



ANALISIS YURIDIS PERLINDUNGAN DATA PRIBADI DALAM OPERASIONAL LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI (LPBBTI)

Andre Maulana Wahyudi, Paramita Prananingtyas, Bagus Rahmanda

Program Studi S1 Hukum, Fakultas Hukum, Universitas Diponegoro

E-mail : andrewahyudi72@gmail.com

Abstrak

Perkembangan teknologi dan informasi di era digital telah mendorong pertumbuhan Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) di Indonesia. Dalam operasionalnya, LPBBTI mengandalkan pemrosesan data pribadi pengguna, yang menimbulkan tantangan dalam aspek perlindungan data. Regulasi perlindungan data pribadi di Indonesia terus berkembang, terutama dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Namun, tantangan terkait penyalahgunaan data pribadi, kebocoran informasi, dan tindakan ilegal oleh penyelenggara LPBBTI masih sering terjadi. Penelitian ini bertujuan untuk (1) menganalisis perbandingan regulasi perlindungan data pribadi dalam LPBBTI antara Indonesia dan Singapura, serta (2) mengidentifikasi bentuk pertanggungjawaban penyelenggara LPBBTI berdasarkan UU PDP. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perbandingan hukum terhadap regulasi perlindungan data pribadi di kedua negara. Hasil penelitian menunjukkan bahwa Indonesia masih menghadapi tantangan dalam implementasi UU PDP, khususnya dalam penegakan hukum dan mekanisme perlindungan konsumen dalam ekosistem LPBBTI. Sebaliknya, Singapura telah memiliki Personal Data Protection Act (PDPA) 2012 yang lebih matang dengan sistem pengawasan yang lebih ketat, termasuk mekanisme Data Breach Notification dan sanksi tegas bagi pelanggar. Di Indonesia, mekanisme perlindungan masih memerlukan penguatan dari sisi pengawasan oleh Otoritas Jasa Keuangan (OJK) dan peningkatan kepatuhan penyelenggara LPBBTI terhadap regulasi perlindungan data pribadi. Penelitian ini merekomendasikan penguatan regulasi teknis, peningkatan pengawasan, serta edukasi bagi masyarakat dan pelaku industri LPBBTI dalam menerapkan standar perlindungan data pribadi yang lebih baik. Dengan langkah-langkah tersebut, diharapkan kepercayaan masyarakat terhadap layanan finansial berbasis teknologi dapat meningkat dan risiko kebocoran data dapat diminimalkan.

Kata kunci :Perlindungan Data Pribadi; Layanan Pendanaan Bersama Berbasis Teknologi Informasi; *Fintech*

Abstract

The advancement of technology and information in the digital era has driven the growth of Technology-Based Collective Funding Services (LPBBTI) in Indonesia. In its operations, LPBBTI relies on the processing of users' personal data, which raises challenges in data protection. Indonesia's personal data protection regulations have evolved, particularly with the enactment of Law Number 27 of 2022 on Personal Data Protection (UU PDP). However, issues related to data misuse, information breaches, and illegal practices by LPBBTI providers remain prevalent. This study aims to (1) analyze the regulatory comparison of personal data protection in LPBBTI between Indonesia and Singapore, and (2) identify the forms of liability imposed on LPBBTI providers under the UU PDP. This research employs a normative juridical method with a comparative legal approach to examine personal data protection regulations in both countries. The findings indicate that Indonesia still faces challenges in implementing the UU PDP, particularly in law enforcement and consumer protection mechanisms within the LPBBTI ecosystem. In contrast, Singapore has a more established Personal Data Protection Act (PDPA) of 2012, featuring strict supervision systems, a Data Breach Notification mechanism, and firm sanctions for violators. In Indonesia, protection mechanisms still require strengthening in terms of regulatory enforcement by the Financial Services Authority (OJK) and increasing compliance among LPBBTI providers with personal data protection regulations. This study recommends enhancing technical regulations, strengthening oversight, and educating both the public and LPBBTI industry players in adopting

higher standards for personal data protection. These efforts are expected to increase public trust in technology-based financial services and minimize data breach risks.

Keywords : *Personal Data Protection; Technology-Based Collective Funding Services; Fintech.*

