian bahwa pihak ketiga yang menggunakan data di bawah instruksinya tidak melampaui batas tujuan yang ditetapkan. Namun

kewajiban pengawasan tanpa mekanisme teknis pelaksanaan bersifat deklaratif dan tidak dapat dioperasionalisasikan secara efektif di lapangan.

Mekanisme teknis pelaksanaan kewajiban pengawasan tersebut seharusnya diatur dalam Peraturan Pemerintah pelaksana Pasal 16 ayat (3) UU PDP, yang mendelegasikan pengaturan lebih lanjut mengenai ketentuan teknis pemrosesan data kepada Peraturan Pemerintah. Namun, Peraturan Pemerintah ini belum diterbitkan, sehingga kewajiban Pasal 37 tidak memiliki petunjuk teknis operasional yang memadai. Kondisi ini menyebabkan kewajiban pengawasan pengendali data terhadap pihak ketiga dalam praktiknya sangat bergantung pada iktikad baik penyelenggara, bukan pada kewajiban hukum yang terukur dan dapat ditegakkan. Peraturan OJK Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi sebenarnya telah berupaya mengisi kekosongan ini melalui Pasal 157 yang mengatur bahwa pertukaran data antara penyelenggara dan pihak lain harus didasarkan pada perjanjian kerahasiaan data. Perjanjian kerahasiaan data tersebut paling sedikit harus memuat: (a) jenis data yang dipertukarkan; (b) penggunaan dan pengungkapan data; (c) hak dan kewajiban para pihak; (d) pertanggungjawaban para pihak; serta (e) jangka waktu penggunaan dan penyimpanan data. Penyelenggara juga diwajibkan untuk memastikan bahwa pihak penerima data mematuhi ketentuan dalam perjanjian kerahasiaan data tersebut. Ketentuan Pasal 157 POJK Nomor 40 Tahun 2024 ini merupakan langkah maju yang signifikan dalam konteks perlindungan data di sektor fintech lending. Namun, terdapat dua persoalan mendasar yang membatasi efektivitasnya. Pertama, ketentuan tersebut berada di tingkat peraturan sektoral OJK, bukan di tingkat undang-undang, sehingga hierarkinya di bawah UU PDP. Apabila terdapat konflik atau ketidaksesuaian antara POJK dan UU PDP, maka UU

PDP yang berlaku. Kedua dan lebih krusial, Pasal 157 POJK mengatur mekanisme transfer data antara penyelenggara dan pihak ketiga, tetapi tidak secara tegas mengatur bahwa tujuan pemrosesan yang disampaikan oleh pengendali data kepada subjek data menjadi batas mutlak penggunaan data dalam perjanjian kerahasiaan tersebut. Dengan kata lain, POJK mengatur mekanisme transfer yang aman, tetapi tidak mengintegrasikannya dengan prinsip *purpose limitation* yang diatur dalam Pasal 28 UU PDP.

Kondisi ini menciptakan apa yang dapat disebut sebagai inversi hierarki norma, yang dimana dalam praktiknya, perlindungan data pengguna layanan pinjaman online lebih banyak bergantung pada POJK Nomor 40 Tahun 2024 daripada pada UU PDP sebagai undang-undang induknya. Regulasi sektoral berfungsi sebagai pelindung utama, sementara undang-undang yang seharusnya menjadi fondasi normatif justru tidak memberikan pengaturan yang cukup operasional. Inversi hierarki norma ini bermasalah secara teoritis karena mengakibatkan ketidakkonsistenan perlindungan: pengguna layanan yang diatur oleh OJK mendapat perlindungan yang lebih konkret daripada pengguna layanan yang berada di luar lingkup pengawasan OJK, padahal UU PDP seharusnya berlaku universal.

Kasus *ShopeePay Later* kembali menjadi relevan sebagai ilustrasi. Dalam kasus tersebut, pengadu melaporkan bahwa pihak penagihan menghubungi sejumlah nomor telepon yang bukan merupakan kontak darurat maupun nomor yang terdaftar pada akun pengguna. Meskipun PT Commerce Finance beroperasi sebagai lembaga pembiayaan resmi di bawah pengawasan OJK dan dengan demikian tunduk pada POJK Nomor 40 Tahun 2024 pelanggaran tetap terjadi. Hal

ini menunjukkan bahwa bahkan mekanisme perlindungan yang lebih operasional pun tidak efektif tanpa pengawasan yang aktif dan sanksi yang berdampak jera.

Keempat, Ketiadaan Sanksi Khusus atas Pelanggaran Tujuan Pemrosesan dan Dampak Kritikal dari Absennya Peraturan Pemerintah Pelaksana. Keterbatasan keempat merupakan yang paling fundamental dari perspektif penegakan hukum. Ketiga keterbatasan sebelumnya — ketiadaan integrasi antara Pasal 21 dan Pasal 27, ketiadaan instrumen verifikasi kepatuhan terhadap Pasal 28, serta lemahnya pengaturan pihak ketiga — semuanya diperparah oleh kenyataan bahwa UU PDP tidak menyediakan sanksi khusus yang secara eksplisit ditujukan terhadap pelanggaran tujuan pemrosesan data, dan bahwa seluruh ekosistem norma UU PDP beroperasi tanpa Peraturan Pemerintah pelaksana yang menjadi petunjuk teknis operasionalnya.

