

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era *digital* saat ini, data pribadi telah menjadi salah satu aset berharga, khususnya dalam sektor pembiayaan konsumen. Data pribadi mencakup informasi tentang individu tertentu yang harus disimpan, dikelola, serta dijaga keakuratannya dan kerahasiaannya oleh perusahaan pembiayaan. Berangkat dari Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 35/POJK.05/2018 Tahun 2018 tentang Penyelenggaraan Usaha Perusahaan Pembiayaan¹ (untuk selanjutnya disebut “POJK 35/2018”) pada Pasal 1, perusahaan pembiayaan didefinisikan sebagai badan usaha yang menyelenggarakan kegiatan pembiayaan untuk barang dan/atau jasa. Dan, Pasal 2 ayat (1) huruf c mengatur bahwa salah satu bidang usahanya mencakup pembiayaan multiguna (untuk selanjutnya disebut “Perusahaan Pembiayaan”).

Tahun 1970-an, Jerman dan Swedia menjadi negara pertama yang mengatur perlindungan data pribadi melalui perundang-undangan.² Perusahaan Pembiayaan, sebagai penyedia layanan keuangan, secara rutin mengumpulkan dan mengelola data pribadi Pengguna untuk berbagai keperluan operasional, termasuk verifikasi identitas, penilaian kredit, dan pengelolaan transaksi. Data yang dikumpulkan mencakup informasi sensitif, seperti nama, alamat, nomor

¹ Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 35/POJK.05/2018 Tahun 2018 tentang Penyelenggaraan Usaha Perusahaan Pembiayaan

² Dian Laksmi Dewi, Cokorde Istri; Rudin, Denny; Tungga, Benyamin. “Perjanjian Kerahasiaan Bagi Karyawan Pengelola Data Pribadi Perusahaan.” *Jurnal Kertha Patrika*, vol. 46, no. 2, 2024, hal. 127-142.

telepon, hingga data keuangan pribadi. Dengan meningkatnya digitalisasi, muncul juga risiko yang signifikan terhadap keamanan dan privasi data pribadi ini.

Risiko tersebut mencakup potensi pencurian identitas, penipuan, atau eksploitasi lainnya yang dapat merugikan individu. Dalam beberapa kasus, informasi pribadi yang bocor dapat digunakan oleh pihak tidak bertanggung jawab untuk melakukan tindakan ilegal, seperti membuka rekening palsu atau melakukan penipuan finansial. Di Indonesia, kasus kebocoran data telah meningkat secara signifikan, dengan laporan bahwa pada kuartal II (dua) tahun 2022 saja terdapat 1,04 juta akun pribadi yang mengalami kebocoran.³ Dalam konteks ini, Perusahaan tidak hanya memiliki tanggung jawab moral untuk melindungi data tersebut tetapi juga memiliki kewajiban hukum sesuai dengan peraturan yang berlaku. Masyarakat sebagai Pengguna layanan sering kali tidak menyadari risiko yang ada. Mereka memberikan data pribadi kepada perusahaan tanpa memahami sepenuhnya bagaimana data tersebut akan digunakan, siapa yang memiliki akses, dan langkah-langkah perlindungan yang diterapkan.

Kondisi ini menuntut adanya kesadaran yang lebih tinggi mengenai pentingnya perlindungan data pribadi. Pada tahun 2022, Dewan Perwakilan Rakyat Republik Indonesia (DPR RI) telah mengesahkan Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (untuk selanjutnya disebut “UU No. 27/2022”)⁴ sebagai langkah untuk memberikan keamanan dan perlindungan kepada masyarakat. Namun, meskipun regulasi telah ada, tantangan tetap muncul

³ Cloud Raya, “Waspada! Kebocoran Data Dampak, Penyebab, dan Cara Mencegahnya”, <https://cloudraya.com/blog/waspada-kebocoran-data/>, diakses pada 22 November 2024

⁴ Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi

dalam implementasinya. Banyak Pengguna tidak menerapkan praktik keamanan yang baik dalam berbagi informasi pribadi di dunia maya.