I. PENDAHULUAN

Kegiatan Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) di Indonesia terus berkembang pesat dimana dalam kegiatannya layanan tersebut meliputi pihak pemberi dana dan penerima dana. Kebijakan terkait fintech sendiri dibuat melalui Otoritas Jasa Keuangan (OJK) dan Bank Sentral Indonesia yaitu (BI). Klasifikasi yang dilakukan oleh OJK adalah tersusunnya klasifikasi perusahaan fintech yang masuk dalam kewenangan OJK atau tidak, terdapat berbagai jenis usaha seperti perbankan, pinjam meminjam (peer to peer lending), crowd funding, channelling kredit dan lain sebagainya, sedangkan klasifikasi perusahaan fintech di bidang sistem pembayaran akan diatur oleh Bank Indonesia.¹ Pemberian dana berdasarkan ketentuan pasal 1 Angka 10 Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10 /POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi ialah orang perseorangan, badan hukum, dan/atau badan usaha yang memberikan pendanaan Sementara dari pihak penerima dana seperti orang perseorangan, badan hukum, dan/atau badan usaha yang menerima pendanaan sesuai ketentuan Pasal 1 Angka 9 Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 10 /POJK.06/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi. Permasalahan yang terjadi dalam penyelenggaraann Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) terdapat praktik yang illegal dilakukan oleh perusahaan serta pinjaman yang macet dan adanya campur tangan dari pihak penagih yaitu debt collector yang tidak sewajarnya hingga mencederai hak dari peminjam.² Pihak yang menghadapi jika adanya masalah dalam penyelenggaraan Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) ialah biasanya ditemukan dengan menghubungi pihak berwajib seperti pihak kepolisian. Jika terdapat masalah dalam keberjalanan layanan ini maka individu tersebut dapat melaporkan pengaduan pada Otoritas Jasa Keuangan (OJK) sebagai lembaga pengawas dari keberlangsungan layanan tersebut. Dimana salah satunya mengacu kepada ketentuan Undang-Undang Republik Indonesia Nomor 21 Tahun 2021 tentang Otoritas Jasa Keuangan pada dasarnya menyediakan layanan pengaduan, sebagaimana tertuang dalam Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 18/POJK.07/2018 tentang Layanan Pengaduan Konsumen di Sektor Jasa Keuangan. Dimana pihak yang berhadapan dengan masalah dalam penyelenggaraan

¹ Departemen Perlindungan Konsumen OJK, Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Perlindungan Konsumen Pada Fintech, (Jakarta: Departemen Perlindungan Konsumen OJK, 2017), hal. 51.

² Jeremy Zefanya Yante A., "Dampak Permasalahan Pinjaman Online dan Perlindungan Hukum bagi Konsumen Pinjaman Online", Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal, Vol. 2, No. 1, 2022, hlm. 73-87. <https://doi.org/10.15294/ipmhi.v2i1.53736>

Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) juga dapat melaporkan kepada Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI).

Di Singapura, pengawasan dan pengaturan terhadap sektor teknologi finansial (fintech) dilakukan oleh sejumlah otoritas yang berwenang. Otoritas utama yang bertindak sebagai regulator adalah Otoritas Moneter Singapura (Monetary Authority of Singapore/MAS), yang berfungsi sebagai bank sentral sekaligus lembaga pengawas seluruh sektor keuangan, mencakup perbankan, asuransi, perantara pasar modal, penasihat keuangan, hingga bursa efek.³ Regulator lain yang berada pada industri fintech seperti Info-Communications Media Development Authority of Singapore (IMDA) yang bertanggung jawab atas regulasi sector informasi dan media komunikasi dan mengambil alih tanggung jawab perlindungan data pribadi setelah bergabung dengan Infocomm dari Singapura (IDA) dan Otoritas Pengembangan Media Singapura (MDA) pada tahun 2016.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi telah resmi disahkan serta disetujui. Pengesahan ini terjadi di tengah maraknya kasus kebocoran data pribadi yang terus berlanjut. Sesuai dengan pertimbangan yang tercantum, undang-undang ini bertujuan untuk menjamin hak setiap warga negara atas perlindungan data pribadinya, meningkatkan kesadaran publik, dan menjamin pengakuan serta penghormatan akan pentingnya menjaga data pribadi. Diharapkan bahwa undang-undang ini dapat menjadi landasan hukum yang kokoh untuk pengelolaan dan perlindungan data pribadi, baik bagi warga negara maupun bagi para penyelenggara pemerintahan, guna mencegah potensi pelanggaran privasi di masa mendatang.⁴ Melihat hal tersebut ini membuktikan bahwa Singapura sendiri memiliki tingkat keamanan siber yang lebih tinggi dibanding Indonesia sendiri dan menjadikan indikator dari keberhasilan dari perlindungan data pribadi yang dilakukan oleh negara.

Dari latar belakang tersebut dapat dirumuskan beberapa rumusan permasalahan sebagai berikut :

1. Bagaimana perbandingan pengaturan dari Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) tentang data pribadi di negara Indonesia dan Singapura.?
2. Bagaimana bentuk pertanggungjawaban perlindungan data pribadi dari Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) ditinjau dari Undang - Undang Perlindungan Data Pribadi No 27 Tahun 2022.?