Mengenai sanksi, UU PDP telah mengatur sanksi administratif dalam Pasal 57 yang mencakup pelanggaran terhadap berbagai kewajiban pengendali data. Pasal 57 ayat (3) mengatur bahwa sanksi administratif dapat berupa teguran tertulis, penghentian sementara kegiatan pemrosesan, penghapusan atau pemusnahan data pribadi, denda administratif, dan/atau pengumuman kepada publik mengenai pelanggaran yang dilakukan. Denda administratif ditetapkan paling tinggi sebesar 2% (dua persen) dari pendapatan tahunan atau penerimaan tahunan terhadap variabel pelanggaran. Persoalannya, Pasal 57 tidak mengidentifikasi secara khusus pelanggaran *purpose limitation* sebagai kategori pelanggaran tersendiri yang dikenai sanksi dengan tingkat keparahan tertentu. Sanksi yang diatur bersifat umum dan berlaku untuk semua jenis pelanggaran kewajiban pengendali data. Hal ini berbeda dengan GDPR yang dalam Pasal 83 membedakan tingkat sanksi berdasarkan tingkat keparahan pelanggaran: pelanggaran terhadap prinsip-prinsip

dasar pemrosesan data — termasuk *purpose limitation* — diancam dengan denda paling tinggi sebesar 20 juta Euro atau 4% dari total omzet tahunan global, tergantung mana yang lebih besar. Diferensiasi sanksi ini memberikan sinyal yang jelas kepada pengendali data mengenai pelanggaran mana yang dianggap paling serius, sehingga mendorong kepatuhan yang lebih besar terhadap prinsip-prinsip yang paling fundamental.

Dari sisi sanksi pidana, Pasal 65 UU PDP mengatur larangan pemrosesan data pribadi secara melawan hukum, termasuk larangan memperoleh, mengumpulkan, mengungkapkan, dan menggunakan data pribadi yang bukan miliknya secara melawan hukum. Ketentuan pidana ini secara fokus menyasar perolehan dan pengungkapan data secara melawan hukum. Yang tidak secara eksplisit dijangkau adalah pelanggaran *purpose limitation*: penggunaan data yang awalnya diperoleh secara sah tetapi kemudian digunakan untuk tujuan yang berbeda dari tujuan yang disampaikan kepada subjek data. Penggunaan data kontak pengguna *ShopeePay Later* oleh pihak penagih untuk menghubungi nomor-nomor yang bukan kontak darurat merupakan contoh pelanggaran *purpose limitation* di mana data diperoleh secara sah. Dengan pengguna menyetujui pengumpulan data saat registrasi, namun kemudian digunakan melampaui tujuan yang semestinya.

Hal ini merupakan kekosongan hukum yang nampak jelas dalam UU PDP: ada norma yang mewajibkan pemrosesan sesuai tujuan (Pasal 28), namun tidak ada sanksi pidana yang secara spesifik menjerat pelanggaran norma tersebut ketika pelanggaran terjadi atas data yang diperoleh secara sah. Pasal 65 UU PDP hanya menjangkau pelanggaran perolehan data secara melawan hukum, bukan pelanggaran penggunaan data yang telah diperoleh secara sah namun digunakan melampaui tujuan. Ini adalah celah normatif yang serius. Persoalan yang paling

fundamental dan sekaligus yang paling nyata adalah ketiadaan Peraturan Pemerintah pelaksana yang diamanatkan oleh beberapa pasal kritis dalam UU PDP. Setidaknya tiga pasal mendelegasikan pengaturan teknis operasional kepada Peraturan Pemerintah. Pertama, Pasal 16 ayat (3) UU PDP mendelegasikan pengaturan lebih lanjut mengenai ketentuan pengumpulan data pribadi kepada Peraturan Pemerintah. Kedua, Pasal 12 ayat (2) UU PDP mendelegasikan pengaturan mengenai tata cara pengenaan ganti rugi atas penyalahgunaan data pribadi kepada Peraturan Pemerintah. Ketiga, Pasal 34 ayat (3) UU PDP mendelegasikan pengaturan mengenai mekanisme penilaian dampak perlindungan data pribadi kepada Peraturan Pemerintah.

Ketiga Peraturan Pemerintah yang diamanatkan tersebut, hingga penelitian ini disusun pada tahun 2026, belum juga diterbitkan oleh pemerintah. Ketiadaan Peraturan Pemerintah ini menciptakan kekosongan operasional yang paling nyata dalam ekosistem UU PDP: norma-norma substantif yang sudah ada — termasuk Pasal 27 yang mewajibkan spesifisitas tujuan dan Pasal 28 yang mewajibkan pemrosesan sesuai tujuan — tidak dapat dioperasionalisasikan secara efektif karena tidak ada petunjuk teknis yang menjadi referensi bagi penyelenggara dalam implementasinya maupun bagi pengawas dalam penilaiannya. Rinjani dan Firmansyah dalam penelitian mereka mengenai hambatan implementasi UU PDP menemukan bahwa salah satu faktor terbesar yang menghambat efektivitas UU PDP adalah belum terbentuknya struktur kelembagaan dan regulasi teknis yang diperlukan untuk mendukung pelaksanaannya. Tanpa Peraturan Pemerintah pelaksana, pengendali data tidak memiliki standar yang jelas mengenai apa yang harus dilakukan untuk mematuhi UU PDP, dan lembaga pengawas tidak memiliki parameter yang terukur untuk menilai kepatuhan tersebut. Annur dalam laporannya