Di sisi lain, Perusahaan Pembiayaan perlu menerapkan kebijakan privasi yang transparan dan efektif untuk membangun kepercayaan dengan Pengguna. Mereka harus melakukan penilaian risiko secara berkala dan menerapkan langkah-langkah mitigasi untuk melindungi data sensitif dari ancaman siber. Dengan pendekatan yang proaktif dalam manajemen privasi data, perusahaan dapat mengurangi risiko pelanggaran privasi dan meningkatkan reputasi mereka di mata publik.

Kesadaran akan pentingnya perlindungan data pribadi di era *digital* harus ditingkatkan baik di kalangan masyarakat maupun Perusahaan. Hanya dengan kolaborasi antara Pengguna dan penyedia layanan keuangan dapat tercipta lingkungan yang aman bagi pengelolaan data pribadi.

Dalam operasionalnya, Perusahaan Pembiayaan sering kali melibatkan pihak ketiga, seperti penyedia layanan teknologi atau *vendor* analitik (untuk selanjutnya disebut “Pihak Ketiga”), untuk mendukung pengelolaan data Pengguna. Pihak Ketiga ini berfungsi sebagai *Data Processor*, yang memproses data atas nama Perusahaan Pembiayaan yang bertindak sebagai *Data Controller*. Hubungan antara kedua pihak ini diatur dalam Kontrak bisnis yang seharusnya mencakup aspek-aspek penting perlindungan data, termasuk tanggung jawab masing-masing pihak dalam menjaga keamanan dan kerahasiaan data pribadi.

Hubungan hukum antara Perusahaan Pembiayaan dan Pihak Ketiga yang memproses data pribadi diatur melalui Kontrak bisnis yang seharusnya mencerminkan tanggung jawab dan kewajiban kedua pihak dalam melindungi

data Pengguna. Kontrak ini berfungsi sebagai landasan hukum yang mengikat, menetapkan hak dan kewajiban masing-masing pihak dalam konteks pengelolaan data.

Namun, dalam banyak kasus, Kontrak ini tidak disusun secara komprehensif. Mengingat bahwa dalam menyusun kontrak pemrosesan data pribadi (untuk selanjutnya disebut “Kontrak”), terdapat batasan yang tegas, seperti larangan untuk menyusun Kontrak terkait bisnis perjudian online, pornografi, narkoba, dan tindak kejahatan lainnya. Sebagaimana dinyatakan dalam Pasal 55 UU No. 27/2022, yang mengatur bahwa Perusahaan dapat melakukan transfer data pribadi kepada Pihak Ketiga, dengan setiap transfer data pribadi lintas batas yang terjadi atas Kerjasama yang dilakukan Perusahaan dengan Pihak Ketiga harus dilakukan dengan memperhatikan prinsip transparansi dan akuntabilitas.

Selain itu, di sektor keuangan, penawaran produk tidak boleh dilakukan tanpa persetujuan eksplisit dari konsumen. Meskipun di sektor lain penawaran produk dapat dilakukan berdasarkan pemrosesan kepentingan yang sah, sektor industri keuangan memiliki ketentuan khusus yang melarang penawaran produk tanpa persetujuan langsung dari subjek data, sesuai dengan POJK No. 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Keuangan. Oleh karena itu, penting untuk mencantumkan dasar pemrosesan persetujuan secara eksplisit dalam Kontrak agar Kontrak tersebut tidak menjadi batal akibat absennya alasan yang sah, terutama jika terjadi pemrosesan data untuk penawaran produk tanpa persetujuan konsumen di sektor industri keuangan.⁵

⁵ Awaludin Marwan,, “Dinamika Kontrak Pelindungan Data Pribadi”, <https://privasimu.com/blogs/dinamika-Kontrak-pelindungan-data-pribadi>, diakses pada 22 November 2024