II. METODE PENELITIAN

Metode pendekatan yang digunakan adalah metode pendekatan yuridis normative yaitu salah satu jenis metodologi penelitian hukum yang mendasarkan analisisnya kepada peraturan perundang-undangan yang berlaku serta relevan

³ Monetary Authority of Singapore, "About MAS", <http://www.mas.gov.sg/AboutMAS.aspx>

⁴ Lina Miftahul Jannah, FIA UI, 21 September 2022, "Undang-Undang Perlindungan Data Pribadi dan Tantangan Implementasinya", <https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/> diakses pada 9 Januari 2025

dengan permasalahan hukum yang menjadi fokus penelitian dengan hubungannya dalam penerapan peraturan-peraturan hukum dalam prakteknya di lapangan. Yuridis normatif memiliki pokok kajian berupa hukum yang dikonsepkan sebagai norma atau suatu kaidah yang berlaku di masyarakat yang menjadi acuan perilaku setiap orang penelitian ini akan berfokus pada inventarisasi hukum positif, asas-asas dan doktrin hukum, penemuan hukum dalam perkara in concreto, sistematika hukum, taraf sinkronisasi hukum, perbandingan hukum, dan juga sejarah hukum penelitian dengan hubungannya dalam penerapan peraturan-peraturan hukum pada prakteknya di lapangan. Yuridis normatif memiliki pokok kajian berupa hukum yang dikonsepkan sebagai norma atau kaidah yang berlaku di dalam masyarakat dan menjadi acuan perilaku setiap orang penelitian ini akan berfokus pada inventarisasi hukum positif, asas-asas dan doktrin hukum, penemuan hukum dalam perkara in concreto, sistematika hukum, taraf sinkronisasi hukum, perbandingan hukum, dan juga sejarah hukum bahan-bahan yang akan digunakan dalam penelitian ini akan dikumpulkan melalui mengumpulkan data dan informasi melalui mencari tulisan, buku, jurnal, aturan perundang - undangan yang mengatur, dilakukan dengan menelaah sumber-sumber yang disebutkan diatas agar penelitian ini bisa menemukan solusi yang dibutuhkan.⁵

Penelitian ini menggunakan penelitian deskriptif-analitis bertujuan untuk dapat menggambarkan secara sistematis dan akurat serta melihat karakteristik pada bidang tertentu yaitu dengan menggambarkan peraturan perundang-undangan yang berlaku dihubungkan dengan teori-teori hukum dan praktek pelaksanaan hukum positif yang berkaitan dengan permasalahan yang diangkat. Data yang akan dikumpulkan murni bersifat deskriptif sehingga tidak dimaksudkan untuk menguji hipotesis serta digunakan nya jenis spesifikasi ini terkait akan judul penelitian yang akan dilaksanakan yaitu ANALISIS YURIDIS PERLINDUNGAN DATA PRIBADI DALAM OPERASIONAL Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) dimana penulis akan berusaha meng gambarkannya secara sistematis dan akurat agar bisa mendapatkan penjelasan yang deskriptif.

Dalam penelitian ini , data adalah bagian yang penting dalam proses penelitian, karena data yang akurat diperlukan agar penelitian dapat dilakukan dengan jelas. Terdapat dua jenis sumber data yang digunakan, yaitu sumber data primer dan data sekunder. Adapun bahan hukum primer (Undang-Undang Dasar Republik Indonesia Tahun 1945), (Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen), (Kitab Undang-Undang Hukum Perdata), (Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi), (*Personal Data Protection Act 2012*), (*Personal Data Protection Act No.40 of 2020*).

Adapun bahan hukum sekunder (Hasil karya ilmiah), (Tulisan atau pendapat-pendapat hukum dari para sarjana), (Buku-buku yang disusun oleh para pakar hukum), (Bahan Hukum Tersier)

Metode yang digunakan untuk mengumpulkan data dalam penelitian ini adalah studi kepustakaan. Penulis akan melakukan metode pengumpulan data yang diarahkan kepada pencarian data dan informasi melalui dokumen-dokumen, jurnal

⁵ Ronny Haniatjo Soemitro, *Metode Penelitian Hukum dan Jurimetri*, (Jakarta: PT Ghalia Indonesia, 1990)

ataupun buku, yang dapat mendukung dalam proses penelitian dan disertakannya peraturan perundang-undangan yang berkaitan dengan penelitian atau bahan hukum lainnya yang sesuai.

Metode deskriptif kualitatif digunakan untuk dapat menganalisis data primer dan sekunder penelitian dicatat tipe data dengan mempertimbangkan penerapannya dalam peraturan perundang-undangan yang berkaitan dengan topik penelitian. Selanjutnya, hukum positif digunakan untuk menganalisis data secara interpretatif, dan kesimpulan ditarik untuk menjawab masalah kemudian data tersebut membentuk uraian atau laporan yang terperinci.