mengenai perlindungan data pribadi di Indonesia menyoroti bahwa kekosongan regulasi teknis ini telah menciptakan ketidakpastian hukum yang signifikan bagi pelaku industri, yang pada gilirannya mengakibatkan inkonsistensi dalam implementasi perlindungan data di berbagai sektor, termasuk sektor fintech lending. Kondisi ini secara langsung berdampak pada kemampuan pengguna layanan pinjaman online untuk mendapatkan perlindungan yang efektif terhadap penyalahgunaan data pribadi mereka. Ironisnya, kondisi demikian menciptakan paradoks regulasi: negara memiliki undang-undang perlindungan data yang relatif komprehensif dalam substansi normatifnya, namun undang-undang tersebut tidak dapat berfungsi efektif karena infrastruktur regulasi teknis yang menjadi prasyarat operasionalisasinya belum tersedia. Paradoks ini merupakan manifestasi dari apa yang dalam teori hukum dikenal sebagai *regulatory gap* atau kesenjangan antara norma yang tertulis dan kapasitas sistem untuk menegakkan norma tersebut dalam kenyataan.

Keempat keterbatasan yang telah dianalisis tidak berdiri sendiri-sendiri melainkan membentuk sebuah rantai kausal yang saling memperparah. Rantai kausal dimulai dari Keterbatasan Pertama: karena Pasal 21 tidak mengintegrasikan standar spesifisitas Pasal 27, pengendali data dapat merumuskan tujuan pemrosesan secara sangat luas dalam klausul persetujuan. Tujuan yang luas ini kemudian menjadi lahan subur bagi Keterbatasan Kedua: karena tujuan yang diberitahukan terlalu umum untuk dijadikan patokan kepatuhan, tidak ada instrumen yang dapat mengukur secara objektif apakah penggunaan data dalam penagihan telah melampaui tujuan tersebut. Keterbatasan Kedua ini kemudian diperparah oleh Keterbatasan Ketiga: karena Pasal 21 tidak mengatur secara spesifik bagaimana tujuan yang diberitahukan mengikat pihak ketiga dalam

penagihan, *debt collector* memiliki ruang untuk beroperasi di luar batas tujuan tanpa tanggung jawab yang jelas. Dan seluruh rantai keterbatasan ini dibiarkan tanpa penyelesaian efektif karena Keterbatasan Keempat: tidak ada sanksi khusus untuk pelanggaran *purpose limitation*, dan tidak ada Peraturan Pemerintah pelaksana yang menyediakan parameter teknis untuk menilai kepatuhan.

Jika diletakkan dalam kerangka teori efektivitas hukum Soerjono Soekanto, keempat keterbatasan ini berkorespondensi dengan kelemahan pada seluruh lima faktor yang menentukan efektivitas hukum. Faktor substansi hukum: Pasal 21 tidak memuat norma yang terintegrasi dengan baik. Faktor aparat penegak hukum: lembaga pengawas perlindungan data yang diamanatkan UU PDP belum beroperasi penuh. Faktor sarana dan fasilitas: Peraturan Pemerintah pelaksana sebagai petunjuk teknis belum tersedia. Faktor masyarakat: pengguna layanan pinjaman online umumnya memiliki literasi data yang rendah sehingga tidak mampu memanfaatkan hak-hak yang diberikan UU PDP. Faktor budaya hukum: kepatuhan terhadap ketentuan perlindungan data belum menjadi budaya dalam industri fintech lending di Indonesia.

Kondisi ini menggambarkan bahwa efektivitas UU PDP dalam melindungi privasi pengguna layanan pinjaman online dari penyalahgunaan data dalam praktik penagihan bukan sekadar persoalan normatif, melainkan persoalan sistemik yang mencakup seluruh ekosistem penegakan hukum. Solusi yang efektif karenanya tidak dapat bersifat parsial — tidak cukup hanya mengubah redaksi Pasal 21 — melainkan harus mencakup pembenahan pada seluruh lapisan ekosistem: normatif, kelembagaan, teknis, dan kultural.

Keterbatasan pengaturan tujuan pemrosesan data pribadi dalam Pasal 21 UU PDP berimplikasi langsung terhadap mekanisme pertanggungjawaban hukum atas

penyalahgunaan data pribadi dalam praktik penagihan pinjaman online. Sebagai ketentuan yang mewajibkan pengendali data pribadi untuk memberitahukan tujuan pemrosesan data kepada subjek data pribadi, Pasal 21 UU PDP seharusnya menjadi dasar untuk menentukan apakah suatu penggunaan data pribadi masih berada dalam ruang lingkup tujuan yang sah atau telah melampaui tujuan yang disampaikan sebelumnya. Akan tetapi, sebagaimana telah diuraikan pada pembahasan sebelumnya, Pasal 21 UU PDP tidak memberikan parameter yang jelas mengenai tingkat spesifikasi tujuan pemrosesan dan tidak secara eksplisit melarang penggunaan data pribadi di luar tujuan yang telah diberitahukan kepada subjek data pribadi.