Meskipun setelah diterbitkannya UU No. 27/2022 mengalami perkembangan yang cukup pesat dari sisi perlindungan, sebagian besar studi yang ada masih bersifat umum dan belum banyak yang mengulas secara spesifik mengenai struktur dan substansi perjanjian kerja sama pemrosesan data pribadi khususnya pada Perusahaan Pembiayaan. Fokus mayoritas penelitian sebelumnya masih terbatas pada perlindungan data oleh perusahaan penyedia layanan utama, tanpa menyoroti secara mendalam hubungan kerjasama hukum antara Perusahaan Pembiayaan sebagai pengendali data pribadi dan Pihak Ketiga sebagai prosesor data pribadi yang memproses data atas nama perusahaan.

Padahal, dalam praktiknya, Perusahaan Pembiayaan memiliki ketergantungan yang tinggi terhadap kerja sama dengan berbagai pihak ketiga, seperti penyedia teknologi informasi, penyedia verifikasi identitas, hingga platform analitik data. Pihak Ketiga ini kerap mengakses dan memproses data pribadi pengguna dalam kapasitasnya sebagai prosesor, namun hubungan hukumnya sering kali hanya ditopang oleh *Non-Disclosure Agreement* (NDA) yang bersifat terbatas. Sehingga menimbulkan berbagai masalah dalam perlindungan data pribadi. Beberapa kelemahan yang sering ditemukan dalam Kontrak bisnis antara Perusahaan dan Pihak Ketiga meliputi:

1. Tidak adanya klausul spesifik tentang kewajiban keamanan data, yakni dengan tidak mencantumkan ketentuan yang jelas mengenai langkah-langkah keamanan yang harus diambil oleh Pihak Ketiga untuk melindungi data pribadi. Hal ini dapat menyebabkan ketidakpastian mengenai tanggung jawab keamanan data, sehingga meningkatkan risiko kebocoran informasi.

2. Kurangnya ketentuan tentang mekanisme audit dan pelaporan, yakni tanpa adanya mekanisme audit yang jelas, Perusahaan mungkin tidak dapat memantau secara efektif bagaimana Pihak Ketiga mengelola dan melindungi data pribadi. Ketidakmampuan untuk melakukan audit dapat mengakibatkan kurangnya akuntabilitas dari Pihak Ketiga, yang berpotensi menimbulkan masalah serius jika terjadi pelanggaran.
3. Ketiadaan sanksi atau tindakan korektif, dalam klausul pada Kontrak tidak terdapat sanksi atau tindakan korektif yang jelas jika Pihak Ketiga gagal memenuhi kewajiban perlindungan data. Hal ini membuat Perusahaan kesulitan untuk menegakkan tanggung jawab hukum terhadap Pihak Ketiga jika terjadi pelanggaran.

Sejumlah penelitian hukum turut memperkuat urgensi kelemahan di atas. Menurut Devina Patricia pada tahun 2023⁶ melalui skripsinya yang berjudul *Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi dalam Pinjaman Online Ilegal Ditinjau dari Undang-Undang Perlindungan Data Pribadi*, mengungkapkan bahwa:

“Maraknya penyalahgunaan data dalam praktik pinjaman *online* ilegal sering kali dipicu oleh ketiadaan kontrak hukum yang jelas serta lemahnya mekanisme pengawasan terhadap pihak ketiga. Ketika tidak terdapat pengaturan kontraktual yang rinci, maka hak dan kewajiban antar pihak menjadi kabur, dan subjek data menjadi pihak yang paling rentan mengalami pelanggaran privasi”.

⁶ Devina Patricia, “Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi dalam Pinjaman Online Ilegal Ditinjau dari Undang-Undang Perlindungan Data Pribadi”. Skripsi, Jakarta:Program Studi Hukum Fakultas Hukum Universitas Pelita Harapan, 2023.