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

1. Kasus Kebocoran Data Pribadi Pada Negara Indonesia dan Singapura

a) Kasus kebocoran data pribadi di Indonesia

K kerap terjadi di Indonesia menunjukkan seberapa rentan dan seriusnya masalah dalam sistem pengelolaan data di Indonesia. Jumlah insiden kebocoran data di Indonesia telah meningkat secara signifikan dalam beberapa tahun terakhir dengan jumlah ribuan hingga jutaan data pengguna dalam berbagai dalam berbagai sektor seperti e-commerce, perbankan, hingga layanan Kesehatan dimana terjadinya kebocoran data mengarah pada data tersebut diperjualbelikan di pasar gelap dunia maya. Menurut laporan Surshark sendiri, negara Indonesia menempati peringkat ke-13 secara global dalam hal jumlah kebocoran data, dengan total 156,8 juta data yang bocor terhitung sejak 2004 hingga 15 April 2024. Kebocoran data pribadi yang terjadi dalam perusahaan fintech sendiri berlangsung pada Cermati dengan total 2,9 juta data pengguna berupa akun email, kata sandi, nama, alamat, nomor telepon, bank, nomor pajak, NIK, jenis kelamin, perusahaan, dan paling terpenting adalah nama dari ibu kandung. Data pribadi ini diperjual belikan pada laman situs dark web atau pasar gelap dengan harga berkisar US\$500 hingga US\$100.000. Pada bisnis fintech sendiri dalam sistem peer to peer lending sendiri tidak terlepas dari kebocoran data dimana pada tahun 2020 mengalami kebocoran data oleh KreditPlus disebutkan oleh firma keamanan siber asal Amerika Serikat Cyble mengalami kebocoran data pribadi sebanyak 890.000 nasabah yang terdiri dari nama, alamat e-mail, kata sandi, alamat rumah, nomor telepon, data dari pekerjaan serta perusahaan, data kartu keluarga (KK) yang dijual dengan harga sekitar Rp 50.000 oleh oknum Raidforums dengan nickname "ShinyHunters".⁶

b) Kasus Kebocoran data pribadi pada negara Singapura Singapura Sebagai salah satu negara maju di Asia Tenggara mempunyai masalah dalam

⁶ Kompas.com, "KreditplusAkuiKebocoranDataPengguna", dalam <https://tekno.kompas.com/read/2020/08/05/06370007/kreditplus-akui-kebocoran-datapengguna>.

urusan kebocoran data pribadi dimana sistem pembayaran yang berinovasi memiliki celah dalam kerjanya Hal tersebut dapat diupayakan agar kebocoran data pribadi tidak terjadi dengan upaya preventif, namun dalam aktivitas pembayaran teknologi terdapat insiden yang terjadi dimana pada periode waktu 2024-2025 terdapat insiden kebocoran data pribadi yang melibatkan masyarakat Singapura dimana jumlah dari laporan kebocoran data pribadi berjumlah lebih dari 11.000 nasabah dua bank besar, yaitu DBS Bank of China (BoC) menjadi target serangan siber terhadap pihak ketiga yang digunakan oleh kedua bank tersebut, yaitu perusahaan pencetakan dan distribusi dokumen Bernama Toppan Next Tech (TNT) dimana TNT selaku vendor eksternal yang menangani pencetakan dan pengiriman komunikasi fisik dari nasabah yang menjadi korban serangan ransomware yang berhasil menembus sistem mereka dan menyebarkan informasi pribadi dari nasabah kedua bank tersebut dimana insiden ini menyoroiti tantangan yang besar dalam pengelolaan data pribadi khususnya data yang dikelola atau disimpan oleh pihak ketiga.⁷

2. Pertanggungjawaban Perlindungan Data Pribadi di Indonesia dan Singapura

- a) Pertanggungjawaban perlindungan data pribadi pemerintah Indonesia
Pemerintah Indonesia sendiri mempunyai sebuah sistem dalam menanggulangi data pribadi dimana sistem ini adalah semua perangkat keras dan lunak sebagai penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi atau penghubung, dan perangkat elektronik lainnya.

Apabila merujuk pada Undang-Undang Perlindungan Data Pribadi (UU PDP), tanggung jawab pemerintah atas terjadinya kebocoran data pribadi dikategorikan sebagai tanggung jawab dari pengendali data pribadi yang berbentuk oleh badan publik. Pengendali data pribadi merupakan individu, badan publik, atau organisasi internasional yang secara mandiri maupun bersama-sama bertanggung jawab dalam melakukan pemrosesan data pribadi atas nama pengendali data. Pengendali data memiliki kewajiban untuk mencegah terjadinya kebocoran data pribadi dengan menjamin keamanan informasi tersebut dari akses dan pengungkapan yang tidak sah, penyalahgunaan, perusakan, maupun penghapusan data tanpa izin. Jika terjadinya kebocoran data pribadi , maka pengendali data pribadi wajib

⁷ The Straits Times. (2024, April 6). *More than 11,000 DBS, Bank of China customers' information compromised after data attack on vendor*. The Straits Times.
<https://www.straitstimes.com/singapore/more-than-11000-dbs-bank-of-china-customers-information-compromised-after-data-attack-on-vendor>.