Implikasi pertama dari keterbatasan arsitektur norma Pasal 21 UU PDP adalah ketidakpastian normatif dalam menentukan kapan suatu penggunaan data pribadi dapat dikualifikasikan sebagai pelanggaran *purpose limitation*. Ketidakpastian ini bukan persoalan empiris semata — bukan sekadar soal kesulitan pembuktian faktual — melainkan persoalan normatif yang lebih mendasar: norma yang ada tidak memberikan parameter yang cukup jelas untuk menentukan batas antara penggunaan data yang sah dan yang melampaui tujuan yang diizinkan. Untuk memahami implikasi ini secara lebih konkret, pertimbangkan skenario berikut yang merepresentasikan kasus ShopeePay Later. Seorang pengguna mendaftarkan diri pada layanan ShopeePay Later dan menyetujui klausul persetujuan yang berbunyi (secara parafrase): "Kami mengumpulkan dan menggunakan data pribadi Anda, termasuk informasi kontak di perangkat Anda, untuk keperluan layanan keuangan kami, verifikasi identitas, pencegahan penipuan, dan kepatuhan terhadap kewajiban hukum yang berlaku." Klausul seperti ini secara formal memenuhi kewajiban Pasal 21 UU PDP karena tujuan pemrosesan telah disebutkan. Dan juga klausul ini

mencakup penggunaan data kontak untuk menghubungi pihak ketiga dalam proses penagihan. Karena tidak dapat ditentukan secara pasti berdasarkan Pasal 21 dan Pasal 28 UU PDP secara bersama-sama. Dari perspektif pengendali data, "keperluan layanan keuangan" dapat diinterpretasikan sangat luas untuk mencakup penagihan melalui pihak ketiga. Dari perspektif subjek data, interpretasi tersebut melampaui ekspektasi yang wajar karena verifikasi identitas dan pencegahan penipuan jelas tidak memerlukan penghubungan pihak-pihak yang tidak terlibat dalam perjanjian pinjaman. Ketidakpastian interpretasi ini merupakan akibat langsung dari keterbatasan pertama: karena Pasal 21 tidak mensyaratkan tujuan yang spesifik dan Pasal 27 tidak diintegrasikan ke dalam Pasal 21, klausul yang sangat luas seperti "keperluan layanan keuangan" dapat dianggap memenuhi syarat Pasal 21 secara formal. Dan karena tidak ada parameter objektif yang ditetapkan oleh Peraturan Pemerintah pelaksana, tidak ada cara yang pasti untuk menentukan di mana batas antara penggunaan yang sah dan penggunaan yang melampaui tujuan. Dalam doktrin perlindungan data, ketidakpastian interpretasi ini diselesaikan melalui prinsip *contextual integrity* yang dikembangkan oleh Helen Nissenbaum: penggunaan informasi dianggap sesuai apabila sesuai dengan norma-norma berbagi informasi dalam konteks tertentu di mana informasi tersebut awalnya diberikan. Penerapan prinsip ini dalam konteks pinjaman online menunjukkan bahwa data kontak yang diberikan dalam konteks registrasi layanan keuangan seharusnya hanya digunakan dalam konteks yang sama: hubungan langsung antara penyelenggara dan pengguna. Penggunaannya untuk menghubungi pihak ketiga di luar konteks tersebut melanggar *contextual integrity* dan karenanya merupakan pelanggaran privasi. Namun prinsip ini belum secara eksplisit diadopsi dalam UU PDP sebagai standar interpretasi, sehingga tidak dapat langsung

digunakan sebagai basis tuntutan hukum. Ketidakpastian normatif ini memiliki dampak yang sangat nyata bagi korban penyalahgunaan data. Pengguna yang datanya digunakan melampaui tujuan yang dinyatakan menghadapi hambatan normatif yang besar untuk menuntut pertanggungjawaban pengendali data: mereka tidak dapat dengan mudah menunjukkan bahwa penggunaan data tersebut secara definitif melampaui tujuan yang diizinkan, karena tujuan yang diizinkan itu sendiri dirumuskan secara tidak jelas.

Implikasi kedua berkaitan dengan penetapan pihak yang harus bertanggung jawab ketika pelanggaran *purpose limitation* terjadi dalam struktur penagihan yang melibatkan lebih dari satu pihak. Struktur penagihan dalam industri pinjaman online sering bersifat berlapis: penyelenggara sebagai pengendali data memberikan akses kepada pihak ketiga sebagai prosesor data, yang kemudian melaksanakan penagihan. Ketika pihak ketiga menggunakan data melampaui tujuan yang ditetapkan, siapa yang bertanggung jawab? UU PDP telah memberikan jawaban normatif atas pertanyaan ini melalui dua ketentuan yang berpotensi berbenturan. Di satu sisi, Pasal 50 UU PDP menegaskan bahwa pengendali data bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawaban dalam pelaksanaan kewajiban pemrosesan data pribadi. Pasal 51 ayat (3) memperkuat ketentuan ini dengan menyatakan bahwa pemrosesan data yang dilakukan oleh prosesor termasuk dalam tanggung jawab pengendali data. Dengan demikian, dalam kerangka ini, penyelenggara pinjaman online sebagai pengendali data bertanggung jawab atas tindakan *debt collector* sebagai prosesornya, termasuk apabila *debt collector* menggunakan data melampaui tujuan yang ditetapkan. Di sisi lain, Pasal 51 ayat (6) UU PDP mengatur bahwa apabila prosesor melakukan pemrosesan di luar perintah dan tujuan yang ditetapkan pengendali, tanggung

jawab beralih kepada prosesor. Ketentuan ini menciptakan apa yang dalam teori hukum dapat disebut sebagai *shifting liability clause*: pengalihan tanggung jawab dari pengendali ke prosesor berdasarkan kondisi tertentu. Namun, kondisi yang memicu pengalihan tanggung jawab tersebut — yaitu tindakan prosesor yang dilakukan "di luar perintah dan tujuan yang ditetapkan pengendali" — sangat sulit dibuktikan dalam kondisi di mana perintah pengendali kepada prosesor dirumuskan secara luas dan tidak spesifik.

