KAJIAN YURIDIS PERLIDUNGAN DATA PRIBADI DALAM MELINDUNGI KONTAK DARURAT PADA LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI

SKRIPSI

UNTUK MEMENUHI PERSYARATAN

MENCAPAI DERAJAT S-1

O l e h :

Muhammad Nugraha Hermawan

NIM. A1011221097

PROGRAM SARJANA PROGRAM STUDI ILMU HUKUM



KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI

UNIVERSITAS TANJUNGPURA

FAKULTAS HUKUM

PONTIANAK

2026

KAJIAN YURIDIS PERLIDUNGAN DATA PRIBADI DALAM MELINDUNGI KONTAK DARURAT PADA LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI

SKRIPSI

Oleh:

Muhammad Nugraha Hermawan

NIM: A1011221097

PROGRAM SARJANA PROGRAM STUDI HUKUM

Skripsi Diajukan Sebagai Salah Satu Syarat Untuk

Memperoleh Gelar Sarjana Hukum

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI

UNIVERSITAS TANJUNGPURA

FAKULTAS HUKUM

PONTIANAK

2026

KAJIAN YURIDIS PERLIDUNGAN DATA PRIBADI DALAM MELINDUNGI KONTAK DARURAT PADA LAYANAN PENDANAAN BERBASIS BERSAMA TEKNOLOGI INFORMASI

Oleh:

Muhammad Nugraha Hermawan
NIM. A1011221097

Disetujui Oleh:

Pembimbing I	Pembimbing II
Dr Siti Rohani, S.H, M.Hum	**Hj. Ismawartati, S.H., M.H.**
NIP. 197509232000032001	**NIP. 196107251990022001**

Disahkan Oleh:
Dekan Fakultas Hukum

Dr. Hj. Sri Ismawati, S.H., M.Hum.
NIP. 196610291992022001

Tanggal Lulus: 6 April 2026

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI

UNIVERSITAS TANJUNGPURA

FAKULTAS HUKUM

PONTIANAK

2026

TIM PENGUJI:

Jabatan	Nama dan NIP	Pangkat /Golongan	Tanda Tangan
Ketua Penguji / Pembimbing I	Dr. Siti Rohani, S.H., M.Hum. NIP. 197509232000032001	IV/a/LK	
Sekretaris Penguji / Pembimbing II	Hj. Ismawartati, S.H., M.H. NIP. 196107251990022001	IV/b/LK	
Penguji I	Dr. Qahar Awaka, S.H., LL.M. NIP. 198112122006041002	III/b/L	
Penguji II	Hj. Rachmawati, S.H., M.H. NIP. 196411041989032001	IV/b/LK	

Berdasarkan Surat Keputusan Dekan Fakultas Hukum

Universitas Tanjungpura

Pontianak

Nomor: 1072 DST/UN22.1/DT.00.10/2026

Tanggal: 30 Maret 2026

PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	:	Muhammad Nugraha Hermawan
NIM	:	A1011221097
Bagian	:	Hukum Ekonomi
Program Studi	:	Ilmu Hukum
Judul Skripsi	:	Kajian Yuridis Perlindungan Data Pribadi Dalam Melindungi Kontak Darurat Pada Layanan Pendanaan Bersama Berbasis Teknologi Informasi

Menyatakan dengan sebenarnya bahwa :

1. Bahwa dalam melaksanakan otonomi keilmuan dan kebebasan akademi, mahasiswa wajib menjunjung tinggi nilai kejujuran dan etika akademik, terutama larangan untuk melakukan plagiat dalam menghasilkan karya ilmiah, sehingga kreativitas dalam bidang akademik dapat tumbuh dan berkembang.
2. Oleh karena itu, jika dikemudian hari terbukti hasil penulisan Skripsi/Tugas Akhir ini ternyata merupakan hasil dari jiplakan/pengambil alihan tulisan atau buah pikiran milik orang lain (hasil plagiat), maka saya menerima sanksi akademik sesuai dengan ketentuan yang berlaku.

Pontianak, 6 Maret 2026
Yang membuat pernyataan,



Muhammad Nugraha Hermawan
NIM. A1011221097

HALAMAN PERSEMBAHAN

Puji dan syukur saya haturkan kepada Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan penulisan skripsi ini yang berjudul **"KAJIAN YURIDIS PERLINDUNGAN DATA PRIBADI DALAM MELINDUNGI KONTAK PRIBADI PADA LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI".** Penulis sadari selesainya penulisan skripsi ini tidak hanya atas dasar kemampuan penulis sendiri, melainkan dorongan, bantuan, maupun doa dari berbagai pihak. Oleh karena itu, dengan kerendahan hati dan segala hormat penulis menyampaikan rasa terimakasih dan penghargaan kepada:

A. Bapak Prof. Dr. H. Garuda Wiko., S.H., M.Hum., selaku Rektor Universitas Tanjungpura.
B. Ibu Dr. Hj. Sri Ismawati, S.H., M.Hum., selaku Dekan Fakultas Hukum Universitas Tanjungpura.
C. Bapak Edy Suasono, S.H., M,H., selaku Dosen Pembimbing Akademik yang telah memberikan bimbingan, saran, dan masukan selama penulisan menempuh perkuliahan di Fakultas Hukum Universitas Tanjungpura.
D. Ibu Dr. Siti Rohani, S.H., M.Hum, Selaku Pembimbing I yang telah memberikan bimbingan, masukan, dan saran untuk penulisan skripsi ini hingga selesai.
E. Ibu Ismawartati, S.H., M,H., Selaku Pembimbing II yang juga telah memberikan bimbingan, bantuan, dan saran untuk penulisan skripsi ini hingga selesai.

F. Bapak Dr. Qahar Awaka, S.H., LL.M., selaku Penguji I telah memberikan saran dan masukan untuk kesempurnaan skripsi ini.

G. Ibu Rachmawatti, S.H., M.H., selaku penguji II yang telah memberikan saran dan maskan untuk kesempurnaan skripsi ini.

H. Bapak/Ibu Dosen Fakultas Hukum Universitas Tanjungpura yang telah memberikan ilmu pengetahuan hukum ataupun pengalaman selama masa perkuliahan.

I. Bapak/Ibu Staff Fakultas Hukum Universitas Tanjungpura yang telah membantu kelancaran pemberkasan skripsi ini.

J. Kepada Ibunda Mutiah, yang telah membiayai dan mendorong penulis untuk menyelesaikan penulisan ini.

K. Kepada Almarhum Ayahanda Drs. Titus Nursiwan. M.Kes, yang telah menjadi motivasi untuk berhasil sehingga dapat menyelesaikan penulisan.

L. Kepada Bayu Setiawan S.Kom dan dr. Mirantika Audina, selaku saudara dan saudari yang telah memberikan dorongan, doa, dan bantuan kepada penulis sehingga dapat menyelesaikan penulisan.

M. Kepada Putri Artanti Nurifani, selaku pacar penulis yang telah menemani, mendorong, dan membantu penulisan skripsi ini hingga selesai.

N. Kepada Chandra Al-Muhidi, Lucki Ananda Gulzard, Muhammad Atha Zenobia, dan Doni Wibowo, yang telah membantu dan menemani penulisan dalam penulisan skripsi ini serta teman-teman baik dari kampus ataupun di luar kampus yang tidak bisa penulis sebutkan satu persatu telah menemani penulisan skripsi penulis hingga selesai.

KATA PENGANTAR

Puji dan syukur atas berkat dan rahmat Tuhan Yang Maha Esa penulis dapat menyelesaikan penulisan skripsi dengan judul **"KAJIAN YURIDIS PERLINDUNGAN DATA PRIBADI DALAM MELINDUNGI DATA PRIBADI PADA LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI".**

Dalam penyusunan dan penulisan skripsi ini tentu tidak terlepas dari bantuan, bimbingan, serta dukungan dari berbagai pihak, baik secara langsung maupun tidak langsung. Oleh karena itu, pada kesempatan ini penulis mengucapkan terimakasih, syukur, dan penghargaan yang sebesar-besarnya kepada orang yang penulis sayangi dan banggakan.

Penulis menyadari bahwa skripsi ini masih terlalu jauh dari kata sempurna. Oleh karena itu, kritik, saran, dan masukan yang dapat membangun sangat penulis harapkan demi perbaikan dan kesempurnaan. Penulis juga berharap skripsi ini juga dapat bermanfaat bagi siapapun yang memerlukan nya dan penulis juga berharap skripsi ini dapat bermanfaat bagi Ilmu Pengetahuan khususnya Ilmu Hukum. Akhir kata, penulis harap semoga skripsi ini dapat bermanfaat serta penulis ucapkan terimakasih.