menyampaikan pemberitahuan secara tertulis paling lambat 3x24 jam kepada pengguna dan lembaga yang menyelenggarakan data pribadi.⁸

- b) Pertanggungjawaban perlindungan data pribadi pemerintah Singapura
- Pada negara Singapura sendiri permasalahan yang hadapi cukup kompleks dalam pengelolaan data pribadi terkhusus pada sektor public yang menyimpan data warga negara yang berjumlah jutaan data pribadi. Berdasarkan pelaporan pada 1 April 2022 hingga 31 maret 2023 laporan yang disusun sebagai bentuk pertanggungjawaban terhadap rekomendasi yang diberikan oleh Public Sector Data Security Review Committee (PSDSRC) pada tahun 2019 terdapat nya 182 insiden dari data pribadi selama periode pelaporan tersebut. Permasalahan yang dihadapi oleh pemerintah singapura juga dalam hal penerapan dari infrastruktur teknologi yang memadai secara merata dan meningkatkan kapasitas sumber daya manusia agar mampu memahami pentingnya keamanan data dalam menjalankan tugas pelayanan publik. Untuk mengatasi permasalahan tersebut pemerintah Singapura mempunyai langkah insentif dimana terbagi dalam tiga pendekatan utama yaitu teknologi, kebijakan, dan edukasi. Salah satu langkah inovatif yang diambil adalah peluncuran Central Privacy Toolkit pada Maret 2023 dimana toolkit ini merupakan portal swalayan yang memungkinkan pegawai dari pemerintah untuk menerapkan Teknik peningkatan privasi terhadap dataset yang mereka gunakan dengan bertujuan menjaga nilai guna data pribadi untuk keperluan analisis dan pelayanan, tanpa mengorbankan perlindungan terhadap informasi pribadi. Selain dari itu pemerintahan Singapura juga menyelesaikan penerapan sistem Whole-of-Government Data Loss Protection (DLP) pada semua perangkat laptop yang digunakan oleh pegawai pemerintah. DLP sendiri berfungsi sebagai alat pencegahan kehilangan data atau kebocoran informasi penting secara tidak disengaja dimana hal ini merupakan bentuk pertanggungjawaban bersifat preventif berbasis teknologi yang secara aktif melindungi data dalam keseharian pekerjaan birokrasi. Langkah yang ditetapkan oleh pemerintah Singapura menunjukan bentuk pertanggungjawaban hukum dan administrative yang konkret dalam melindungi data pribadi warga negara. Pelaporan berkala yang disusun secara transparan memperlihatkan akuntabilitas dalam tata Kelola data pribadi. Penurunan yang terjadi dalam tingkat keparahan insiden menunjukan peningkatan pengguna teknologi protektif, serta kesadaran dan kompetensi SDM yang ditingkatkan secara aktif menjadi

⁸ Nafiatul Munawaroh, "Tanggung Jawab Pemerintah atas Kebocoran Data Pribadi," Hukumonline.com, 9 Juni 2023, <https://www.hukumonline.com/klinik/a/tanggung-jawab-pemerintah-atas-kebocoran-data-pribadi-lt66881c826cc33/>.

bukti bahwa pendekatan secara holistic yang digunakan pemerintah Singapura membuahkan hasil.⁹

B. Pembahasan

1. Perbandingan pengaturan dari Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) tentang data pribadi di negara Indonesia dan Singapura

a) Pengaturan Perlindungan Data Pribadi pada sistem *peer to peer lending* di Indonesia

Penggunaan serta berkembangnya teknologi informasi yang terus naik pesat menimbulkan dampak yang begitu besar terhadap berbagai sektor terutama pada sektor keuangan. Pada negara Indonesia perlindungan data pribadi telah menjadi fokus yang di perhatikan oleh pemerintah dimana munculnya beberapa peraturan perundang-undangan yang diatur pada Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan data pribadi Indonesia, Peraturan Otoritas Jasa Keuangan No. 10/POJK.05/2022 tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi, dan Undang- Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang- Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Namun peraturan yang mengatur tentang perlindungan data pribadi yang ada di Indonesia sendiri bersifat sektoral karena memiliki pemahaman serta definisi yang berbeda antara satu peraturan dengan peraturan lainnya. Dengan disahkan nya Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi diharapkan menjadi satu payung hukum bagi masyarakat Indonesia. Penyelenggara Sistem Elektronik (Sertifikat PSE) sebagai syarat untuk menjalankan operasional usahanya. Ketentuan ini diatur dalam Pasal 8 ayat (3) huruf (e) Peraturan Otoritas Jasa Keuangan (POJK) No. 77 Tahun 2016, yang merujuk pada Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Sertifikat tersebut berlaku selama lima tahun dan berfungsi sebagai bukti bahwa suatu entitas telah terdaftar sebagai Penyelenggara Sistem Elektronik. Selain itu, Peraturan Pemerintah No. 82 Tahun 2012 juga memuat ketentuan mengenai data pribadi, yang didefinisikan sebagai informasi perseorangan tertentu yang harus disimpan, dipelihara, dijaga keakuratannya, dan dilindungi kerahasiaannya. Dalam hal ini, perolehan dan pengumpulan data pribadi oleh penyelenggara sistem elektronik wajib dibatasi hanya pada informasi yang relevan, memiliki tujuan yang jelas, serta dilakukan secara akurat dan sesuai kebutuhan. Khususnya dalam konteks peer-to-peer lending, pengumpulan data pribadi calon