Philipus M. Hadjon dan Tatiek Sri Djatmiati dalam diskusi mengenai argumentasi hukum menekankan bahwa ketentuan hukum yang mengatur pengalihan tanggung jawab memerlukan kriteria yang jelas dan objektif agar tidak membuka peluang bagi pihak yang lebih kuat untuk menghindar dari tanggung jawab. Dalam konteks Pasal 51 ayat (6) UU PDP, kriteria "di luar perintah dan tujuan yang ditetapkan pengendali" adalah kriteria yang sangat bergantung pada bagaimana penyelenggara merumuskan instruksi dan batas penggunaan data dalam perjanjian dengan *debt collector*. Penyelenggara yang merumuskan instruksi secara sangat luas — misalnya "gunakan data yang tersedia untuk kegiatan penagihan" — akan sangat mudah berargumen bahwa apapun yang dilakukan *debt collector* masih berada dalam cakupan instruksi tersebut, sehingga tanggung jawab tidak beralih ke prosesor. Kondisi ini menciptakan potensi *moral hazard* dimana penyelenggara pinjaman online dapat menggunakan struktur pengendali-prosesor untuk meminimalkan tanggung jawab hukumnya atas pelanggaran yang dilakukan oleh *debt collector*. Dengan merumuskan instruksi kepada *debt collector* secara luas, penyelenggara secara teoritis memberikan ruang bagi *debt collector* untuk melakukan praktik penagihan yang melanggar privasi, sekaligus dapat berargumen bahwa tindakan tersebut dilakukan "dalam pelaksanaan tugas" sehingga tanggung

jawab tidak beralih ke prosesor berdasarkan Pasal 51 ayat (6). Di sisi lain, jika penyelenggara berdalih bahwa *debt collector* bertindak di luar instruksi, maka tanggung jawab beralih ke *debt collector* yang mungkin tidak memiliki kemampuan finansial untuk memenuhi tuntutan ganti rugi.

Pane dan Kansil dalam analisis mereka mengenai tanggung jawab penyelenggara pinjol menekankan bahwa ketidakjelasan batas tanggung jawab antara pengendali dan prosesor data dalam UU PDP merupakan salah satu faktor yang paling menghambat penegakan hukum perlindungan data di sektor fintech lending. Tanpa kejelasan batas tersebut, korban penyalahgunaan data menghadapi situasi di mana penyelenggara dan *debt collector* dapat saling melempar tanggung jawab, sementara korban tidak memiliki mekanisme yang memadai untuk menentukan siapa yang seharusnya menanggung akibat hukum dari pelanggaran yang dialaminya.

Implikasi ketiga dan yang paling berdampak pada perlindungan pengguna layanan pinjaman online adalah inefektivitas penegakan hukum terhadap pelanggaran *purpose limitation* yang disebabkan oleh keterbatasan arsitektur norma Pasal 21 UU PDP. Inefektivitas penegakan hukum ini termanifestasi dalam beberapa dimensi yang saling memperkuat. Hal ini terjadi karena ketiadaan lembaga pengawas yang secara aktif memantau kepatuhan terhadap prinsip *purpose limitation* dalam praktik penagihan pinjaman online. UU PDP telah mengatur pembentukan lembaga yang berwenang dalam perlindungan data pribadi. Namun, lembaga tersebut belum beroperasi secara penuh dan mandiri, serta belum memiliki kewenangan yang jelas dalam konteks pengawasan sektor fintech lending yang saat ini masih berada di bawah kewenangan OJK. OJK sebagai regulator sektor keuangan memiliki kewenangan pengawasan terhadap penyelenggara

layanan pendanaan bersama berbasis teknologi informasi berdasarkan POJK Nomor 40 Tahun 2024. Namun kewenangan OJK lebih berfokus pada aspek kehati-hatian keuangan dan perlindungan konsumen dalam konteks layanan keuangan, bukan secara spesifik pada penegakan prinsip *purpose limitation* dalam pemrosesan data pribadi. Kondisi ini menciptakan *regulatory gap*: ada dua lembaga yang memiliki yurisdiksi parsial atas persoalan yang sama, tetapi tidak ada yang memiliki kewenangan dan kapasitas yang lengkap untuk menanganinya secara efektif.

Selain itu juga rendahnya tingkat pelaporan oleh korban penyalahgunaan data. Survei dan penelitian menunjukkan bahwa sebagian besar korban penyalahgunaan data pribadi tidak melaporkan pelanggaran yang dialaminya, baik karena tidak mengetahui saluran pelaporan yang tersedia, tidak yakin bahwa laporannya akan ditindaklanjuti secara efektif, atau tidak memiliki bukti yang cukup untuk mendukung laporannya. Rendahnya tingkat pelaporan ini secara langsung berdampak pada kemampuan regulator untuk mendeteksi pola pelanggaran dan mengambil tindakan penegakan hukum yang diperlukan. Hak tersebut diperburuk dengan lemahnya efek jera dari sanksi yang ada. Denda administratif sebesar paling tinggi 2% dari pendapatan tahunan, meskipun secara nominal tidak kecil bagi penyelenggara skala menengah, tidak memberikan efek jera yang signifikan bagi penyelenggara berskala besar yang memiliki omzet ratusan miliar rupiah per tahun. Perbandingan dengan GDPR yang memiliki denda hingga 4% omzet global menunjukkan perbedaan yang sangat signifikan dalam tingkat kesungguhan norma sanksi. Lebih jauh, tanpa Peraturan Pemerintah yang menetapkan parameter teknis pelanggaran, denda administratif pun sulit diterapkan secara konsisten karena tidak

ada standar yang jelas mengenai kondisi apa yang memenuhi syarat sebagai pelanggaran yang dapat dikenai sanksi.