Kemudian, Jonathan Matthew di tahun 2024⁷, dalam penelitian jurnalnya yang berjudul Kesadaran Urgensi Peran Pengendali dan Prosesor Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, menekankan:

“Pentingnya keterlibatan aktif dari kedua belah pihak pengendali dan prosesor data pribadi dalam menyusun sistem pelindungan yang terstandarisasi dan memiliki parameter keamanan yang dapat diuji. Hal ini menjadi sangat penting mengingat beban tanggung jawab pelindungan data tidak hanya berada pada pengendali, tetapi juga pada sejauh mana prosesor dapat menjalankan pemrosesan data secara bertanggung jawab”.

Melalui kesenjangan literatur dan realitas tersebut, penelitian ini menjadi relevan karena secara langsung menempatkan fokus pada bagaimana ketentuan pelindungan data pribadi dalam UU No. 27/2022 diimplementasikan secara praktis melalui perjanjian kerja sama antara Perusahaan Pembiayaan dan Pihak Ketiga sebagai prosesor data pribadi. Penelitian ini tidak hanya mengkaji norma hukum positif yang berlaku, tetapi juga mengevaluasi substansi kontrak bisnis yang digunakan dan bagaimana kontrak tersebut dapat dijadikan sebagai instrumen untuk menjamin pelindungan hukum terhadap pengguna sebagai subjek data. Dan juga kelemahan-kelemahan sebagaimana tersebut di atas memperburuk kesenjangan pelindungan hukum terhadap data pribadi. Tanpa panduan yang jelas dalam Kontrak, Perusahaan Pembiayaan mungkin kesulitan untuk menegakkan tanggung jawab hukum Pihak Ketiga jika terjadi pelanggaran. Akibatnya,

⁷ Jonathan Matthew Pakpahan, “Kesadaran Urgensi Peran Pengendali dan Prosesor Data Pribadi dalam Rangka Pelindungan Data Pribadi Individu Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi”. Jurnal Hukum to-ra, Bandung: Universitas Padjajaran, 2024

Pengguna data berada dalam posisi yang sangat rentan terhadap penyalahgunaan informasi pribadi mereka.

Dampak dari kelemahan dalam Kontrak bisnis ini sangat signifikan. Pertama-tama, kurangnya pengaturan yang jelas dapat menyebabkan kebocoran data yang sulit terdeteksi. Ketika data pribadi jatuh ke tangan pihak yang tidak bertanggung jawab, informasi tersebut dapat disalahgunakan untuk berbagai tindakan kejahatan. Selain itu, kelemahan dalam Kontrak juga dapat mengurangi kepercayaan masyarakat terhadap Perusahaan Pembiayaan. Ketika konsumen merasa bahwa data pribadi mereka tidak dilindungi dengan baik, mereka cenderung enggan untuk menggunakan layanan dari perusahaan tersebut. Hal ini dapat berdampak negatif pada reputasi perusahaan dan keberlanjutan bisnis mereka di pasar yang semakin kompetitif.⁸

Kemudian, banyak Perusahaan Pembiayaan mungkin tidak memiliki kontrol penuh terhadap bagaimana data Pengguna dikelola oleh Pihak Ketiga. Hal ini dapat terjadi karena kurangnya transparansi dalam proses pemrosesan data atau tidak adanya mekanisme audit yang memadai untuk memastikan bahwa pemrosesan data dilakukan sesuai dengan standar hukum yang berlaku. Ketidakpastian ini membuka celah dalam perlindungan data pribadi, yang dapat mengakibatkan berbagai risiko besar.