⁹ Smart Nation and Digital Government Office, "Fourth Update on the Government's Personal Data Protection Efforts," 31 Juli 2023, <https://www.mddi.gov.sg/media-centre/press-releases/31072023/>.

penerima pinjaman harus dibatasi pada informasi yang relevan dan proporsional dengan tujuan transaksi elektronik, yakni untuk melakukan analisis kelayakan dalam pemberian pinjaman.

Penyelenggara layanan peer-to-peer lending juga diwajibkan untuk memperoleh sertifikasi Sistem Manajemen Pengamanan Informasi, sebagaimana diatur dalam Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Dalam regulasi tersebut, juga diatur mengenai perlindungan data pribadi, yakni data individu tertentu yang harus disimpan, dipelihara, dijaga keakuratannya, serta dilindungi kerahasiaannya. Definisi data pribadi dalam peraturan ini sejalan dengan pengertian yang tercantum dalam Peraturan Pemerintah No. 82 Tahun 2012 dan Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016, sehingga membentuk keselarasan norma dalam perlindungan data pribadi pada sistem elektronik.

b) Pengaturan Perlindungan Data Pribadi pada sistem *peer to peer lending* di Singapura

Model bisnis yang memungkinkan pemberi pinjaman dan seorang peminjam bertemu secara langsung melalui platform digital tanpa intermediasi dari lembaga keuangan tradisional. Namun tidak dapat dipungkiri model dari transaksi ini menyimpan banyak risiko hukum yang di antaranya adalah terancamnya keamanan data. Setiap proses verifikasi, penilaian risiko ataupun pencairan dana mengharuskan seorang pengguna untuk menyerahkan sejumlah besar data pribadi. Berawal dari data identitas informasi keuangan, hingga rekam jejak kredit pengguna dimana data data tersebut bersifat krusial dan sangat penting untuk dijaga oleh seorang pemilik data. Oleh karena hal tersebut yang sangat mengancam data pribadi pengguna dan sangat merugikan perlindungan data pribadi dalam peer to peer lending menjadi isu krusial yang wajib diatur secara ketat oleh hukum dari pemerintah Singapura yang mengeluarkan *Personal Data Protection Act (PDPA) Singapura dan kebijakan dari Monetary Authority of Singapore (MAS)*.

Pada negara Singapura sendiri pemerintah Singapura sudah terlebih dahulu menanggapi perihal data pribadi dimana pembentukan dari Undang-Undang Perlindungan Data Pribadi sudah terbentuk pada Oktober 2012 dan diberlakukan pada 2013 lalu. Berbeda dengan Indonesia yang baru disahkan pada 17 Oktober tahun 2022. Pembentukan daripada Undang-Undang Perlindungan Data Pribadi merupakan bentuk dalam melakukan perlindungan data pribadi oleh pemerintah Singapura dimana hal ini merupakan dorongan untuk mencapai era digitalisasi yang mempunyai informasi pribadi yang penting bagi masyarakat itu sendiri

dari hal tersebut terbentuk nya Undang-Undang *Personal Data Protection Act 2012*.¹⁰

Jika dibandingkan peraturan mengenai perlindungan data pribadi di negara Indonesia dan Singapura maka dapat dilihat bahwa Indonesia dan Singapura mempunyai rujukan yang sama mengenai data pribadi karena mengikuti perkembangan dari pengaturan yang berada di Eropa yaitu *General Data Protection Regulation* dan mengikuti perkembangan dari *European union dan Organisation for Economic Cooperation and Development (OECD)*. Perbedaan yang terdapat di negara Indonesia dan Singapura adalah bagian hak penggunaan dan pengguna dianggap telah memberikan izin penggunaan data pribadi. Dimana pada undang-undang di negara Singapura hal tersebut diatur pada undang-undang perlindungan data pribadi di Singapura berbeda dengan undang-undang perlindungan data pribadi di Indonesia dimana hal tersebut tidak diatur.