Kondisi inefektivitas penegakan hukum ini memiliki konsekuensi yang sangat merugikan bagi pengguna layanan pinjaman online: dalam ketiadaan pertanggungjawaban yang efektif, tidak ada insentif yang cukup kuat bagi penyelenggara untuk secara sukarela mematuhi prinsip *purpose limitation*. Pelanggaran menjadi rasional secara ekonomi apabila keuntungan yang diperoleh dari penggunaan data secara agresif dalam penagihan lebih besar daripada risiko sanksi yang dihadapi. Ini merupakan kegagalan fundamental dari sistem regulasi perlindungan data: sistem yang seharusnya mendorong kepatuhan melalui insentif dan sanksi justru menciptakan struktur insentif yang mendorong ketidakpatuhan. Kasus ShopeePay Later, yang terjadi pada penyelenggara resmi yang diawasi OJK, menjadi bukti nyata dari kondisi ini. Fakta bahwa pelanggaran privasi dalam penagihan tetap terjadi meskipun PT Commerce Finance beroperasi di bawah pengawasan regulator menunjukkan bahwa kerangka perlindungan yang ada — baik UU PDP maupun POJK Nomor 40 Tahun 2024 — belum cukup kuat untuk mencegah terjadinya pelanggaran privasi bahkan dalam ekosistem layanan keuangan yang telah berizin.

Temuan ini sejalan dengan kesimpulan Syahruddin dan Zulfa yang menyatakan bahwa ketidakcukupan penegakan hukum perlindungan data pribadi di Indonesia bukan semata-mata disebabkan oleh ketidaklengkapan norma substantif, melainkan oleh ketidaktersediaan mekanisme penegakan yang efektif yang mampu memberikan perlindungan nyata kepada subjek data dan efek jera yang sungguh-sungguh kepada pengendali data yang melanggar.

Analisis komparatif dengan GDPR Uni Eropa memberikan perspektif yang penting untuk memahami bagaimana keterbatasan arsitektur norma seperti yang terdapat dalam Pasal 21 UU PDP dapat diatasi secara efektif dalam sistem hukum perlindungan data yang lebih matang. Perbandingan ini tidak dimaksudkan untuk menyarankan adopsi model GDPR secara mentah ke dalam konteks Indonesia yang memiliki karakteristik hukum, sosial, dan ekonomi yang berbeda, melainkan untuk mengidentifikasi prinsip-prinsip arsitektur norma yang dapat diadaptasi. Dalam hal pengintegrasian norma, GDPR Pasal 5 memuat seluruh prinsip dasar pemrosesan data dalam satu pasal yang komprehensif dan saling merujuk: *lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality*, dan *accountability*. Pasal 5 ayat (2) kemudian secara eksplisit menetapkan prinsip akuntabilitas yang mewajibkan pengendali data untuk dapat menunjukkan kepatuhan terhadap seluruh prinsip dalam Pasal 5. Arsitektur ini memastikan bahwa kewajiban pemberitahuan (sebanding dengan Pasal 21 UU PDP) tidak dapat dipenuhi secara formal tanpa juga memenuhi standar kualitas tujuan yang dipersyaratkan oleh prinsip *purpose limitation* dalam pasal yang sama. Dalam hal mekanisme verifikasi kepatuhan, GDPR mensyaratkan pengendali data untuk melaksanakan *Data Protection Impact Assessment* (DPIA) untuk pemrosesan yang memiliki risiko tinggi terhadap hak-hak subjek data. Pasal 17 GDPR juga memberikan hak kepada subjek data untuk meminta penghapusan data apabila data diproses melampaui tujuan yang ditetapkan. Selain itu, Pasal 77 GDPR memberikan hak kepada subjek data untuk mengajukan pengaduan kepada otoritas pengawas apabila merasa pemrosesan datanya melanggar GDPR. Ketersediaan mekanisme ini memungkinkan verifikasi kepatuhan yang lebih efektif daripada yang dimungkinkan oleh mekanisme yang ada dalam UU PDP.

Dalam hal pengawasan dan sanksi, GDPR mensyaratkan setiap negara anggota Uni Eropa untuk membentuk otoritas pengawas perlindungan data yang independen, memiliki sumber daya yang memadai, dan berwenang untuk menginvestigasi pengaduan, melakukan audit, dan menjatuhkan sanksi. Diferensiasi sanksi dalam Pasal 83 GDPR — yang membedakan antara pelanggaran yang lebih ringan (denda hingga 10 juta Euro atau 2% omzet) dan pelanggaran prinsip dasar yang lebih serius (denda hingga 20 juta Euro atau 4% omzet) — memberikan sinyal yang jelas mengenai hierarki kepentingan normatif yang dilindungi dan mendorong kepatuhan yang lebih besar terhadap prinsip-prinsip yang paling fundamental.