Salah satu risiko utama adalah kebocoran data, di mana informasi sensitif dapat jatuh ke tangan pihak yang tidak bertanggung jawab. Kebocoran data telah menjadi masalah yang semakin umum di era *digital*, dengan banyak insiden yang melibatkan pencurian informasi pribadi dari berbagai lembaga. Misalnya, kasus

⁸ Jenda Ingan Mahuli, "Perlindungan Hukum Terhadap Data Pribadi dalam Era Digital", All Fields of Science Journal Liaison Academia and Society 3, no. 4, 2023, hal. 188-194.

kebocoran data besar-besaran yang melibatkan Direktorat Kependudukan dan Pencatatan Sipil (Dukcapil) menunjukkan betapa rentannya data pribadi terhadap serangan siber. Data yang bocor, seperti nama, alamat, dan Nomor Induk Kependudukan (NIK), dapat disalahgunakan untuk berbagai tujuan jahat, termasuk pengajuan pinjaman online tanpa sepengetahuan pemilik data.⁹

Selain kebocoran data, ada juga risiko penyalahgunaan data untuk tujuan komersial atau kriminal. Data pribadi yang diperoleh secara ilegal dapat digunakan untuk melakukan penipuan identitas atau bahkan untuk kegiatan kriminal lainnya. Pelaku kejahatan siber dapat menggunakan informasi ini untuk mengajukan pinjaman atau membuka rekening bank atas nama korban, merugikan individu dan merusak reputasi Perusahaan Pembiayaan.¹⁰

Dalam konteks ini, Perusahaan Pembiayaan tidak hanya bertanggung jawab secara moral untuk melindungi data Pengguna tetapi juga memiliki kewajiban hukum untuk memastikan bahwa semua Pihak Ketiga yang terlibat dalam pengolahan data mematuhi peraturan perlindungan data yang berlaku. Kegagalan dalam mengawasi dan mengendalikan Pihak Ketiga dapat mengakibatkan konsekuensi hukum serius bagi perusahaan serta kerugian finansial dan reputasi.

Salah satu prinsip utama yang diatur dalam UU No. 27/2022 adalah transparansi, yang mewajibkan perusahaan untuk memberikan informasi yang jelas dan lengkap kepada Pengguna tentang pemrosesan data pribadi mereka.

⁹ VIDA, "Dampak Negatif Internet Bagi Keamanan Data Pribadi, <https://vida.id/id/blog/dampak-negatif-internet>, diakses pada tanggal 22 November 2024

¹⁰ Pusat Operasi Keamanan Siber Nasional, "Panduan Menghadapi Data Breach", <https://www.ojk.go.id/id/csirt/Documents/Panduan%20Menghadapi%20Insiden%20Data%20Breach.pdf>, diakses pada tanggal 22 November 2024

Transparansi ini mencakup kewajiban perusahaan untuk menginformasikan Pengguna mengenai berbagai aspek penting terkait penggunaan data pribadi, termasuk siapa Pihak Ketiga yang mengelola data mereka, tujuan pemrosesan data tersebut, serta langkah-langkah yang diambil untuk melindungi data selama proses tersebut. Meskipun prinsip transparansi telah diatur secara tegas dalam UU No. 27/2022, kenyataannya, kesenjangan transparansi masih menjadi isu serius dalam praktik.

Pengguna sering kali tidak diberitahu secara spesifik mengenai Pihak Ketiga yang terlibat dalam pengelolaan data mereka. Hal ini dapat menciptakan ketidakpastian dan kekhawatiran di kalangan Pengguna mengenai siapa yang memiliki akses terhadap informasi sensitif mereka. Selain itu, tujuan Penggunaan data pribadi juga sering kali tidak dijelaskan dengan cukup rinci, sehingga Pengguna tidak dapat memahami sepenuhnya bagaimana data mereka akan dimanfaatkan. Ketidakjelasan ini berpotensi merugikan hak-hak Pengguna dan mengurangi kepercayaan masyarakat terhadap Perusahaan. Dalam jangka panjang, kurangnya transparansi dapat berdampak negatif pada reputasi perusahaan dan keberlanjutan bisnis mereka.

Lebih jauh lagi, rendahnya tingkat transparansi membatasi hak Pengguna untuk mengontrol data pribadi mereka sendiri. Pengguna memiliki hak untuk meminta penghapusan data atau memperbaiki informasi yang tidak akurat, namun tanpa adanya informasi yang jelas tentang bagaimana cara melakukannya, hak-hak ini menjadi sulit untuk diakses. Dalam konteks ini, penting untuk merujuk pada Undang Undang Dasar Negara Republik Indonesia 1945 (untuk selanjutnya

disebut “UUD NRI 1945”) ¹¹, khususnya pada Pasal 28G ayat (1) yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda. Hal ini menunjukkan bahwa perlindungan terhadap data pribadi adalah bagian integral dari hak asasi manusia.

Selain itu, Pasal 28H ayat (4) UUD NRI 1945 menegaskan bahwa setiap orang berhak untuk mendapatkan perlindungan atas diri pribadi dan identitasnya. Dengan demikian, Perusahaan harus menyadari bahwa tanggung jawab mereka tidak hanya bersifat moral tetapi juga hukum dalam melindungi data pribadi Pengguna. Kegagalan untuk memenuhi kewajiban transparansi ini dapat berakibat pada pelanggaran hak-hak konstitusional individu dan dapat memicu konsekuensi hukum bagi perusahaan.

Oleh karena itu, Perusahaan Pembiayaan perlu mengambil langkah proaktif untuk meningkatkan transparansi dalam pengelolaan data pribadi. Ini termasuk menyediakan informasi yang jelas dan mudah diakses mengenai kebijakan privasi mereka, menjelaskan dengan rinci bagaimana data akan digunakan dan dilindungi, serta memastikan bahwa semua Pihak Ketiga yang terlibat dalam pemrosesan data mematuhi standar perlindungan yang ditetapkan oleh UU No. 27/2022. Dengan langkah-langkah ini, perusahaan tidak hanya akan memenuhi kewajiban hukum mereka tetapi juga membangun kepercayaan dengan Pengguna serta menciptakan lingkungan bisnis yang lebih berkelanjutan dan bertanggung jawab.

Selain aspek transparansi, pengawasan terhadap Pihak Ketiga juga merupakan tantangan besar dalam perlindungan data pribadi. UU No. 27/2022

¹¹ Undang Undang Dasar Negara Republik Indonesia 1945

menetapkan bahwa Perusahaan Pembiayaan sebagai *Data Controller* bertanggung jawab untuk memastikan bahwa Pihak Ketiga yang mereka tunjuk untuk memproses data mematuhi standar keamanan dan perlindungan data yang berlaku. Namun, dalam praktiknya, banyak Perusahaan yang belum memiliki mekanisme pengawasan yang memadai.

Ketiadaan pengawasan ini menciptakan risiko signifikan, terutama jika Pihak Ketiga tidak menerapkan langkah-langkah keamanan yang cukup. Hal ini dapat mengakibatkan kebocoran data yang sulit terdeteksi, sehingga menempatkan Pengguna dalam posisi yang sangat rentan. Kesenjangan dalam transparansi dan pengawasan secara langsung meningkatkan potensi risiko kebocoran data pribadi. Ketika data pribadi jatuh ke tangan pihak yang tidak bertanggung jawab, informasi tersebut dapat disalahgunakan untuk berbagai tindakan ilegal, seperti:¹²

1. Penipuan identitas dimaksud dengan Pelaku dapat menggunakan data pribadi untuk membuka rekening palsu atau melakukan transaksi ilegal atas nama individu.
2. Pemerasan dilakukan dengan informasi sensitif yang dapat dimanfaatkan untuk memeras individu yang bersangkutan.
3. Penyalahgunaan untuk kepentingan komersial dengan data dapat dijual atau digunakan tanpa izin untuk tujuan pemasaran atau promosi.

Dampak dari kebocoran data tidak hanya merugikan Pengguna secara langsung, tetapi juga dapat mencoreng reputasi Perusahaan. Insiden semacam ini

¹² Fadli, Muhammad, Dijan Widijowati, and Dwi Andayani. "Pencurian Data Pribadi di Dunia Maya (Phising Cybercrime) yang ditinjau dalam Perspektif Kriminologi." *Co-Value Jurnal Ekonomi Koperasi dan kewirausahaan* 14, no. 12, 2024.

sering kali memicu kehilangan kepercayaan konsumen, yang pada akhirnya berdampak negatif pada keberlanjutan bisnis perusahaan. Selain itu, perusahaan juga menghadapi risiko hukum, termasuk denda dan sanksi administratif, jika terbukti melanggar UU No. 27/2022.

Mengingat pada tanggal 17 Oktober 2024, UU No. 27/2022 resmi diberlakukan sepenuhnya setelah melalui masa transisi selama dua tahun sejak disahkan. Sehingga terdapat urgensi untuk segera mengatur Kontrak terkait pemrosesan data antara Perusahaan dan Pihak Ketiga semakin mendesak. Dengan adanya UU No. 27/2022 ini, Perusahaan memiliki kewajiban hukum yang lebih jelas untuk melindungi data pribadi Pengguna, dan Kontrak menjadi instrumen kunci dalam memastikan kepatuhan terhadap regulasi tersebut. Tanpa pengaturan yang komprehensif dalam Kontrak, Perusahaan berisiko menghadapi konsekuensi hukum yang serius, termasuk denda dan sanksi administratif, jika terjadi pelanggaran terhadap perlindungan data. Selain itu, ketidakpastian dalam hubungan hukum dengan Pihak Ketiga dapat mengakibatkan kerentanan terhadap kebocoran data dan penyalahgunaan informasi pribadi.

Tanpa adanya Kontrak antara Perusahaan Pembiayaan dengan Pihak Ketiga akan menimbulkan kompleksitas isu yang dihadapi, sehingga penelitian ini berfokus mengenai perlindungan data Pengguna terhadap pemrosesan data pribadi yang dilakukan oleh Pihak Ketiga di Perusahaan. Penelitian ini bertujuan untuk menganalisis sejauh mana perusahaan-perusahaan ini melindungi dan melakukan pengawasan terhadap Pihak Ketiga, serta mengevaluasi dampaknya terhadap keamanan data Pengguna. Dengan mengidentifikasi tantangan dan celah yang ada dalam praktik perlindungan data saat ini, diharapkan hasil penelitian ini

dapat memberikan rekomendasi yang bermanfaat bagi Perusahaan Pembiayaan untuk memperbaiki ruang lingkup kerjasama pada pengelolaan data pribadi Pengguna mereka. Upaya ini tidak hanya akan melindungi hak-hak Pengguna, tetapi juga berkontribusi pada peningkatan kepercayaan masyarakat terhadap sektor pembiayaan, terutama di tengah perkembangan pesat era *digital* yang kita alami saat ini. Karena itu penulis tertarik untuk menulis thesis ini dengan judul **“PELINDUNGAN DATA PRIBADI PENGGUNA DALAM PEMROSESAN DATA OLEH PIHAK KETIGA DI SEKTOR PEMBIAYAAN KONSUMEN DENGAN IMPLEMENTASI PRAKTIS PADA KONTRAK BISNIS”**.

1.2 Rumusan Masalah

Masalah utama pada hal ini adalah Pengguna tidak mengetahui secara spesifik siapa atau pihak yang mengolah data sehingga adanya kesenjangan dari sisi transparansi dan pengawasan. Hal ini ditimbulkan dengan kurangnya pengaturan dalam klausul pada Kontrak antara Perusahaan dengan Pihak Ketiga yang mengolah data. Dalam penelitian thesis ini terdapat 2 (dua) pertanyaan penelitian yang hendak dijawab oleh penulis mengenai bentuk perlindungan data Pengguna. Dan berdasarkan masalah di atas tersebut penulis mempertegas dalam bentuk pertanyaan yakni sebagai berikut:

1. Bagaimana pengaturan hukum perlindungan data pribadi Pengguna dalam UU No. 27/2022 terhadap pemrosesan data pribadi oleh Pihak Ketiga di Perusahaan Pembiayaan?
2. Bagaimana ketentuan dalam Perjanjian Kerjasama antara Perusahaan Pembiayaan dan Pihak Ketiga berdasarkan pada prinsip dan kewajiban dalam UU No. 27/2022?

1.3 Tujuan Penelitian

Penulis telah memaparkan mengenai latar belakang dan rumusan masalah sehingga tujuan dari adanya peneliti ini untuk:

1. Memecahkan persoalan hukum, yang timbul dalam konteks yang diteliti, dengan mengidentifikasi dan memberikan solusi terhadap permasalahan yang ada dalam sistem hukum.
2. Melakukan penemuan ide dan atau teori hukum, dengan mengidentifikasi kendala yang dihadapi dalam pengawasan dan penegakan berdasarkan perjanjian kerjasama antara Perusahaan dengan Pihak Ketiga.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoretis

Penelitian ini memiliki potensi untuk memberikan kontribusi signifikan pada pengembangan ilmu hukum, khususnya di bidang hukum teknologi informasi dan perlindungan data pribadi bagi para Pengguna, diantaranya:

1. Dapat menginformasikan ilmu pengetahuan yang bermanfaat mengenai perlindungan data pribadi, terutama dalam kerjasama pemrosesan data antara Perusahaan dengan Pihak Ketiga kepada pembaca.
2. Menerapkan/merekonstruksi teori yang dipelajari
3. Memperoleh suatu manfaat dalam bidang hukum secara khususnya mempelajari hukum perlindungan data yang ada.

1.4.2 Manfaat Praktis

Diharapkan hasil penelitian ini dapat menjadi wawasan baru untuk meningkatkan kesadaran masyarakat, Perusahaan, dan Pihak Ketiga tentang

pentingnya perlindungan data pribadi dan implikasi hukum dari pelanggaran terhadap UU No. 27/2022. Serta melalui penelitian ini dapat memberikan rekomendasi konkret mengenai langkah-langkah yang dapat diambil untuk meningkatkan keamanan data pribadi, baik dalam lingkungan internal Perusahaan maupun dalam hubungan dengan Pihak Ketiga.

1.5 Sistematika Penulisan

1. **Bab I Pendahuluan**, memulai tesis ini dengan memberikan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, dan terakhir gambaran singkat tentang sistematika penulisan tesis.
2. **Bab II Tinjauan Pustaka**, menguraikan teori dan konsep utama yang relevan dengan penelitian ini, yaitu teori perlindungan hukum, teori perlindungan hak atas privasi, teori kontrak relasional, asas perlindungan data pribadi dalam UU No. 27/2022. Serta konsep perlindungan data pribadi (definisi data pribadi, hak subjek data, peran dan tanggung jawab Para Pihak), konsep pengaturan perjanjian Kerjasama.
3. **Bab III Metode Penelitian**, menguraikan jenis penelitian yang digunakan, serta jenis data yang relevan, teknik pengumpulan data, jenis pendekatan penelitian, dan teknik analisis data.
4. **Bab IV Hasil Penelitian dan Analisis**, memberikan uraian secara rinci tentang temuan dari penelitian ini. Bagian pertama dari bab ini akan membahas prinsip hukum yang diatur dalam UU No. 27/2022 dengan implementasi praktik pemrosesan data, kemudian pembahasan kedua pengaturan Kontrak bisnis dapat diintegrasikan secara efektif untuk

melindungi data pribadi Pengguna. Temuan mencakup kesenjangan yang ada, rekomendasi penyusunan Kontrak yang lebih efektif, serta langkah-langkah untuk meningkatkan pengawasan terhadap Pihak Ketiga.

5. **Bab V Kesimpulan dan Saran**, merangkum hasil penelitian dengan kesimpulan utama hasil dari implementasi ketentuan UU No. 27/2022 dengan praktik bisnis dalam hal transparansi, pengawasan, dan kepatuhan dalam pemrosesan data. Bab ini juga memberikan saran praktis dan rekomendasi kebijakan yang dapat diterapkan.