2. Bentuk pertanggungjawaban perlindungan data pribadi dari Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) ditinjau dari Undang - Undang Perlindungan Data Pribadi No 27 Tahun 2022

Dengan kemajuan dalam sektor keuangan mempunyai banyak tantangan dari hal tersebut diantaranya adalah data pribadi yang menjadi masalah utama dari transaksi berbasis teknologi informasi yang mewajibkan pengguna untuk memasukkan data pribadi. Dengan keberadaan *fintech* mendatangkan proses transaksi keuangan meliputi pembayaran, pinjaman uang, transfer, ataupun jual beli saham.¹¹

a) Pertanggungjawaban data pribadi dalam Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Pertanggungjawaban hukum muncul akibat adanya perbuatan melawan hukum yang bertentangan dengan kewajiban dari hukum seorang pelaku atau melanggar hak dari subjektif seseorang, atau melanggar kaidah yang bertentangan dari asas kepatutan, ketelitian serta sikap hati-hati dalam pergaulan hidup masyarakat.¹²

¹⁰ Warren B. Chik, "The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform", *Computer Law & Security Review*, Vol. 29, Issue 5, ScienceDirect, 2013, hlm. 555 <https://doi.org/10.1016/j.clsr.2013.07.010>

¹¹ Berry A. Harahap, et al., *Perkembangan Financial Technology Terkait Central Bank Digital Currency (CBDC) Terhadap Transmisi Kebijakan Moneter dan Makroekonomi*, Working Paper Departemen Kebijakan Ekonomi dan Moneter (DKEM), Bank Indonesia, 2017, <https://www.bi.go.id/id/publikasi/wp/Documents/WP-2-2017.pdf>

¹² Andria Luhur Prakoso, "Prinsip Pertanggungjawaban Perdata Dalam Perspektif Kitab Undang Undang Hukum Perdata Dan Undang Undang Nomor 32 Tahun 2009 tentang Perlindungan Dan Pengelolaan Lingkungan Hidup", Makalah disampaikan dalam Prosiding Seminar Nasional Tanggung Jawab Pelaku Bisnis dalam Pengelolaan Lingkungan Hidup, Kementerian Lingkungan Hidup dan Kehutanan World Wide Fund (WWF), Universitas Muhammadiyah Surakarta, Surakarta 5 Maret 2016, hlm.214

Subjek hukum yang dapat dimintai pertanggungjawaban dalam hal ini dapat diklasifikasikan kepada dua kategori yaitu:¹³

1) Tindakan yang dilakukan terhadap diri sendiri yang mengakibatkan kerugian, baik secara fisik (materiel) maupun nonfisik (immateriel), seperti luka atau cacat tubuh, dapat disebabkan oleh kesengajaan atau kelalaian pihak lain. Dalam hal demikian, pihak yang dirugikan berhak menuntut ganti rugi sesuai dengan ketentuan perundang-undangan yang berlaku.

2) Tindakan yang dikenakan terhadap badan hukum umumnya didasarkan pada kesalahan yang dilakukan oleh organ perusahaan, seperti direksi, komisaris, atau rapat umum pemegang saham. Namun, tindakan tersebut hanya dapat dipertanggungjawabkan apabila terdapat hubungan kausal yang jelas antara perbuatan yang dilakukan dan ruang lingkup tugas serta wewenang organ yang bersangkutan.

Undang-Undang No 27 Tahun 2022 tentang Perlindungan Data Pribadi memberikan pengguna hak untuk melaporkan masalah mereka kepada lembaga perlindungan data pribadi agar masalah dapat ditangani dan pengguna memiliki hak untuk diberitahu atas terjadinya kebocoran data pribadi oleh penyelenggara.

b) Bentuk sanksi atau hukuman menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

. Pemerintah Indonesia sendiri dalam merespon ancaman hilangnya data pribadi tersebut dengan mengesahkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Meskipun undang-undang tersebut telah diberlakukan, hingga saat ini belum terbentuk lembaga yang bertanggung jawab untuk mengawasi dan menjamin keamanan data.¹⁴

Sanksi yang dijatuhkan apabila penyelenggara terbukti gagal dalam melindungi data pribadi diberikan putusan pidana berupa denda. Apabila denda tersebut tidak dapat dibayarkan maka akan dilakukan lelang oleh jaksa terhadap harta kekayaan perusahaan atau dilakukan hukuman kurungan penjara sesuai dengan ancaman tindak pidana yang diputuskan oleh hakim dalam putusan pengadilan sebagaimana disebutkan dalam pasal 71. Tidak hanya pelelangan tetapi juga pembekuan juga dilakukan hal ini disebutkan pada pasal 72 dimana pembekuan dilakukan kepada pihak penyelenggara apabila tidak dapat melunasi denda dengan jangka waktu lima tahun oleh hakim dalam putusan pengadilan yang tidak lupa bahwa pembekuan juga berlaku untuk kegagalan dalam pembayaran ganti rugi.