Jika dikomparasikan, hal yang paling relevan dari GDPR untuk konteks Indonesia adalah bukan tentang besaran sanksi atau mekanisme spesifiknya, melainkan tentang pentingnya arsitektur norma yang kohesif: sebuah sistem di mana norma-norma substantif yang menetapkan standar perlindungan data dihubungkan secara eksplisit dengan norma-norma prosedural yang menetapkan mekanisme kepatuhan, verifikasi, dan penegakan. Tanpa kohesi arsitektural ini, bahkan norma substantif yang baik pun tidak dapat berfungsi secara efektif. Indonesia telah memiliki norma substantif yang baik dalam UU PDP, termasuk dalam Pasal 27 dan Pasal 28 yang mengatur *purpose limitation*. Yang diperlukan sekarang adalah penguatan arsitektur norma yang menghubungkan norma-norma tersebut secara kohesif — dan ini merupakan agenda regulasi yang sangat mendesak untuk dilaksanakan.

D. PENUTUP

Kesimpulan

1. Pasal 21 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah menetapkan kewajiban bagi pengendali data untuk

menyampaikan tujuan pemrosesan data pribadi kepada subjek data sebelum pemrosesan dilakukan. Dalam konteks layanan pinjaman online, ketentuan ini menempatkan penyelenggara sebagai pengendali data yang secara hukum terikat pada tujuan yang telah dinyatakan pada saat pengumpulan data, umumnya untuk keperluan verifikasi identitas dan analisis kelayakan kredit. Tujuan tersebut berfungsi sebagai batas hukum yang mengikat seluruh rangkaian pemrosesan berikutnya, termasuk pada tahap penagihan. Akan tetapi, Pasal 21 tidak mengintegrasikan secara eksplisit kewajiban pemberitahuan tersebut dengan standar spesifisitas tujuan yang diatur dalam Pasal 27 maupun larangan penggunaan data di luar tujuan sebagaimana diamanatkan Pasal 28. Akibatnya, penyelenggara pinjaman online dapat merumuskan tujuan pemrosesan secara terlalu luas dalam klausul persetujuan dan secara formal memenuhi Pasal 21, tanpa harus mematuhi prinsip purpose limitation secara substantif. Inilah yang menjadi keterbatasan utama arsitektur norma Pasal 21 UU PDP dalam mengatur penggunaan data pribadi pada layanan pinjaman online

2. Keterbatasan pengaturan tujuan pemrosesan data pribadi dalam Pasal 21 UU PDP berimplikasi langsung terhadap pertanggungjawaban hukum atas penyalahgunaan data pribadi dalam praktik penagihan pinjaman online. Keterbatasan tersebut terwujud melalui tiga implikasi yang saling memperkuat: pertama, ketidakpastian normatif dalam menentukan kapan suatu penggunaan data dapat dikualifikasikan sebagai pelanggaran purpose limitation, mengingat tujuan yang dicantumkan dalam klausul persetujuan lazimnya dirumuskan terlalu luas dan tidak memiliki parameter objektif; kedua, terbukanya potensi moral hazard dalam struktur pertanggungjawaban

antara pengendali data (penyelenggara pinjaman online) dan prosesor data (debt collector) berdasarkan Pasal 51 UU PDP, di mana ambiguitas klausul pengalihan tanggung jawab memungkinkan masing-masing pihak untuk saling melempar tanggung jawab ketika terjadi pelanggaran privasi; dan ketiga, inefektivitas penegakan hukum yang disebabkan oleh belum beroperasinya lembaga pengawas perlindungan data secara penuh, rendahnya tingkat pelaporan oleh korban, lemahnya efek jera sanksi administratif, serta belum diterbitkannya Peraturan Pemerintah pelaksana yang diamanatkan Pasal 16 ayat (3), Pasal 12 ayat (2), dan Pasal 34 ayat (3) UU PDP. Kondisi ini tercermin dalam kasus ShopeePay Later yang diselenggarakan oleh PT Commerce Finance, di mana pelanggaran privasi berupa penghubungan pihak di luar kontak darurat terdaftar tetap terjadi meskipun penyelenggara beroperasi secara resmi di bawah pengawasan Otoritas Jasa Keuangan, membuktikan bahwa permasalahan ini berakar pada ketidaklengkapan arsitektur norma UU PDP itu sendiri.

Saran

1. Untuk mengatasi keterbatasan pengaturan tujuan pemrosesan data pribadi dalam Pasal 21 UU PDP sebagaimana diidentifikasi dalam rumusan masalah pertama, pembentuk undang-undang perlu melakukan penguatan arsitektur norma melalui penambahan ketentuan yang secara eksplisit mengintegrasikan kewajiban pemberitahuan tujuan dalam Pasal 21 dengan standar spesifisitas tujuan dalam Pasal 27 dan kewajiban pemrosesan sesuai tujuan dalam Pasal 28. Penguatan ini dapat diwujudkan dengan menegaskan dalam Pasal 21 bahwa tujuan pemrosesan yang disampaikan kepada subjek data wajib memenuhi kriteria terbatas, spesifik, dan eksplisit, sehingga klausul

persetujuan yang terlalu luas tidak dapat dianggap memenuhi kewajiban pemberitahuan secara sah. Selain itu, Pemerintah perlu segera menerbitkan Peraturan Pemerintah pelaksana berdasarkan delegasi Pasal 16 ayat (3) UU PDP yang memuat parameter teknis mengenai standar spesifisitas tujuan, sehingga terdapat acuan terukur bagi penyelenggara pinjaman online dalam merumuskan tujuan pemrosesan maupun bagi lembaga pengawas dalam menilai kepatuhan.

2. Untuk mengatasi implikasi terhadap pertanggungjawaban hukum atas penyalahgunaan data pribadi dalam praktik penagihan pinjaman online sebagaimana diidentifikasi dalam rumusan masalah kedua, diperlukan dua langkah pembenahan yang saling melengkapi. Pertama, pembentuk undang-undang perlu memperjelas klausul pengalihan tanggung jawab dalam Pasal 51 ayat (6) UU PDP dengan menetapkan kriteria objektif mengenai kondisi yang dapat dikategorikan sebagai tindakan prosesor yang dilakukan "di luar perintah pengendali," sekaligus menambahkan norma sanksi yang secara spesifik menjangkau pelanggaran purpose limitation atas data yang diperoleh secara sah namun digunakan melampaui tujuan yang ditetapkan, mengisi kekosongan norma yang saat ini ada dalam Pasal 65 UU PDP. Kedua, Otoritas Jasa Keuangan perlu memperkuat Pasal 157 Peraturan OJK Nomor 40 Tahun 2024 dengan mewajibkan perjanjian kerahasiaan data antara penyelenggara dan debt collector untuk secara tegas mencantumkan tujuan pemrosesan yang telah disampaikan kepada subjek data sebagai batas mutlak penggunaan data dalam penagihan, serta segera mengoperasionalkan lembaga pengawas perlindungan data pribadi yang independen agar pengawasan kepatuhan terhadap prinsip

purpose limitation dapat berjalan secara efektif dan memberikan efek jera yang nyata bagi pelaku usaha.

REFERENSI

Alfitri, Nur Alfiana, Rahmawati, dan Firmansyah. 2024. "Perlindungan Terhadap Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi." Journal Social Society 4(2): 92–111.

Annur, Cindy Mutia. 2022. "Rawannya Perlindungan Data Pribadi di Indonesia." Katadata.

European Parliament and Council of the European Union. 2016. General Data Protection Regulation (GDPR).

Hadjon, Philipus M., dan Tatiek Sri Djatmiati. 2005. Argumentasi Hukum. Yogyakarta: Gadjah Mada University Press.

Kurniawati, Husni, dan Yunanto. 2022. "Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Debitur dalam Aktivitas Pinjaman Online." Jurnal Ius Constituendum 7(1): 102–114.

Maharianti, Dyah. 2025. "DC Shopee SPayLater Menagih ke Nomor yang Bukan Kontak Darurat atau Pemilik Akun." Media Konsumen, 30 Mei 2025.

Manurung, Evelyn A. P., dan Emmy F. Thalib. 2023. "Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022." Jurnal Hukum Saraswati 5(2): 135–145.

Marzuki, Peter Mahmud. 2016. Penelitian Hukum. Edisi Revisi. Jakarta: Kencana Prenada Media Group.

Minsiri, Poramate. 2022. "Thailand Personal Data Protection Act and Its Implications for Business Operations." Asian Journal of Law and Policy 3(1): 50–65.

Otoritas Jasa Keuangan. 2024. Peraturan Otoritas Jasa Keuangan Nomor 40 Tahun 2024 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi.

Pane, Ian Dharsono Wijaya, dan Christine Kansil. 2023. "Tanggung Jawab Penyelenggara Pinjol terhadap Data Pribadi dalam Layanan Fintech." Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis 53(1): 1–19.

Pemerintah Republik Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Republik Indonesia. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Rinjani, Muhamad Adri, dan Ricky Firmansyah. 2025. "Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia." Jurnal Analisis Hukum

8(1): 70–83.

Rosadi, Sinta Dewi. 2015. Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional. Bandung: Refika Aditama.

Schwartz, Paul, dan Karl-Nikolaus Peifer. 2013. "Comparative Information Privacy Law." Harvard International Law Journal 54(1): 233–270.

Soekanto, Soerjono. 2008. Faktor-Faktor yang Mempengaruhi Penegakan Hukum. Jakarta: PT RajaGrafindo Persada.

Solove, Daniel J. 2006. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154(3): 477–564.

Solove, Daniel J. 2008. Understanding Privacy. Cambridge: Harvard University Press.

Sunggono, Bambang. 2012. Metodologi Penelitian Hukum. Jakarta: PT RajaGrafindo Persada.

Syahruddin, Nurul Insi, dan Eva Achjani Zulfa. 2024. "Personal Data Protection Violations by Fintech Lending in Indonesia." Journal of Law, Politic and Humanities 4(4): 999–1006.

Tsamara, Nadiah. 2021. "Perbandingan Aturan Perlindungan Privasi atas Data Pribadi antara Indonesia dengan Beberapa Negara." Jurnal Suara Hukum 3(1): 53–84.

United Nations. 1948. Universal Declaration of Human Rights.

Waron, ARPM. 2023. "Perlindungan Hukum Terhadap Data Pribadi Pihak Peminjam yang Disebar oleh Layanan Pinjaman Online yang Berstatus Ilegal." Jurnal Pendidikan Tambusai 8: 17115–17132.

Warren, Samuel D., dan Louis D. Brandeis. 2005. "The Right to Privacy." Information

Ethics: Privacy, Property, and Power 4(5): 209–22