DAFTAR ISI

COVER..... i
HALAMAN PERNYATAAN..... ii
KATA PENGANTAR..... v
DAFTAR ISI..... vi
ABSTRAK..... viii
ABSTRACT..... ix
BAB I PENDAHULUAN..... 1
A. Latar Belakang Masalah..... 1
B. Rumusan Masalah..... 18
C. Tujuan Penelitian..... 18
D. Manfaat Penelitian..... 19
E. Keaslian Penelitian..... 19
F. Kerangka Teori..... 26
1. Perlindungan Hukum..... 26
2. Privasi dan Hak atas Data Pribadi..... 27
3. Pertanggungjawaban Hukum..... 28
4. Perlindungan Data Pribadi.....29
5. Kontrak dan Persetujuan dalam Pengelolaan Data.....31
6. Kepastian Hukum..... 34
G. Kerangka Konsep..... 34
BAB II TINJAUAN PUSTAKA..... 37
A. Tinjauan Umum Perlindungan Hukum..... 37
B. Tinjauan Umum Privasi dan Hak atas Data Pribadi..... 39
C. Tinjauan Umum Pertanggungjawaban Hukum..... 43
D. Tinajauan Umum Perlindungan Data Pribadi..... 45
E. Tinjauan Umum Kontrak dan Persetujuan dalam Perngelolaan Data48
F. Tinjauan Umum Kepastian Hukum..... 50
BAB III METODE PENELITIAN..... 54
A. Jenis dan Sifat Penelitian..... 54
B. Jenis Data..... 55
C. Cara Pengumpulan Data..... 56
D. Analisis Data..... 57
BAB IV PENELITIAN DAN PEMBAHASAN..... 60
A. Implementasi Regulasi Otoritas Jasa Keuangan dalam Perlindungan Data Kontak Darurat Nasabah Fintech Lending dan Kesesuaiannya

dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan DataPribadi…….. 60

B. Pertanggungjawaban Hukum Penyelenggara *Fintech Lending* Berizin terhadap Kebocoran Data Kontak Darurat dan Mekanisme Penegakan Hukum bagi Perlindungan Pemilik Data 70

BAB V HASIL 87

A. Kesimpulan 87

B. Saran 89

DAFTAR PUSTAKA 92

ABSTRAK

Penelitian ini dilatarbelakangi oleh maraknya praktik penyalahgunaan data kontak darurat dalam layanan *financial technology* (*fintech*) *lending* di Indonesia. Penyelenggara fintech sering mengumpulkan data kontak darurat tanpa persetujuan eksplisit dari pihak yang dicantumkan, yang kemudian disalahgunakan untuk penagihan utang dengan cara intimidasi dan pencemaran nama baik. Kondisi ini menunjukkan kesenjangan antara regulasi perlindungan data pribadi yang telah ada dengan implementasinya di lapangan.

Tujuan penelitian ini adalah untuk menganalisis implementasi regulasi Otoritas Jasa Keuangan (OJK) dalam melindungi kontak darurat nasabah fintech lending dan kesesuaiannya dengan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta mengkaji bentuk pertanggungjawaban hukum penyelenggara fintech dan mekanisme penegakan hukum bagi perlindungan pemilik data. Penelitian ini menggunakan metode yuridis normatif dengan sifat deskriptif analitis. Data diperoleh melalui studi kepustakaan terhadap peraturan perundang-undangan, literatur hukum, dan dokumentasi kasus pelanggaran.

Hasil penelitian menunjukkan bahwa regulasi Otoritas Jasa Keuangan (OJK) melalui POJK 77/2016, POJK 10/2022, dan POJK 40/2024 telah mengatur kewajiban perlindungan data pribadi dan sesuai dengan prinsip-prinsip Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022, meliputi prinsip persetujuan, pembatasan tujuan, keamanan data, akuntabilitas, dan transparansi. Namun, implementasinya masih lemah karena banyak penyelenggara tidak melakukan validasi atau meminta persetujuan eksplisit dari kontak darurat. Pertanggungjawaban hukum penyelenggara fintech mencakup tiga dimensi: administratif (sanksi peringatan, denda hingga 2% pendapatan tahunan, pencabutan izin), perdata (ganti rugi berdasarkan Pasal 1365 KUHPerdata), dan pidana (berdasarkan Undang-Undang Informasi Transaksi Elektronik dan Undang-Undang Perlindungan Data Pribadi dengan sanksi penjara hingga 5 tahun dan denda hingga Rp5 miliar). Mekanisme penegakan hukum yang tersedia meliputi pelaporan ke Otoritas Jasa Keuangan (OJK), Lembaga Pelindungan Data Pribadi, Kepolisian, serta gugatan perdata, namun efektivitasnya masih terkendala lemahnya pengawasan dan rendahnya kesadaran hukum masyarakat.

Kesimpulan penelitian ini adalah bahwa meskipun kerangka hukum perlindungan data kontak darurat telah komprehensif, implementasinya belum efektif sehingga kontak darurat tetap rentan terhadap penyalahgunaan. Diperlukan penguatan regulasi dengan mewajibkan validasi kontak darurat melalui persetujuan eksplisit, peningkatan kapasitas pengawasan Otoritas Jasa Keuangan (OJK), penegakan sanksi yang tegas, serta peningkatan literasi digital masyarakat.

Kata Kunci: Perlindungan Data Pribadi, Kontak Darurat, Fintech Lending, Otoritas Jasa Keuangan

ABSTRACT

This research is motivated by the widespread practice of misusing emergency contact data in financial technology (fintech) lending services in Indonesia. Fintech providers often collect emergency contact data without explicit consent from the listed parties, which is then misused for debt collection through intimidation and defamation. This condition demonstrates a gap between existing personal data protection regulations and their implementation in practice.

The purpose of this research is to analyze the implementation of Financial Services Authority (OJK) regulations in protecting emergency contacts of fintech lending customers and its conformity with Law Number 27 of 2022 concerning Personal Data Protection, as well as to examine forms of legal liability of fintech providers and law enforcement mechanisms for data owner protection. This research uses normative juridical method with descriptive analytical approach. Data was obtained through literature study of legislation, legal literature, and documentation of violation cases.

The research findings show that OJK regulations through POJK 77/2016, POJK 10/2022, and POJK 40/2024 have regulated personal data protection obligations and are consistent with the principles of PDP Law Number 27 of 2022, including principles of consent, purpose limitation, data security, accountability, and transparency. However, implementation remains weak as many providers do not validate or obtain explicit consent from emergency contacts. Legal liability of fintech providers encompasses three dimensions: administrative (warning sanctions, fines up to 2% of annual revenue, license revocation), civil (compensation based on Article 1365 of Civil Code), and criminal (based on ITE Law and PDP Law with imprisonment up to 5 years and fines up to IDR 5 billion). Available law enforcement mechanisms include reporting to OJK, Personal Data Protection Agency, Police, and civil lawsuits, but effectiveness is still constrained by weak supervision and low public legal awareness.

The conclusion of this research is that although the legal framework for emergency contact data protection is comprehensive, its implementation has not been effective, leaving emergency contacts vulnerable to misuse. Strengthening regulations by mandating emergency contact validation through explicit consent, enhancing OJK supervisory capacity, strict sanction enforcement, and improving public digital literacy are necessary.

***Keywords**: Personal Data Protection, Emergency Contact, Fintech Lending, Financial Services Authority*

BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi di era digital saat ini telah membawa perubahan fundamental dalam berbagai aspek kehidupan masyarakat, termasuk dalam hal pengelolaan dan pemanfaatan data pribadi. Transformasi digital yang masif ini tidak hanya mengubah cara manusia berinteraksi, berkomunikasi, dan bertransaksi, tetapi juga menciptakan ekosistem baru di mana data pribadi menjadi komoditas yang sangat berharga dan strategis. Dalam konteks ini, layanan berbasis teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari, mulai dari aplikasi perbankan digital, layanan transportasi online, *platform* media sosial, hingga berbagai aplikasi yang menyediakan layanan kesehatan, pendidikan, dan kebutuhan lainnya. Seiring dengan pertumbuhan pesat layanan-layanan tersebut, muncul pula berbagai isu krusial terkait perlindungan data pribadi pengguna yang perlu mendapat perhatian serius dari berbagai pemangku kepentingan.

Salah satu aspek yang menjadi perhatian khusus dalam konteks perlindungan data pribadi adalah pengelolaan informasi kontak darurat yang diminta oleh berbagai penyedia layanan berbasis teknologi informasi. Kontak darurat merupakan informasi sensitif yang mencakup data pribadi pihak ketiga, yaitu orang-orang yang dipercaya oleh pengguna layanan untuk dihubungi dalam situasi darurat atau ketika pengguna tidak dapat dihubungi secara

langsung.[1] Data kontak darurat ini biasanya mencakup nama lengkap, nomor telepon, alamat *email*, bahkan dalam beberapa kasus mencakup hubungan keluarga atau kedekatan relasi antara pengguna dengan kontak darurat tersebut. Praktik pengumpulan data kontak darurat ini telah menjadi standar dalam industri teknologi informasi, khususnya pada aplikasi yang menyediakan layanan keuangan seperti pinjaman *online*, layanan transportasi, dan berbagai platform digital lainnya yang memerlukan mekanisme verifikasi atau komunikasi alternatif dengan pengguna.

Permasalahan mendasar yang muncul adalah bahwa pengumpulan data kontak darurat ini seringkali dilakukan tanpa persetujuan eksplisit dari pihak yang dijadikan kontak darurat. Dalam banyak kasus, individu yang tercantum sebagai kontak darurat tidak mengetahui bahwa data pribadi mereka telah dikumpulkan, disimpan, dan berpotensi digunakan oleh penyedia layanan teknologi informasi.[2] Kondisi ini menimbulkan pertanyaan fundamental tentang legitimasi pengumpulan data tersebut dan sejauh mana praktik ini dapat dibenarkan dari perspektif hukum perlindungan data pribadi. Lebih jauh lagi, dalam beberapa kasus yang terungkap di masyarakat, data kontak darurat ini tidak hanya digunakan untuk keperluan komunikasi darurat yang sah, tetapi juga disalahgunakan untuk tujuan penagihan utang, pemasaran produk, atau bahkan dijual kepada pihak ketiga tanpa sepengetahuan dan persetujuan

---

[1] Dian Andi Nur Aziz, Siswo Hadi Sumantri, dan Anang Puji Utama, "Kebijakan Pelindungan Data Pribadi Dalam Pinjaman Online Berdasarkan Pendekatan Human Security," *Jurnal Damai dan Resolusi Konflik* 6, no. 3 (2020),hlm 50.

[2] Cintya Deani et al., "Darurat Sepihak Dalam Perjanjian Pinjaman Online" 24, no. 2 (2024), hlm 8.

pemilik data maupun pengguna layanan yang mencantumkan kontak darurat tersebut.

Indonesia sebagai negara dengan populasi pengguna internet terbesar di Asia Tenggara menghadapi tantangan serius dalam hal perlindungan data pribadi. Berdasarkan berbagai survei dan kajian, Indonesia memiliki pengguna internet aktif dengan tingkat penetrasi *smartphone* yang terus meningkat setiap tahunnya. Tingginya adopsi teknologi digital ini berbanding lurus dengan meningkatnya kerentanan terhadap pelanggaran privasi dan penyalahgunaan data pribadi. Kasus-kasus kebocoran data pribadi yang melibatkan jutaan akun pengguna dari berbagai platform digital telah terjadi berulang kali, menunjukkan bahwa infrastruktur keamanan data dan kesadaran akan pentingnya perlindungan data pribadi masih belum memadai. Dalam konteks kontak darurat, permasalahan menjadi lebih kompleks karena melibatkan tidak hanya data pribadi pengguna layanan, tetapi juga data pribadi pihak ketiga yang tidak memiliki hubungan kontraktual langsung dengan penyedia layanan.[3]

Sebelum berlakunya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, Indonesia menghadapi kekosongan hukum yang signifikan dalam hal pengaturan komprehensif tentang perlindungan data pribadi. Meskipun telah ada beberapa regulasi sektoral yang menyinggung aspek perlindungan data pribadi, seperti Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang

[3] Meilita Tryana Sembiring dan Carine, "Peninjauan Prospek SmartphoneGlobal: Studi Pustaka," *Talenta Conference Series* 2 (2019), hlm 109.

Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektmenjjadironik, serta berbagai peraturan sektoral dari Otoritas Jasa Keuangan, Kementerian Komunikasi dan Informatika, dan instansi terkait lainnya, namun pengaturan tersebut masih bersifat parsial dan tidak memberikan perlindungan yang komprehensif dan koheren. Keadaan ini mengakibatkan praktik pengumpulan, pengolahan, dan pemanfaatan data pribadi, termasuk data kontak darurat, dilakukan tanpa standar yang jelas dan pengawasan yang memadai, sehingga berpotensi merugikan hak-hak subjek data.

Dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi pada tanggal 17 Oktober 2022, Indonesia akhirnya memiliki kerangka hukum yang komprehensif untuk melindungi data pribadi warga negaranya.[4] Undang-undang ini mengadopsi prinsip-prinsip perlindungan data yang telah diakui secara internasional, termasuk prinsip persetujuan, prinsip pembatasan tujuan, prinsip minimalisasi data, prinsip akurasi, prinsip pembatasan penyimpanan, prinsip integritas dan kerahasiaan, serta prinsip akuntabilitas. Lebih lanjut, undang-undang ini juga memberikan berbagai hak kepada subjek data, termasuk hak untuk mendapatkan informasi, hak untuk mengakses data pribadi, hak untuk memperbaiki data yang tidak akurat, hak untuk menghapus data, hak untuk membatasi pemrosesan data, hak untuk memindahkan data, dan hak untuk menolak pemrosesan data pribadi

[4] Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 190.

dalam kondisi tertentu. Namun demikian, implementasi undang-undang ini dalam praktik, khususnya terkait perlindungan data kontak darurat, masih memerlukan kajian mendalam untuk memastikan efektivitas perlindungan yang diberikan.

Dalam konteks perlindungan data kontak darurat, terdapat beberapa dimensi hukum yang perlu dikaji secara komprehensif. Pertama, dari perspektif legitimasi pengumpulan data, perlu dikaji apakah pengumpulan data kontak darurat oleh penyedia layanan teknologi informasi memiliki dasar hukum yang sah sesuai dengan ketentuan Undang-Undang Pelindungan Data Pribadi. Undang-undang tersebut menetapkan bahwa pemrosesan data pribadi harus dilakukan berdasarkan persetujuan subjek data atau berdasarkan dasar hukum lain yang sah seperti pelaksanaan kontrak, pemenuhan kewajiban hukum, perlindungan kepentingan vital, pelaksanaan tugas untuk kepentingan umum, atau kepentingan yang sah dari pengendali data. Dalam kasus kontak darurat, pengumpulan data dilakukan atas inisiatif pengguna layanan, namun tanpa persetujuan dari pihak yang dijadikan kontak darurat, sehingga menimbulkan pertanyaan tentang dasar hukum yang dapat dijadikan justifikasi untuk praktik pengumpulan data tersebut.

Kedua, terkait dengan kewajiban pengendali data pribadi dan prosesor data pribadi dalam mengelola data kontak darurat. Undang-Undang Pelindungan Data Pribadi menetapkan berbagai kewajiban yang harus dipenuhi oleh pengendali data dan prosesor data, termasuk kewajiban untuk memberikan informasi yang jelas dan transparan tentang pemrosesan data, kewajiban untuk

memastikan keamanan data pribadi, kewajiban untuk melakukan penilaian dampak perlindungan data pribadi untuk pemrosesan yang berisiko tinggi, dan kewajiban untuk melaporkan kebocoran data pribadi kepada otoritas yang berwenang dan kepada subjek data yang terdampak. Dalam praktik, banyak penyedia layanan teknologi informasi yang belum sepenuhnya memenuhi kewajiban-kewajiban tersebut, khususnya dalam hal transparansi tentang bagaimana data kontak darurat digunakan dan dilindungi, serta dalam hal penerapan langkah-langkah keamanan yang memadai untuk mencegah akses tidak sah atau kebocoran data.

Ketiga, mengenai hak-hak subjek data, khususnya hak dari individu yang dijadikan kontak darurat tanpa sepengetahuan atau persetujuan eksplisit mereka. Pertanyaan fundamental yang muncul adalah apakah individu yang dijadikan kontak darurat memiliki hak yang sama dengan pengguna layanan yang mencantumkan mereka sebagai kontak darurat, termasuk hak untuk mengetahui bahwa data pribadi mereka telah dikumpulkan, hak untuk mengakses informasi tentang pemrosesan data pribadi mereka, hak untuk meminta penghapusan data pribadi mereka, dan hak untuk mengajukan keberatan terhadap pemrosesan data pribadi mereka. Implementasi hak-hak ini dalam konteks kontak darurat menjadi kompleks karena ketiadaan hubungan langsung antara individu yang dijadikan kontak darurat dengan penyedia layanan, serta potensi konflik antara hak privasi kontak darurat dengan kepentingan sah penyedia layanan dalam melakukan verifikasi atau komunikasi dengan pengguna.

Keempat, dari perspektif pertanggungjawaban dan sanksi, perlu dikaji mekanisme pertanggungjawaban yang dapat diterapkan kepada penyedia layanan teknologi informasi yang melanggar ketentuan perlindungan data pribadi dalam pengelolaan data kontak darurat. Undang-Undang Pelindungan Data Pribadi menetapkan berbagai sanksi administratif dan pidana untuk pelanggaran ketentuan perlindungan data pribadi, mulai dari peringatan tertulis, penghentian sementara kegiatan pemrosesan data pribadi, penghapusan atau pemusnahan data pribadi, denda administratif, hingga sanksi pidana berupa penjara dan denda yang cukup signifikan. Namun demikian, efektivitas penegakan sanksi-sanksi tersebut dalam praktik masih perlu dibuktikan, mengingat kompleksitas dalam pembuktian pelanggaran, keterbatasan kapasitas lembaga pengawas, dan tantangan dalam penegakan hukum terhadap entitas digital yang seringkali beroperasi lintas yurisdiksi.[5]

Praktik pengumpulan dan penggunaan data kontak darurat oleh berbagai layanan berbasis teknologi informasi di Indonesia menunjukkan pola yang beragam. Dalam industri *financial technology (fintech)*, khususnya layanan *peer-to-peer lending*, pengumpulan data kontak darurat telah menjadi praktik standar yang digunakan untuk tujuan verifikasi identitas dan sebagai sarana komunikasi alternatif dalam proses penagihan.[6] Banyak aplikasi pinjaman online meminta pengguna untuk menyediakan minimal dua hingga tiga kontak

[5] Ricky Shandy et al., "Aspek Hukum Pencantuman Data Pribadi Secara Sepihak Sebagai Kontak Darurat Dalam Perjanjian Kredit Online" 12 (2023), hlm 37.
[6] Moh Farhat, "Layanan Peer To Peer Lending Pada Fitur Shopee Pinjam (Tinjauan Fatwa Dewan Syariah Nasional Nomor:117/DSN-MUII/ii/2018 Tahun 2018 Tentang Layanan Berbasis Teknologi Informasi Berdasarkan Prinsip Syariah)" UIN DATOKARAMA PALU SULAWESI TENGAH, 2025), hlm 86.

darurat sebagai syarat persetujuan pinjaman. Dalam beberapa kasus yang dilaporkan, kontak darurat dari pengguna yang menunggak pembayaran dihubungi secara intensif oleh pihak *debt collector*, bahkan seringkali dengan cara-cara yang tidak etis seperti ancaman, intimidasi, atau penyebaran informasi yang mempermalukan kepada kontak lain di daftar kontak pengguna. Praktik ini tidak hanya melanggar privasi kontak darurat, tetapi juga berpotensi menimbulkan kerugian psikologis dan sosial bagi individu yang dijadikan kontak darurat.

Dalam industri transportasi *online*, data kontak darurat juga dikumpulkan dengan alasan keamanan pengguna. Aplikasi transportasi online biasanya meminta pengguna untuk menyediakan kontak darurat yang akan dihubungi jika terjadi situasi darurat selama perjalanan. Meskipun tujuan pengumpulan data ini dapat dibenarkan dari perspektif keamanan pengguna, namun tetap terdapat kekhawatiran tentang bagaimana data tersebut disimpan, berapa lama data tersebut disimpan, siapa saja yang memiliki akses terhadap data tersebut, dan apakah data tersebut digunakan untuk tujuan lain di luar konteks keamanan perjalanan. Transparansi tentang praktik pengelolaan data kontak darurat dalam industri transportasi online masih menjadi isu yang perlu mendapat perhatian, mengingat sensitifitas informasi yang dikumpulkan dan potensi risiko jika data tersebut jatuh ke tangan yang salah atau disalahgunakan.[7]

[7] Ajeng Andriani Hapsari dan Devy Mawarnie Puspitasari, *Manajemen Resiko Keuangan : Strategi proteksi Pengambilan Keputusan* (Jakarta: Takaza Innovatix Labs, 2025), hlm 85.

Berbagai *platform e-commerce* dan *marketplace* digital juga mengadopsi praktik pengumpulan data kontak darurat, meskipun dengan tujuan dan skala yang berbeda. Beberapa platform meminta data kontak darurat sebagai bagian dari proses verifikasi akun untuk transaksi bernilai tinggi atau sebagai bagian dari program loyalitas yang memberikan akses kepada fitur kredit atau cicilan. Praktik ini menimbulkan pertanyaan tentang proporsionalitas antara tujuan pengumpulan data dengan sensitivitas data yang dikumpulkan, serta tentang ketersediaan alternatif mekanisme verifikasi yang tidak melibatkan pengumpulan data pribadi pihak ketiga. Prinsip minimalisasi data yang dianut dalam Undang-Undang Pelindungan Data Pribadi mengharuskan pengendali data untuk hanya mengumpulkan data yang memadai, relevan, dan terbatas pada apa yang diperlukan untuk tujuan pemrosesan, sehingga perlu dikaji apakah pengumpulan data kontak darurat dalam berbagai konteks tersebut telah memenuhi prinsip minimalisasi data.[8]

Dari perspektif hukum perbandingan, dapat diamati bahwa berbagai yurisdiksi di dunia telah mengembangkan pendekatan yang berbeda dalam mengatur perlindungan data pribadi, khususnya terkait data pihak ketiga seperti kontak darurat. Uni Eropa melalui *General Data Protection Regulation (GDPR)* yang berlaku sejak tahun 2018 telah menetapkan standar perlindungan data yang sangat ketat, termasuk persyaratan persetujuan yang eksplisit, hak untuk dilupakan, hak portabilitas data, dan kewajiban untuk melakukan data

[8] Republik Indonesia, "Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, pasal 15" (2022).

protection impact assessment untuk pemrosesan data yang berisiko tinggi.[9] Dalam konteks GDPR, pengumpulan data pribadi pihak ketiga seperti kontak darurat tanpa persetujuan eksplisit dari pihak tersebut dapat dikualifikasikan sebagai pelanggaran yang serius dan dapat dikenakan sanksi denda hingga 4% dari omzet global tahunan perusahaan atau 20 juta Euro, mana yang lebih tinggi. Pendekatan yang ketat ini mencerminkan penghargaan yang tinggi terhadap hak privasi individu dan pengakuan bahwa perlindungan data pribadi merupakan hak fundamental yang harus dijaga dengan serius.

Amerika Serikat mengadopsi pendekatan yang berbeda dengan model sektoral dalam pengaturan perlindungan data pribadi, di mana terdapat berbagai regulasi federal dan negara bagian yang mengatur perlindungan data pribadi dalam sektor-sektor tertentu seperti kesehatan, keuangan, dan telekomunikasi. *California Consumer Privacy Act (CCPA)* yang berlaku sejak tahun 2020 dan kemudian diperkuat dengan *California Privacy Rights Act (CPRA)* memberikan hak-hak yang cukup komprehensif kepada konsumen California untuk mengontrol data pribadi mereka, termasuk hak untuk mengetahui data apa yang dikumpulkan, hak untuk menghapus data pribadi, dan hak untuk *opt-out* dari penjualan data pribadi. Meskipun pendekatan Amerika Serikat memberikan fleksibilitas yang lebih besar kepada industri, namun perkembangan regulasi terkini menunjukkan adanya tren penguatan perlindungan privasi konsumen, yang dapat menjadi referensi bagi Indonesia

[9] Farid Rizki Bachtiar, Wisnu Ardytia, dan Demas Brian, "Analisis Penegakan Hukum Data Pribadi Pada Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Di Indonesia Farid," *Amar : Jurnal Ilmiaah Hukum* 3, no. 2 (2025), hlm 76.

dalam mengembangkan regulasi turunan dari Undang-Undang Pelindungan Data Pribadi.[10]

Negara-negara Asia juga telah mengembangkan kerangka hukum perlindungan data pribadi dengan pendekatan yang beragam. Singapura melalui *Personal Data Protection Act (PDPA*) yang berlaku sejak tahun 2012 dan telah mengalami beberapa kali amandemen, menetapkan prinsip-prinsip perlindungan data yang seimbang antara perlindungan privasi individu dengan kebutuhan bisnis. Korea Selatan memiliki *Personal Information Protection Act* (PIPA) yang memberikan perlindungan yang cukup kuat terhadap data pribadi dan telah menunjukkan efektivitas dalam penegakan hukum dengan berbagai kasus sanksi terhadap perusahaan yang melanggar ketentuan perlindungan data. Jepang melalui *Act on the Protection of Personal Information* (APPI) yang telah direvisi beberapa kali untuk menyesuaikan dengan perkembangan teknologi dan standar internasional, mengadopsi konsep anonymized data dan pseudonymized data yang memberikan fleksibilitas dalam pemanfaatan data untuk tujuan penelitian dan pengembangan sambil tetap melindungi privasi individu.[11] Studi perbandingan terhadap berbagai yurisdiksi ini memberikan perspektif yang berharga dalam menganalisis kekuatan dan kelemahan kerangka hukum perlindungan data pribadi di Indonesia, khususnya dalam konteks perlindungan data kontak darurat.

---

[10] Judijanto Loso, Triyantoro Andri, dan Iin Inayah, "Perbandingan Sistem Hukum Perdata dan Common law dalam Perlindungan Data Pribadi di Indonesia," *Sanskara Hukum dan HAM* 4, no. 01 (2025), hlm 7.

[11] Berto Purnomo Sidik dan Sidi Ahyar Wiraguna, "Tinjauan Hukum terhadap Aplikasi Digital sebagai Upaya Meningkatkan Kesadaran Perlindungan Hak Privasi Data Pribadi," *Hukum Inovatif: Jurnal Ilmu Hukum Sosial dan Humaniora* 2, no. April (2025), hlm 126.

Tantangan dalam implementasi perlindungan data kontak darurat tidak hanya bersifat hukum, tetapi juga melibatkan dimensi teknis, ekonomi, dan sosial-budaya. Dari dimensi teknis, diperlukan infrastruktur keamanan siber yang robust untuk melindungi data kontak darurat dari akses tidak sah, kebocoran, atau penyalahgunaan. Hal ini mencakup penerapan enkripsi data baik dalam transit maupun saat disimpan, implementasi *access control* yang ketat untuk membatasi akses hanya kepada personel yang berwenang, penggunaan *secure development practices* dalam pengembangan aplikasi, pelaksanaan security audit dan penetration testing secara berkala, serta pengembangan *incident response plan* untuk menangani kebocoran data jika terjadi.[12] Banyak penyedia layanan teknologi informasi, khususnya startup dan perusahaan kecil menengah, masih memiliki keterbatasan dalam hal kapasitas teknis dan sumber daya untuk mengimplementasikan langkah-langkah keamanan yang memadai, sehingga data kontak darurat yang mereka kelola berisiko tinggi terhadap pelanggaran keamanan.

Dari dimensi ekonomi, terdapat pertimbangan *cost-benefit* dalam implementasi perlindungan data pribadi yang ketat. Bagi penyedia layanan teknologi informasi, implementasi perlindungan data yang komprehensif memerlukan investasi yang signifikan dalam infrastruktur teknis, sumber daya manusia, dan proses bisnis. Di sisi lain, kegagalan dalam melindungi data pribadi dapat mengakibatkan kerugian yang jauh lebih besar, tidak hanya

[12] Aldino Marga Pratama, Syaiful, dan Fadhilur Rahman, *Keamanan Data dan Informasi* (Bandung: Kaizen Media Publishing, 2024), hlm 40.

dalam bentuk sanksi hukum dan denda, tetapi juga dalam bentuk kerusakan reputasi, kehilangan kepercayaan konsumen, dan potensi tuntutan hukum dari subjek data yang dirugikan. Analisis ekonomi tentang perlindungan data pribadi perlu mempertimbangkan tidak hanya biaya langsung implementasi, tetapi juga biaya tidak langsung dari kegagalan perlindungan data, serta manfaat jangka panjang dari membangun kepercayaan konsumen dan kepatuhan terhadap regulasi.[13] Dalam konteks kontak darurat, pertanyaan ekonomi yang relevan adalah apakah praktik pengumpulan data kontak darurat memberikan nilai yang proporsional dengan risiko yang ditimbulkan, dan apakah terdapat alternatif mekanisme yang dapat mencapai tujuan yang sama dengan risiko yang lebih rendah.

Dari dimensi sosial-budaya, kesadaran masyarakat Indonesia tentang pentingnya perlindungan data pribadi masih relatif rendah. Banyak pengguna layanan teknologi informasi yang tidak membaca dengan seksama ketentuan privasi dan syarat penggunaan layanan, dan cenderung menyetujui semua permintaan akses data tanpa memahami implikasi dari persetujuan tersebut. Rendahnya literasi digital dan literasi privasi ini membuat masyarakat rentan terhadap praktik pengumpulan dan penyalahgunaan data pribadi. Lebih lanjut, dalam konteks kontak darurat, banyak pengguna layanan yang tidak menyadari bahwa dengan mencantumkan kontak darurat, mereka secara tidak langsung menyerahkan data pribadi orang lain kepada penyedia layanan, dan bahwa

[13] Rista Maharani dan Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi *Digital Protection of Consumer Personal Data by Electronic System Providers in Digital* Peningkatan substansial dalam penggunaan *platform e-commerce* di Indonesia telah," *Jurnal USM Law Review* 7, no. 1 (2024), hlm 221.

tindakan ini dapat berdampak pada privasi kontak darurat tersebut. Peningkatan kesadaran masyarakat tentang hak-hak privasi mereka dan tentang pentingnya berhati-hati dalam memberikan data pribadi, termasuk data pribadi pihak ketiga, merupakan komponen penting dalam ekosistem perlindungan data pribadi yang efektif.

Peran lembaga pengawas dalam implementasi perlindungan data pribadi sangat krusial untuk memastikan kepatuhan penyedia layanan teknologi informasi terhadap ketentuan hukum yang berlaku.[14] Undang-Undang Pelindungan Data Pribadi mengamanatkan pembentukan lembaga independen yang bertanggung jawab untuk mengawasi implementasi perlindungan data pribadi, menerima dan menangani pengaduan dari subjek data, melakukan investigasi terhadap dugaan pelanggaran, memberikan sanksi administratif kepada pelanggar, serta melakukan sosialisasi dan edukasi kepada masyarakat tentang perlindungan data pribadi. Efektivitas lembaga pengawas ini akan sangat bergantung pada berbagai faktor, termasuk independensi lembaga dari pengaruh politik dan ekonomi, ketersediaan sumber daya manusia yang kompeten dan memadai, dukungan anggaran yang cukup, kewenangan yang jelas dan luas untuk melakukan pengawasan dan penegakan hukum, serta kapasitas teknis untuk memahami kompleksitas teknologi informasi dan model bisnis digital yang terus berkembang.

[14] Ridho Pakina dan Mohammad Solekhan, "Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia," *Journal of Scientech Research and Development* 6, no. 1 (2024), hlm 201.

Dalam konteks perlindungan data kontak darurat, lembaga pengawas perlu mengembangkan pedoman khusus yang memberikan panduan kepada penyedia layanan teknologi informasi tentang praktik terbaik dalam pengumpulan, penyimpanan, dan penggunaan data kontak darurat. Pedoman ini perlu mencakup antara lain persyaratan untuk memperoleh persetujuan eksplisit dari kontak darurat sebelum atau segera setelah data mereka dikumpulkan, kewajiban untuk memberikan informasi yang jelas dan mudah dipahami kepada kontak darurat tentang bagaimana data mereka akan digunakan, pembatasan penggunaan data kontak darurat hanya untuk tujuan yang sah dan spesifik, kewajiban untuk menerapkan langkah-langkah keamanan yang memadai untuk melindungi data kontak darurat, serta mekanisme yang mudah bagi kontak darurat untuk mengajukan keberatan atau meminta penghapusan data mereka. Tanpa pedoman yang jelas dan spesifik, implementasi perlindungan data kontak darurat berisiko menjadi tidak konsisten dan tidak efektif, sehingga tujuan perlindungan yang diamanatkan oleh undang-undang tidak tercapai dengan baik.

Aspek lain yang perlu mendapat perhatian adalah mekanisme penyelesaian sengketa dalam kasus pelanggaran perlindungan data pribadi, khususnya yang melibatkan data kontak darurat. Undang-Undang Pelindungan Data Pribadi memberikan hak kepada subjek data untuk mengajukan gugatan ganti rugi kepada pengendali data atau prosesor data yang melanggar ketentuan perlindungan data pribadi dan menimbulkan kerugian. Namun demikian, dalam praktik, penyelesaian sengketa melalui jalur litigasi seringkali

memerlukan waktu yang lama, biaya yang tinggi, dan beban pembuktian yang berat bagi subjek data. Oleh karena itu, perlu dikembangkan mekanisme penyelesaian sengketa alternatif yang lebih cepat, murah, dan mudah diakses oleh subjek data, seperti mediasi atau arbitrasi yang difasilitasi oleh lembaga pengawas atau lembaga independen lainnya. Mekanisme ini akan sangat berguna khususnya untuk kasus-kasus pelanggaran perlindungan data yang tidak menimbulkan kerugian materiil yang besar namun tetap menimbulkan kerugian immateriil atau pelanggaran hak privasi yang perlu mendapat penyelesaian yang adil.

Perkembangan teknologi seperti *artificial intelligence, big data analytics,* dan *Internet of Things* membawa tantangan baru dalam perlindungan data pribadi, termasuk dalam konteks pengelolaan data kontak darurat. Teknologi-teknologi ini memungkinkan pengumpulan, analisis, dan pemanfaatan data dalam skala dan kecepatan yang belum pernah terjadi sebelumnya, menciptakan potensi manfaat yang sangat besar namun juga risiko yang signifikan terhadap privasi individu.[15] Dalam konteks data kontak darurat, penggunaan teknologi machine learning untuk menganalisis pola komunikasi dan relasi sosial pengguna dapat memberikan insight yang berharga untuk berbagai tujuan seperti deteksi fraud atau personalisasi layanan, namun juga dapat menimbulkan kekhawatiran tentang *surveillance* dan *profiling* yang berlebihan. Kerangka hukum perlindungan data pribadi perlu cukup fleksibel

[15] Nirsal et al., *Big Data : Panduan dan Peluang di Era Digital* (Jambi: PT. Sonpedia Publishing Indonesia, 2024), hlm 43.

dan adaptif untuk mengakomodasi perkembangan teknologi ini sambil tetap memastikan bahwa prinsip-prinsip fundamental perlindungan data pribadi tidak dilanggar.[16]

Berdasarkan uraian di atas, dapat disimpulkan bahwa perlindungan data pribadi, khususnya perlindungan data kontak darurat pada layanan berbasis teknologi informasi, merupakan isu yang kompleks dan multidimensional yang memerlukan kajian yuridis yang mendalam dan komprehensif. Meskipun Indonesia telah memiliki Undang-Undang Pelindungan Data Pribadi sebagai kerangka hukum yang komprehensif, namun implementasi efektif dari undang-undang ini dalam konteks perlindungan data kontak darurat masih menghadapi berbagai tantangan dan memerlukan pengembangan lebih lanjut melalui regulasi turunan, pedoman teknis, dan praktik terbaik industri. Kajian ini menjadi penting dan relevan untuk memberikan analisis hukum yang mendalam tentang bagaimana kerangka hukum perlindungan data pribadi di Indonesia dapat diterapkan secara efektif untuk melindungi data kontak darurat, apa saja hak dan kewajiban para pihak yang terlibat, bagaimana mekanisme penegakan hukum dapat dioptimalkan, dan apa saja rekomendasi kebijakan yang diperlukan untuk menutup gap yang masih ada dalam perlindungan data kontak darurat pada layanan berbasis teknologi informasi.
Berdasarkan uraian – uraian di atas, penulis merasa tertarik untuk melakukan penelitian guna penulisan dengan Judul :

[16] Yose Indarta, *Cyber Law : Dimensi Hukum dalam Era Digital* (Padang: Pustaka Galeri Mandiri, 2024), hlm 38.

KAJIAN YURIDIS PERAN OTORITAS JASA KEUANGAN DALAM MELINDUNGI VALIDASI KONTAK DARURAT PADA LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI

B. Rumusan Masalah

Berdasarkan latar belakang tersebut di atas, maka penulis merumuskan masalah penelitian sebagai berikut:

1. Bagaimana implementasi regulasi perlindungan data pribadi yang dikeluarkan oleh Otoritas Jasa Keuangan (OJK) dalam melindungi kontak darurat nasabah pada layanan *financial technology (fintech) lending*?
2. Bagaimana bentuk pertanggungjawaban hukum penyelenggara layanan keuangan digital yang berizin dan diawasi oleh Kementerian Keuangan dan Otoritas Jasa Keuangan (OJK) terhadap kebocoran atau penyalahgunaan data kontak darurat nasabah?

C. Tujuan Penelitian

Adapun yang menjadi yang menjadi tujuan penelitian ini adalah:

1. Mengidentifikasi dan menganalisis regulasi perlindungan data pribadi yang dikeluarkan oleh Otoritas Jasa Keuangan (OJK) terkait kontak darurat pada layanan *fintech lending*.
2. Merumuskan rekomendasi kebijakan dan mekanisme perlindungan hukum yang lebih efektif bagi pemilik data pribadi khususnya kontak darurat dalam ekosistem layanan keuangan digital

D. Manfaat Penelitian

1. Secara Teoritis

   Diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan ilmu hukum dalam bidang perlindungan data pribadi, khususnya dalam konteks teknologi finansial. Hasil penelitian dapat memperkaya literatur akademik mengenai persinggungan antara hukum perlindungan data pribadi dengan regulasi sektor keuangan digital.

2. Secara Praktis

   1) Memberikan panduan praktis bagi penyelenggara Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) dalam mengembangkan sistem validasi kontak darurat yang sesuai dengan prinsip perlindungan data pribadi dan etika bisnis. Hasil penelitian juga dapat membantu penyelenggara Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) dalam mengantisipasi perkembangan regulasi di masa depan.
   2) Temuan penelitian dapat membantu pembuat kebijakan dalam merumuskan pendekatan regulasi yang mendukung pertumbuhan industri *fintech* sekaligus melindungi hak-hak masyarakat.

E. Keaslian Penelitian

Penelitian yang berjudul "KAJIAN YURIDIS PERLINDUNGAN DATA PRIBADI DALAM MELINDUNGI KONTAK DARURAT PADA LAYANAN PEBDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI". bukanlah hasil duplikat ataupun plagiasi dari penelitian-

penelitian terdahulu, melainkan murni hasil karya penulis sendiri. Terdapat beberapa penelitian yang memiliki topik yang mirip, akan tetapi memiliki perbedaan dengan penelitian ini seperti:

1. Penelitian pertama yang menjadi rujukan penting adalah karya Moh Iqbal Alfayat pada tahun 2023 yang berjudul "**Perlindungan Hukum Terhadap Seseorang yang Dijadikan Emergency Contact Secara Sepihak di Aplikasi Pinjaman Online Legal**".

   Penelitian Moh Iqbal Alfayat memiliki kesamaan mendasar dengan penelitian ini dalam mengidentifikasi permasalahan ketiadaan validasi yang memadai terhadap kontak darurat yang dicantumkan oleh peminjam dalam aplikasi fintech lending. Kedua penelitian sama-sama mengangkat isu krusial mengenai penyalahgunaan data pribadi pihak ketiga yang dijadikan kontak darurat tanpa persetujuan eksplisit dari yang bersangkutan. Hal ini menjadi perhatian serius karena melanggar prinsip-prinsip dasar perlindungan data pribadi sebagaimana diamanatkan dalam berbagai regulasi yang berlaku. Lebih lanjut, baik penelitian Moh Iqbal Alfayat maupun penelitian ini sama-sama mengkaji peran strategis Otoritas Jasa Keuangan sebagai regulator dalam memberikan perlindungan hukum bagi pihak-pihak yang dirugikan oleh praktik pencantuman kontak darurat secara sepihak.

   Meskipun memiliki kesamaan fundamental dalam mengidentifikasi permasalahan, penelitian ini mengambil pendekatan yang berbeda dan lebih luas dibandingkan dengan penelitian Moh Iqbal Alfayat. Perbedaan

mendasar terletak pada upaya penelitian ini untuk mengkaji kesesuaian regulasi yang ada dengan teori-teori perlindungan hukum dan perlindungan data pribadi secara lebih mendalam dan sistematis. Penelitian ini tidak hanya berhenti pada identifikasi masalah, melainkan melakukan analisis komparatif dengan regulasi serupa di negara-negara lain untuk menemukan model ideal yang dapat diadopsi atau diadaptasi dalam konteks Indonesia. Pendekatan komparatif ini memberikan perspektif yang lebih luas dan memungkinkan penelitian ini untuk menghasilkan rekomendasi kebijakan yang lebih kontekstual dan aplikatif. Dengan demikian, penelitian ini berusaha menjembatani kesenjangan antara teori perlindungan hukum dengan praktik implementasinya di lapangan, sekaligus menawarkan solusi yang lebih komprehensif berdasarkan pembelajaran dari pengalaman negara-negara lain yang telah lebih dahulu menghadapi permasalahan serupa.

2. Penelitian kedua yang menjadi rujukan adalah karya Ricky Shandy dan Retno Dewi Pulung Sari pada tahun 2023 dengan judul "**Aspek Hukum Pencantuman Data Pribadi Secara Sepihak Sebagai Kontak Darurat Dalam Perjanjian Kredit Online**".

   Penelitian ini memiliki kesamaan metodologis yang signifikan dengan penelitian yang sedang dilakukan, yakni sama-sama menggunakan pendekatan yuridis normatif dengan fokus pada analisis peraturan perundang-undangan. Kedua penelitian mendasarkan analisisnya pada penggunaan bahan hukum primer yang meliputi peraturan perundang-

undangan yang berlaku, serta bahan hukum sekunder berupa literatur, jurnal, dan hasil penelitian terdahulu. Kerangka regulasi yang digunakan juga menunjukkan kesamaan, di mana kedua penelitian mengacu pada Undang-Undang Perlindungan Data Pribadi, Peraturan Otoritas Jasa Keuangan Nomor 77 Tahun 2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi, serta regulasi terkait lainnya yang mengatur tentang penyelenggaraan *fintech lending* di Indonesia. Kesamaan dalam kerangka regulasi ini menunjukkan bahwa kedua penelitian berangkat dari landasan hukum positif yang sama dalam menganalisis permasalahan perlindungan kontak darurat.

Namun demikian, perbedaan mendasar antara penelitian Ricky Shandy dan Retno Dewi Pulung Sari dengan penelitian ini terletak pada sudut pandang dan fokus analisis yang digunakan. Penelitian ini mengambil sudut pandang regulator dengan menempatkan Otoritas Jasa Keuangan sebagai *focal point* dalam memberikan perlindungan hukum kepada pihak ketiga yang dijadikan kontak darurat tanpa persetujuan. Pendekatan ini memberikan perspektif yang berbeda karena tidak hanya menganalisis aspek-aspek hukum dari sisi normatif semata, tetapi juga mengkaji implementasi dan efektivitas peran regulator dalam menjalankan fungsi pengawasan dan perlindungannya. Penelitian ini menekankan pentingnya validasi kontak darurat sebagai mekanisme preventif yang harus diwajibkan dan diawasi ketat oleh Otoritas Jasa Keuangan (OJK) untuk mencegah terjadinya penyalahgunaan data pribadi. Lebih lanjut, penelitian ini

menganalisis regulasi serta kebijakan ini secara komprehensif, termasuk mengevaluasi efektivitas pengawasan yang telah dilakukan selama ini. Dengan demikian, penelitian ini tidak hanya bersifat deskriptif-analitis, tetapi juga evaluatif dan preskriptif dalam merumuskan rekomendasi perbaikan sistem pengawasan dan perlindungan hukum yang lebih efektif.

3. Penelitian ketiga yang menjadi bahan perbandingan adalah karya Chandra Al Muhidi pada tahun 2025 berjudul "**Kajian Hukum Kontrak Elektronik Pada Lembaga Pembiayaan Bersama Berbasis Teknologi Informasi Home Credit**".

Persamaan antara penelitian Chandra Al Muhidi dengan penelitian ini terletak pada objek kajian yang sama-sama berkaitan dengan mekanisme Lembaga Pembiayaan Bersama Berbasis Teknologi Informasi. Kedua penelitian sama-sama mengkaji aspek-aspek hukum yang terkait dengan penyelenggaraan layanan *fintech lending*, khususnya dalam konteks perlindungan terhadap pihak-pihak yang terlibat dalam transaksi pembiayaan berbasis teknologi informasi. Kesamaan ini menunjukkan bahwa kedua penelitian berangkat dari keprihatinan yang sama terhadap potensi pelanggaran hukum dan perlindungan konsumen dalam ekosistem *fintech lending* yang berkembang pesat di Indonesia.

Meskipun demikian, terdapat perbedaan yang cukup signifikan dalam fokus dan objek penelitian antara karya Chandra Al Muhidi dengan penelitian ini. Penelitian Muhidi lebih terfokus pada kajian hukum kontrak elektronik secara umum dalam konteks Layanan Pendanaan Bersama

Berbasis Teknologi Informasi (LPBBTI), sementara penelitian ini memiliki fokus yang lebih spesifik dan mendalam pada peran Otoritas Jasa Keuangan (OJK) dalam melindungi kontak darurat pada mekanisme Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI). Perbedaan fokus ini membawa implikasi pada kedalaman analisis yang berbeda pula. Jika penelitian Chandra Al Muhidi mengkaji aspek-aspek kontraktual dan legalitas kontrak elektronik secara luas, penelitian ini menggali lebih dalam pada satu aspek spesifik yang selama ini kurang mendapat perhatian, yakni perlindungan terhadap pihak ketiga yang dijadikan kontak darurat. Dengan fokus yang lebih spesifik ini, penelitian ini dapat menghasilkan analisis yang lebih mendalam dan rekomendasi yang lebih operasional terkait dengan mekanisme perlindungan yang harus dijalankan oleh Otoritas Jasa Keuangan (OJK) sebagai regulator.

Dari ketiga penelitian terdahulu yang telah dikaji, dapat disimpulkan bahwa penelitian ini memiliki posisi yang unik dan memberikan kontribusi baru dalam diskursus perlindungan hukum dalam ekosistem *fintech lending*. Penelitian ini tidak hanya mengidentifikasi permasalahan sebagaimana dilakukan oleh Moh Iqbal Alfayat, tidak hanya menganalisis aspek hukum normatif sebagaimana dilakukan oleh Ricky Shandy dan Retno Dewi Pulung Sari, dan tidak hanya mengkaji mekanisme Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) secara umum sebagaimana dilakukan oleh Muhidi. Penelitian ini mengintegrasikan berbagai pendekatan tersebut dengan menempatkan Otoritas Jasa Keuangan

(OJK) sebagai focal point dalam analisis, melakukan perbandingan dengan regulasi negara lain, mengkaji efektivitas implementasi regulasi yang ada, dan menekankan pentingnya mekanisme preventif melalui validasi kontak darurat. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi teoretis dalam pengembangan konsep perlindungan hukum terhadap pihak ketiga dalam transaksi fintech, sekaligus memberikan kontribusi praktis berupa rekomendasi kebijakan yang dapat diimplementasikan oleh Otoritas Jasa Keuangan (OJK) untuk memperkuat sistem perlindungan konsumen dan pihak-pihak terkait dalam ekosistem fintech lending di Indonesia. Melalui pendekatan yang komprehensif dan multi-perspektif ini, penelitian ini berupaya mengisi celah pengetahuan yang belum terjawab oleh penelitian-penelitian sebelumnya, sekaligus menawarkan solusi yang lebih holistik dan aplikatif untuk mengatasi permasalahan penyalahgunaan data pribadi kontak darurat dalam aplikasi pinjaman online.

Dalam hal ini bahwasannya tulisan ini belum pernah diteliti oleh penulis lain. Dikarenakan penulisan saya ini, meneliti tentang **"KAJIAN YURIDIS PERLINDUNGAN DATA PRIBADI DALAM MELINDUNGI KONTAK PRIBADI PADA LAYANAN PENDANAAN BERSAMA BERBASIS TEKNOLOGI INFORMASI"**.

F. Kerangka Teori

1. Perlindungan Hukum

Perlindungan hukum merupakan konsep fundamental dalam sistem hukum yang bertujuan memberikan pengayoman terhadap hak asasi manusia yang dirugikan. Menurut Satjipto Rahardjo, perlindungan hukum adalah memberikan pengayoman kepada hak asasi manusia yang dirugikan orang lain dan perlindungan tersebut diberikan kepada masyarakat agar mereka dapat menikmati semua hak-hak yang diberikan oleh hukum.[17]

Perlindungan hukum ke dalam dua bentuk, yaitu perlindungan hukum preventif dan perlindungan hukum represif, di mana perlindungan hukum preventif merupakan perlindungan yang diberikan oleh pemerintah dengan tujuan mencegah terjadinya pelanggaran sebelum pelanggaran tersebut terjadi, yang diwujudkan melalui peraturan perundang-undangan sebagai sarana pencegahan sekaligus pemberian rambu-rambu atau batasan dalam pelaksanaan kewajiban, dan dalam konteks perlindungan data pribadi mencakup kewajiban penyedia layanan untuk menerapkan prinsip-prinsip perlindungan data, melakukan penilaian dampak perlindungan data pribadi, serta menerapkan langkah-langkah teknis dan organisatoris yang memadai, sedangkan perlindungan hukum represif bertujuan untuk menyelesaikan sengketa setelah terjadinya pelanggaran, yang pelaksanaannya dilakukan melalui mekanisme peradilan seperti Pengadilan Umum dan Pengadilan

[17]Rahardjo, Satjipto. *Ilmu Hukum*. (Bandung: Citra Aditya Bakti, 2000), hlm 34.

Administrasi di Indonesia, serta dalam konteks perlindungan data pribadi diwujudkan melalui mekanisme penyelesaian sengketa, penegakan sanksi administratif, dan penerapan sanksi pidana terhadap pelanggaran ketentuan perlindungan data pribadi.

Teori perlindungan hukum relevan dalam penelitian ini untuk menganalisis bagaimana hukum memberikan perlindungan terhadap data kontak darurat, baik melalui mekanisme pencegahan (preventif) maupun penyelesaian (represif) ketika terjadi pelanggaran atau penyalahgunaan data.

2. Privasi dan Hak atas Data Pribadi

Privasi merupakan hak fundamental yang diakui dalam berbagai instrumen hak asasi manusia internasional.[18] Alan F. Westin mendefinisikan privasi sebagai klaim individu, kelompok, atau institusi untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang mereka dikomunikasikan kepada orang lain.[19] Konsep privasi informasional (*informational privacy*) khususnya menekankan pada kontrol individu atas informasi pribadi mereka.

Dalam perkembangan teknologi informasi, konsep privasi berkembang menjadi hak atas perlindungan data pribadi (right to data protection). Menurut Paul M. Schwartz dan Karl-Nikolaus Peifer,

[18] Puan Zhinta Azzahra Tarmizii, "Analisis Perlindungan Hak Asasi Manusia di Era Digital : Tantangan dan Solusi," *Jurnal kajian Hukum dan Kebijakan Publik* 2, no. 1 (2024), hlm 33.
[19] Westin, Alan F. *Privacy and Freedom*. (New York: Atheneum, 1967), hlm 183.

perlindungan data pribadi tidak hanya mencakup aspek privasi tetapi juga aspek kontrol individu atas pemrosesan data mereka.[20] Hal ini mencakup hak untuk mengetahui, mengakses, memperbaiki, dan menghapus data pribadi yang diproses oleh pihak lain.

Teori privasi dan hak atas data pribadi dalam penelitian ini digunakan untuk menganalisis kedudukan kontak darurat sebagai data pribadi yang harus dilindungi, serta hak-hak yang melekat pada subjek data (baik pengguna layanan maupun pihak yang dicantumkan sebagai kontak darurat) dalam pengelolaan data tersebut.

3. Pertanggungjawaban Hukum

Pertanggungjawaban hukum merupakan konsep yang berkaitan dengan kewajiban untuk menanggung akibat dari perbuatan yang dilakukan. Hans Kelsen membedakan pertanggungjawaban hukum berdasarkan siapa yang harus bertanggung jawab, yaitu pertanggungjawaban individu (*individual responsibility*) dimana seseorang bertanggung jawab atas perbuatannya sendiri, dan pertanggungjawaban kolektif (*collective responsibility*) dimana seseorang bertanggung jawab atas perbuatan orang lain.

Dalam konteks hukum perdata, dikenal konsep pertanggungjawaban berdasarkan kesalahan (*liability based on fault*) dan pertanggungjawaban tanpa kesalahan atau pertanggungjawaban mutlak

[20] Schwartz, Paul M., and Karl-Nikolaus Peifer. "*Transatlantic Data Privacy Law*." *Georgetown Law Journal* 106, no. 1 (2017),hlm 158.

(*strict liability*). Sementara dalam hukum pidana, pertanggungjawaban didasarkan pada unsur kesalahan (*schuld*) yang mencakup kesengajaan (*dolus*) dan kealpaan (*culpa*).

Ridwan Khairandy menjelaskan bahwa dalam hukum perlindungan konsumen dan transaksi elektronik, berkembang pula konsep pertanggungjawaban produk *(product liability)* dan pertanggungjawaban pelaku usaha *(business liability)* yang dapat bersifat kontraktual maupun berdasarkan perbuatan melawan hukum.[21]

Teori pertanggungjawaban hukum dalam penelitian ini digunakan untuk menganalisis bentuk-bentuk pertanggungjawaban yang dapat diterapkan kepada penyedia layanan berbasis teknologi informasi yang melakukan penyalahgunaan data kontak darurat, baik pertanggungjawaban perdata, pidana, maupun administratif.

4. Perlindungan Data Pribadi

Teori Teori perlindungan data pribadi didasarkan pada gagasan bahwa setiap individu memiliki hak untuk mengendalikan informasi mengenai dirinya.[22] Data pribadi tidak sekadar komoditas ekonomi, melainkan perpanjangan dari martabat dan integritas pribadi yang harus dilindungi melalui seperangkat prinsip, norma, dan mekanisme dalam pengumpulan, penggunaan, penyimpanan, penyebaran, serta pemusnahan data. Dalam

---

[21] Khairandy, Ridwan. *Hukum Kontrak Indonesia dalam Perspektif Perbandingan*. Yogyakarta: FH UII Press, (2013), hlm 75.

[22] Herol Hansen Samin, "Perlindungan Hukum Terhadap Kebocoran Data Pribadi Oleh Pengendali Data Melalui," *Jurnal Sains Student Research* 1, no. 2 (2023), hlm 58.

kerangka negara hukum, pengaturan ini didasarkan pada asas perlindungan, kepastian hukum, kemanfaatan, keseimbangan, kehati-hatian, pertanggungjawaban, dan kerahasiaan.

Di Indonesia, teori ini terwujud melalui Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi yang mengatur asas, jenis data pribadi, hak subjek data, kewajiban pengendali dan prosesor data, hingga sanksi. Undang-undang ini menempatkan individu sebagai pemilik hak aktif melalui pengakuan hak memperoleh informasi, hak akses, hak perbaikan, hak penghapusan, hak pembatasan pemrosesan, hak portabilitas data, dan hak menarik persetujuan. Perlindungan data pribadi bukan hanya kewajiban administratif, tetapi instrumen untuk menjamin kebebasan, otonomi, dan rasa aman individu di ruang digital.

Teori ini menekankan prinsip-prinsip pemrosesan data seperti pembatasan pengumpulan, tujuan spesifik, minimalisasi data, akurasi, keamanan, keterbukaan, dan akuntabilitas. Pengendali data hanya boleh mengumpulkan data yang relevan, menggunakan sesuai tujuan yang sah, menjaga dari akses tidak sah, serta memberikan mekanisme pengawasan bagi subjek data. Dalam layanan bersama berbasis teknologi informasi yang meminta akses kontak pribadi, diperlukan persetujuan yang sah, diinformasikan, dan spesifik agar pengguna memahami tujuan, ruang lingkup, dan risiko pemberian akses.

Pada tataran teoritis, perlindungan data pribadi berkaitan dengan hak atas privasi dan konsep informational self-determination, yaitu hak individu

menentukan informasi yang boleh diketahui, sejauh mana data diproses, dan untuk tujuan apa. Di era digital, risiko kebocoran, penipuan, peretasan, dan penyalahgunaan komersial semakin tinggi karena data dapat direplikasi dan disebarkan secara cepat. Teori ini menuntut pembatasan kekuasaan negara dan pelaku usaha dalam mengakses data, sekaligus mendorong mekanisme pertanggungjawaban, pengawasan, dan penegakan hukum yang efektif. Dalam konteks perlindungan kontak pribadi pada layanan bersama berbasis teknologi informasi, setiap akses dan pemrosesan harus diletakkan dalam hubungan hukum yang jelas, berbasis persetujuan, diikat oleh asas perlindungan data, serta diawasi melalui sanksi dan upaya hukum apabila terjadi pelanggaran.

5. Kontrak dan Persetujuan dalam Pengelolaan Data

Teori kontrak dan persetujuan dalam pengelolaan data pribadi memandang hubungan hukum antara pengguna dan penyelenggara layanan bersama berbasis teknologi informasi sebagai suatu perjanjian yang dibingkai dalam kontrak elektronik atau klausula baku. Pemrosesan data pribadi, termasuk akses terhadap kontak pribadi, memerlukan dasar hukum yang sah melalui persetujuan subjek data. Persetujuan bukan sekadar formalitas administratif, melainkan manifestasi kesepakatan yang memenuhi syarat sah perjanjian: kesepakatan, kecakapan, objek tertentu,

dan causa yang halal. Pemrosesan data tanpa persetujuan yang sah berpotensi melanggar asas kebebasan berkontrak dan hak atas privasi.[23]

Dalam perspektif perlindungan data pribadi, persetujuan adalah izin yang diberikan subjek data secara bebas, spesifik, diinformasikan, dan jelas sebagai dasar pemrosesan data pribadinya. Persetujuan yang sah mengharuskan subjek data mengetahui tujuan pemrosesan, jenis data yang dikumpulkan, pihak penerima data, dan potensi risiko. Persetujuan yang diperoleh melalui kalimat ambigu, tersembunyi dalam klausula panjang, atau di bawah tekanan dapat dianggap cacat dan tidak sah. Undang-Undang Pelindungan Data Pribadi mengatur persetujuan sebagai salah satu dasar pemrosesan data di samping pelaksanaan perjanjian, pemenuhan kewajiban hukum, perlindungan kepentingan vital, dan kepentingan sah yang seimbang.

Secara kontraktual, persetujuan pemrosesan data dituangkan dalam syarat dan ketentuan atau kebijakan privasi yang diakses melalui aplikasi atau situs web, sering berbentuk *clickwrap atau browsewrap agreement*. Kondisi ini menimbulkan ketidakseimbangan karena pengguna berada dalam posisi lemah tanpa ruang merundingkan isi kontrak, sementara penyelenggara menyusun klausula baku yang memuat izin luas terhadap pengumpulan data, termasuk akses daftar kontak. Dalam layanan bersama berbasis teknologi informasi, banyak kontrak mencantumkan klausula akses

[23] Poppy Winanti dan Wawan Mas'udi, *G 20 Di Tengah Perubahan Besar* (Yogyakarta: Gadjah Mada University Press, 2023) hlm 55.

kontak dengan alasan verifikasi atau penagihan, namun pengguna tidak memahami bahwa kontak pihak ketiga turut terekspos tanpa persetujuan langsung. Hal ini menimbulkan problem yuridis karena kontrak tidak dapat dijadikan dasar merampas hak privasi pihak lain yang tidak ikut mengikatkan diri dalam perjanjian.[24]

Undang-Undang Pelindungan Data Pribadi mensyaratkan persetujuan pemrosesan data dilakukan secara tertulis atau terekam, baik elektronik maupun nonelektronik, dengan kekuatan hukum yang sama sepanjang memenuhi ketentuan kejelasan, keterbacaan, dan kemudahan akses. Permintaan persetujuan harus dibedakan dari klausula lain, disusun dalam bahasa sederhana, dan tanpa unsur pemaksaan. Klausula yang memuat permintaan pemrosesan data tanpa persetujuan eksplisit dinyatakan batal demi hukum. Ketentuan ini merefleksikan prinsip transparansi dan fairness, di mana pengendali data wajib menunjukkan bukti persetujuan dan dilarang mengumpulkan data yang tidak relevan. Dalam konteks perlindungan kontak pribadi pada layanan bersama, akses terhadap kontak harus ditempatkan dalam kerangka perjanjian yang seimbang, dengan persetujuan yang benar-benar diinformasikan, serta menghormati hak pemilik data dan pihak ketiga, sehingga kontrak tidak menjadi instrumen legalisasi pelanggaran privasi di ruang digital.

[24] Meghuel Lehandro Salindeho, Merry Elisabeth Kalalo, dan Hendrik Pondaag, "Perlindungan Hukum Bagi Pihak Ketiga Yang Dicantumkan," *Lex Privatum* 15, no. 3 (2025), hlm 67.

6. Kepastian Hukum

Kepastian hukum merupakan produk dari hukum atau lebih khusus dari perundang-undangan. Kepastian hukum dalam situasi tertentu mensyaratkan adanya aturan yang jelas, konsisten, mudah diperoleh, diterbitkan oleh kekuasaan negara, dan dapat dimengerti oleh masyarakat.

Kepastian hukum mengandung beberapa arti, yaitu adanya kejelasan, tidak menimbulkan multitafsir, tidak menimbulkan kontradiksi, dan dapat dilaksanakan. Peter Mahmud Marzuki menyatakan bahwa kepastian hukum mengandung dua pengertian: pertama, adanya aturan yang bersifat umum membuat individu mengetahui perbuatan apa yang boleh atau tidak boleh dilakukan; kedua, berupa keamanan hukum bagi individu dari kesewenangan pemerintah karena dengan adanya aturan yang bersifat umum, individu dapat mengetahui apa saja yang boleh dibebankan atau dilakukan oleh negara terhadap individu.[25]

Teori kepastian hukum dalam penelitian ini digunakan untuk menganalisis sejauh mana pengaturan hukum perlindungan data pribadi di Indonesia, khususnya terkait kontak darurat, memberikan kepastian hukum bagi para pihak yang terlibat, baik pengguna layanan, kontak darurat, maupun penyedia layanan.

G. Kerangka Konsep

Praktik pencantuman kontak darurat tanpa validasi dalam Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) menimbulkan

[25] Marzuki, Peter Mahmud. *Pengantar Ilmu Hukum*. Jakarta: Kencana, (2008), hlm 44.

kerentanan hukum bagi pihak yang dicantumkan secara sepihak. Penelitian menunjukkan bahwa ketiadaan mekanisme verifikasi terhadap persetujuan kontak darurat menjadi akar masalah pelanggaran privasi dan tekanan psikologis terhadap pihak ketiga. Regulasi seperti Undang-Undang Informasi Transaksi Elektronik Nomor 19 Tahun 2016 dan Peraturan Otoritas Jasa Keuangan 77/2016 sebenarnya mewajibkan persetujuan eksplisit dari pemilik data sebelum pencantuman kontak darurat, tetapi implementasinya belum optimal akibat lemahnya pengawasan oleh Otoritas Jasa Keuangan (OJK).

Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) wajib memastikan validasi tertulis atau elektronik dari kontak darurat sebelum pencantuman data. Pelanggaran terhadap kewajiban ini dapat dikategorikan sebagai pelanggaran privasi data berdasarkan Pasal 26 ayat (2) Undang-Undang Informasi Transaksi Elektronik dan berpotensi mengakibatkan sanksi administratif seperti denda hingga pencabutan izin usaha.[26]

Ketiadaan validasi dalam penetapan kontak darurat menimbulkan implikasi hukum yang signifikan, karena menempatkan kontak darurat dalam posisi yang rentan secara hukum, khususnya ketika data pribadinya digunakan atau dihubungi tanpa persetujuan yang sah dalam proses penagihan utang oleh pihak ketiga.

Dari aspek tanggung jawab finansial, kontak darurat pada dasarnya tidak memiliki kewajiban hukum untuk menanggung atau melunasi utang debitur,

[26] Republik Indonesia, "Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 19 Tahun 2016, Pasal 26 ayat (2)," (2008).

meskipun dalam praktiknya sering mengalami tekanan, ancaman, atau intimidasi berupa panggilan telepon maupun kunjungan dari *debt collector* yang berupaya menagih kewajiban tersebut.

Adapun upaya hukum yang dapat ditempuh oleh kontak darurat sebagai korban antara lain mengajukan gugatan perbuatan melawan hukum sebagaimana diatur dalam Pasal 1365 Kitab Undang-Undang Hukum Perdata, serta melaporkan dugaan pelanggaran ketentuan Undang-Undang Informasi dan Transaksi Elektronik (Undang-Umdamg Informasi Transaksi Elektronik) kepada aparat penegak hukum apabila terdapat penyalahgunaan data pribadi atau tindakan yang melanggar hukum.

Praktik pencantuman kontak darurat tanpa validasi dalam Layanan Pendanaan Bersama Berbasis Teknologi Informasi (LPBBTI) menimbulkan kerentanan hukum bagi pihak yang dicantumkan secara sepihak. Penelitian menunjukkan bahwa ketiadaan mekanisme verifikasi terhadap persetujuan kontak darurat menjadi akar masalah pelanggaran privasi dan tekanan psikologis terhadap pihak ketiga. Regulasi seperti Undang-Undang Informasi Transaksi Elektronik Nomor 19 Tahun 2016 dan Peraturan Otoritas Jasa Keuangan 77/2016 sebenarnya mewajibkan persetujuan eksplisit dari pemilik data sebelum pencantuman kontak darurat, tetapi implementasinya belum optimal akibat lemahnya pengawasan oleh Otoritas Jasa Keuangan (OJK).