IV. KESIMPULAN

¹³ Neng Yani Nurhayani, Hukum Perdata, Ctk. Pertama, CV.Pustaka Setia, Bandung, 2015, hlm. 260-261

¹⁴ Azza Fitrahul Faizah et al., "Penguatan Perlindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura," Hakim: Jurnal Ilmu Hukum dan Sosial1, no. 3 (2023), hlm.7 , <https://doi.org/10.51903/hakim.v1i3.1222>

Perlindungan pengaturan data pribadi dari Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) tentang data pribadi di negara Indonesia dan Singapura menunjukkan bahwa kedua negara telah mengambil langkah signifikan dalam mengatur perlindungan data pribadi meskipun dalam keberjalanannya terdapat perbedaan mendasar dalam pendekatan dan implementasi peraturan kepada penyelenggara maupun konsumen individu. Pada negara Indonesia sendiri perlindungan data pribadi diatur melalui berbagai peraturan sektoral yang bersifat spesifik, dengan telah disahkan nya Undang-Undang No. 27 Tahun 2022 sebagai payung hukum yang diharapkan dapat menyatukan berbagai regulasi yang ada. Undang-undang ini menekankan pentingnya persetujuan eksplisit dari individu sebelum pemrosesan data pribadi dilakukan, serta menetapkan tanggung jawab bagi pengendali data untuk menjaga kerahasiaan dan keamanan data pribadi. Perbandingan antara kedua negara menunjukkan bahwa Singapura lebih fokus pada organisasi dan bisnis dalam pengaturan perlindungan data, sedangkan Indonesia memberikan hak yang lebih luas kepada individu terkait akses dan penghapusan data pribadi. Jika melihat keseluruhan kedua negara mengikuti perkembangan global dalam perlindungan data pribadi, perbedaan dalam pendekatan dan implementasi mencerminkan konteks hukum dan social masing-masing negara. Hal ini menunjukkan perlunya penyesuaian dan pengembangan lebih lanjut dalam regulasi perlindungan data pribadi di Indonesia untuk meningkatkan kepercayaan masyarakat dan keamanan data di era digital. Kesimpulan diuraikan dalam bentuk paragraf, tidak dalam bentuk numerik.

Bentuk pertanggungjawaban perlindungan data pribadi dari Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) ditinjau dari Undang-Undang No.27 Tahun 2022 memberikan kerangka hukum yang jelas untuk melindungi data pribadi pengguna dalam layanan *peer to peer lending* pengguna memiliki hak untuk melaporkan pelanggaran dan mendapatkan informasi terkait kebocoran data pribadi dan penyelenggara Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) bertanggung jawab untuk menjaga dan melindungi keamanan data pribadi dan wajib mengambil langkah-langkah pencegahan serta penanganan jika terjadi kebocoran data. Kewajiban dari penyelenggara mencakup pengelolaan data pribadi termasuk penghapusan dan pemusnahan data sesuai permintaan pengguna. Kegagalan dalam melindungi data pribadi dapat mengakibatkan sanksi pidana dan administratif, termasuk denda yang signifikan. Selain itu terdapat sanksi administratif yang dapat berupa peringatan, larangan pemrosesan data, dan penghapusan data. Undang-Undang No.27 Tahun 2022 memberikan kepastian hukum bagi pengguna dan penyelenggara dalam pengelolaan data pribadi, serta menetapkan mekanisme sanksi yang tegas untuk memastikan perlindungan data pribadi dalam ekosistem *fintech*.

V. DAFTAR PUSTAKA

A. Buku



Ronny Haniatjo Soemitro.

Metode Penelitian Hukum dan Jurumetri. Jakarta: PT Ghalia Indonesia, 1990.

Neng Yani Nurhayani.

Hukum Perdata. Cetakan Pertama. Bandung: CV. Pustaka Setia, 2015, hlm. 260–261.

B. Jurnal

Andria Luhur Prakoso.

“Prinsip Pertanggungjawaban Perdata Dalam Perspektif Kitab Undang-Undang Hukum Perdata Dan Undang-Undang Nomor 32 Tahun 2009 tentang Perlindungan Dan Pengelolaan Lingkungan Hidup.”

Makalah disampaikan dalam *Prosiding Seminar Nasional Tanggung Jawab Pelaku Bisnis dalam Pengelolaan Lingkungan Hidup*, Kementerian Lingkungan Hidup dan Kehutanan, WWF, Universitas Muhammadiyah Surakarta, 5 Maret 2016, hlm. 214.

Berry A. Harahap, et al.

Perkembangan Financial Technology Terkait Central Bank Digital Currency (CBDC) terhadap Transmisi Kebijakan Moneter dan Makroekonomi.

Working Paper Departemen Kebijakan Ekonomi dan Moneter, Bank Indonesia, 2017.

<https://www.bi.go.id/id/publikasi/wp/Documents/WP-2-2017.pdf>

C. Peraturan dan Keputusan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Kitab Undang-Undang Hukum Perdata (KUHPer)

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Peraturan Otoritas Jasa Keuangan No 10 /POJK.05/2022 Tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi