

ANALISIS YURIDIS PENGENAAN PASAL PENCEMARAN NAMA BAIK DAN CYBERBULLYING DALAM KASUS PENYEBARAN DATA PRIBADI OLEH *FINTECH LENDING*

Mieke Aprilia Utami^{1*}, Sri Ridma Ramadhani², Suriyadi³, Ahmad Murjani⁴

^{1,2,3,4}Program Studi Ilmu Hukum, Fakultas Hukum dan Bisnis, Universitas Cahaya Bangsa, Indonesia

Email Korespondensi: miekehukumucb02@gmail.com*

Email: ramadhaniridma@gmail.com; peapaser30@gmail.com; akhmadmurjaniucb01@gmail.com

ABSTRACT

The practice of debt collection in peer-to-peer lending (fintech lending) in Indonesia is often characterized by digital intimidation and misuse of personal data, violating the constitutional rights of customers. This study aims to empirically examine the effectiveness of defamation articles in the ITE Law (Electronic Information and Transactions Law) and protection instruments in the PDP Law (Personal Data Protection Law) on the guarantee of customers' digital dignity protection. This study employs a quantitative method with a juridical-empirical approach. Data were collected via questionnaires from 100 fintech users selected using purposive sampling technique and analyzed using multiple linear regression. The results indicate that both regulations simultaneously have a positive and significant effect on customer protection, with a contribution of influence (R^2) of 58.2%. Partially, the PDP Law was found to have a more dominant impact ($\beta = 0.452$) compared to the ITE Law ($\beta = 0.284$), indicating that customers feel more protected through preventive data governance mechanisms than reactive criminal approaches. This study concludes that although regulations are on the right track, law enforcement effectiveness is still hindered by a gap of 41.8%, influenced by the complexity of proving mens rea and inter-institutional bureaucracy. Therefore, the implementation of the strict liability principle for fintech operators is recommended to mitigate the risk of cyberbullying in the future.

Keywords: Cyberbullying, Fintech Lending, Personal Data Protection, Strict Liability, UU ITE.

ABSTRAK

Praktik penagihan pinjaman online (*fintech lending*) di Indonesia sering kali diwarnai dengan intimidasi digital dan penyalahgunaan data pribadi yang melanggar hak konstitusional nasabah. Penelitian ini bertujuan untuk menguji secara empiris efektivitas pengenaan pasal pencemaran nama baik dalam UU ITE dan instrumen perlindungan dalam UU PDP terhadap jaminan perlindungan martabat digital nasabah. Penelitian ini menggunakan metode kuantitatif dengan pendekatan yuridis-empiris. Data dikumpulkan melalui kuesioner terhadap 100 responden pengguna *fintech* yang dipilih menggunakan teknik *purposive sampling*, kemudian dianalisis menggunakan regresi linear berganda. Hasil penelitian menunjukkan bahwa kedua regulasi secara simultan memiliki pengaruh positif dan signifikan terhadap perlindungan nasabah dengan kontribusi pengaruh (R^2) sebesar 58,2%. Secara parsial, UU PDP ditemukan memiliki dampak yang lebih dominan ($\beta = 0,452$) dibandingkan UU ITE ($\beta = 0,284$), yang mengindikasikan bahwa nasabah merasa lebih terlindungi melalui mekanisme tata kelola data yang preventif dibandingkan pendekatan pidana yang reaktif. Penelitian ini menyimpulkan bahwa meskipun regulasi sudah berjalan pada koridornya, efektivitas penegakan hukum masih terhambat oleh celah sebesar 41,8% yang dipengaruhi oleh kompleksitas pembuktian mens rea dan birokrasi antar-lembaga. Oleh karena itu, direkomendasikan penerapan prinsip pertanggungjawaban mutlak (*strict liability*) bagi penyelenggara *fintech* untuk memitigasi risiko perundungan siber (*cyberbullying*) di masa depan.

Kata kunci: Cyberbullying, Fintech Lending, Perlindungan Data Pribadi, Strict Liability, UU ITE.

PENDAHULUAN

Pesatnya perkembangan teknologi finansial (*financial technology*) di Indonesia telah mengubah lanskap inklusi keuangan secara signifikan, namun di sisi lain memicu kompleksitas permasalahan hukum baru, khususnya terkait perlindungan data pribadi. Fenomena *fintech lending* atau pinjaman online (pinjol) sering kali diwarnai dengan praktik penagihan yang tidak beretika, di mana penyebaran data pribadi nasabah dijadikan instrumen untuk menekan debitur. Praktik ini sering kali berujung pada tindakan pencemaran nama baik di ruang siber (*cyber defamation*) dan perundungan siber (*cyberbullying*), yang tidak hanya merugikan martabat kemanusiaan korban tetapi juga melanggar hak konstitusional atas privasi. Menurut Prasetyo (2022), penyalahgunaan data pribadi dalam industri pinjol merupakan bentuk pelanggaran hak asasi manusia yang memerlukan ketegasan sanksi pidana untuk memberikan efek jera bagi penyelenggara.

Secara yuridis, tindakan penyebaran data pribadi oleh pihak pinjol sering kali dijerat menggunakan ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, terdapat ambiguitas dalam penerapan pasal-pasal pencemaran nama baik dan *cyberbullying* ketika berhadapan dengan fakta bahwa data yang disebarluaskan sering kali adalah fakta (seperti tunggakan utang), namun cara penyebarannya ditujukan untuk mempermalukan korban. Sebagaimana dijelaskan oleh Hidayat et al. (2023), tantangan utama dalam kasus ini adalah menentukan batasan antara hak kreditor untuk menagih piutang dengan kewajiban melindungi data sensitif debitur sesuai dengan mandat Undang-Undang Perlindungan Data Pribadi (UU PDP). Pelanggaran terhadap batasan ini menciptakan delik hukum yang bersinggungan antara hukum siber dan hukum pidana umum.

Perlindungan data pribadi dalam transaksi digital global telah menjadi perhatian serius, di mana instrumen hukum internasional sering kali menekankan pada prinsip *consent* (persetujuan). Menurut Mitrou (2021) dalam studinya mengenai *data protection*, setiap pengolahan data yang keluar dari tujuan awal pengumpulan merupakan bentuk pelanggaran serius yang dapat dikategorikan sebagai tindakan kriminal. Di Indonesia, meskipun UU PDP telah disahkan, praktik *cyberbullying* yang dilakukan oleh penagih utang pinjol masih sering lolos dari jeratan hukum karena lemahnya pembuktian unsur niat jahat (*mens rea*) dalam menyebarkan informasi tersebut di ruang publik virtual.

Urgensi penelitian ini didasarkan pada data laporan Satgas Pasti OJK yang menunjukkan peningkatan aduan terkait perilaku penagihan tidak beretika sebesar 35% pada tahun terakhir. Sebanyak 60% dari aduan tersebut berkaitan dengan penyebaran data pribadi kepada kontak darurat. Fenomena ini menunjukkan adanya kesenjangan antara keberadaan regulasi (UU ITE dan UU PDP) dengan perlindungan nyata yang dirasakan masyarakat. Oleh karena itu, diperlukan pembuktian secara numerik mengenai sejauh mana penguatan pasal-pasal tersebut efektif dalam memitigasi tindakan pencemaran nama baik di lapangan.

Penelitian ini menjadi krusial untuk memberikan kejelasan interpretasi hukum mengenai penguatan pasal pencemaran nama baik terhadap pelaku penyebaran data pribadi oleh pinjol. Sinkronisasi antara UU ITE dan UU PDP perlu dikaji lebih mendalam untuk menutup celah hukum yang sering dimanfaatkan oleh pihak-pihak tidak bertanggung jawab (kolektor) dalam melakukan intimidasi digital. Oleh karena itu, penelitian ini bertujuan untuk melakukan analisis empiris mengenai efektivitas yuridis penerapan sanksi pidana dalam kasus penyebaran data pribadi, demi mewujudkan kepastian hukum dan perlindungan yang komprehensif bagi masyarakat di tengah masifnya penggunaan layanan keuangan berbasis teknologi.

Kerangka Yuridis Perlindungan Data Pribadi dan Delik Pencemaran Nama Baik; Perlindungan data pribadi merupakan bagian dari hak asasi manusia yang dijamin secara konstitusional, namun implementasinya dalam ruang digital sering kali bersinggungan dengan delik pencemaran nama baik. Secara normatif, Undang-Undang Perlindungan Data Pribadi (UU PDP) mendefinisikan data pribadi sebagai data tentang orang perseorangan yang teridentifikasi secara tersendiri atau dikombinasi dengan informasi lain baik secara langsung maupun tidak langsung. Menurut Prasetyo (2022), penyalahgunaan

data nasabah dalam penagihan hutang daring tidak hanya melanggar hak atas privasi, tetapi juga bertentangan dengan prinsip *lawful basis* atau dasar pemrosesan data yang sah. Penegakan hukum dalam kasus ini menjadi kompleks ketika penyebaran data tersebut diikuti dengan muatan yang menyerang kehormatan seseorang di media sosial.

Dalam konteks hukum siber, delik pencemaran nama baik diatur dalam Pasal 27 ayat (3) UU ITE (yang telah mengalami penyesuaian pada UU No. 1 Tahun 2024). Unsur utama dalam pasal ini adalah adanya muatan penghinaan dan/atau pencemaran nama baik yang didistribusikan ke ruang publik. Sebagaimana dijelaskan oleh Hidayat et al. (2023), tantangan yuridis muncul ketika pihak *fintech* menyebarkan fakta mengenai tunggakan utang debitur; meskipun informasi tersebut benar, jika cara penyampaian dilakukan untuk mempermalukan atau merusak reputasi debitur di depan pihak ketiga, maka unsur "menyerang kehormatan" tetap dapat terpenuhi. Hal ini menunjukkan bahwa kebenaran fakta tidak serta-merta menghapuskan sifat melawan hukum dari tindakan penyebaran data pribadi yang bersifat intimidatif.

Secara global, prinsip perlindungan data pribadi dan martabat digital telah diatur dalam berbagai instrumen hukum internasional yang menekankan pada pembatasan penggunaan data. Menurut Mitrou (2021), setiap tindakan yang mengubah data pribadi menjadi senjata untuk melakukan tekanan psikologis (*social shaming*) merupakan pelanggaran berat terhadap etika siber dan hak privasi individu. Di Indonesia, harmonisasi antara UU ITE sebagai hukum materiil siber dan UU PDP sebagai hukum payung perlindungan data sangat diperlukan untuk menentukan kualifikasi delik. Analisis terhadap mekanisme *cyberbullying* yang dilakukan oleh penyelenggara pinjol menunjukkan bahwa pengenaan pasal pencemaran nama baik harus dilihat secara komprehensif, mencakup aspek perlindungan martabat manusia di atas kepentingan komersial penagihan utang.

Konstruksi Hukum *Cyberbullying* dalam Transaksi *Fintech Lending*; *Cyberbullying* atau perundungan siber dalam aktivitas penagihan pinjaman online sering kali bermanifestasi dalam bentuk intimidasi digital, pelecehan, hingga pengucilan sosial melalui penyebaran data pribadi ke kontak darurat atau media sosial. Secara yuridis, meskipun istilah *cyberbullying* tidak disebutkan secara eksplisit dalam KUHP maupun UU ITE, namun substansi tindakannya dapat dikonstruksikan melalui pasal-pasal mengenai ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi. Menurut Sari (2022), praktik penagihan yang menyebarkan foto wajah debitur disertai narasi penghinaan kepada seluruh kontak ponsel merupakan bentuk nyata dari *cyberstalking* dan *harassment* yang melampaui batas kewajaran penagihan piutang.

Konstruksi hukum terhadap tindakan ini sering kali bersinggungan dengan Pasal 29 UU ITE mengenai pengiriman informasi elektronik yang berisi ancaman kekerasan atau menakut-nakuti secara pribadi. Sebagaimana ditegaskan oleh Fauzi et al. (2023), unsur menakut-nakuti terpenuhi ketika kolektor pinjol secara masif mengirimkan pesan-pesan yang bertujuan merusak kondisi psikis debitur dan menciptakan stigma negatif di lingkungannya. Hal ini menjadi bentuk kekerasan siber yang terstruktur, di mana data pribadi (seperti daftar kontak dan riwayat panggilan) dieksploitasi sebagai senjata untuk melakukan tekanan mental demi kepentingan komersial.

Dalam perspektif hukum pidana internasional, tindakan menekan martabat seseorang melalui platform digital dikategorikan sebagai pelanggaran serius terhadap integritas pribadi. Menurut Smith (2021), *cyberbullying* yang dilakukan oleh entitas korporasi atau agennya (kolektor) terhadap individu menciptakan ketimpangan relasi kuasa yang ekstrem, sehingga memerlukan perlindungan hukum yang bersifat protektif bagi pihak yang lemah. Di Indonesia, keberadaan UU PDP diharapkan mampu memperkuat jeratan hukum bagi penyelenggara *fintech* yang tidak mampu menjaga kerahasiaan data nasabahnya, karena pembiaran terhadap praktik *cyberbullying* oleh pihak ketiga (kolektor) dapat dikategorikan sebagai kegagalan dalam perlindungan data yang berimplikasi pidana maupun administratif.

Pertanggungjawaban Pidana Penyelenggara *Fintech Lending* dalam Penyalahgunaan Data Pribadi;

Pertanggungjawaban pidana dalam ekosistem digital saat ini tidak lagi terbatas pada subjek hukum perorangan seperti kolektor di lapangan, melainkan telah diperluas kepada korporasi sebagai penyelenggara sistem elektronik. Dalam ranah hukum *fintech lending*, korporasi memikul tanggung jawab hukum untuk menjamin keamanan dan kerahasiaan data pribadi yang dikelolanya sejak proses akuisisi hingga penghapusan data. Menurut Prasetyo (2022), kegagalan penyelenggara dalam mencegah penyebaran data pribadi oleh pihak ketiga yang terafiliasi dengannya dapat dikonstruksikan sebagai bentuk kelalaian korporasi (*corporate negligence*) yang memiliki implikasi pidana serius. Berdasarkan kerangka yuridis yang berlaku, terdapat beberapa poin utama yang menentukan pertanggungjawaban korporasi dalam penyalahgunaan data pribadi nasabah yang dapat dijelaskan sebagai berikut: (1) Doktrin *Vicarious Liability*; Korporasi bertanggung jawab atas tindakan melawan hukum (seperti penyebaran data pribadi yang menghina) yang dilakukan oleh karyawan atau pihak ketiga (kolektor) selama tindakan tersebut dilakukan dalam lingkup pekerjaan dan demi kepentingan korporasi (Hidayat et al., 2023), (2) Prinsip *Privacy by Design*; Penyelenggara wajib mengintegrasikan sistem keamanan data sejak awal. Kegagalan sistem yang memungkinkan data nasabah "bocor" ke tangan kolektor untuk tujuan intimidasi dianggap sebagai pelanggaran kewajiban hukum perusahaan (Mitrou, 2021), (3) Pertanggungjawaban Mutlak (*Strict Liability*); Sebagai pengendali data pribadi berdasarkan UU PDP, perusahaan *fintech* memikul beban tanggung jawab untuk membuktikan bahwa mereka telah melakukan upaya maksimal dalam melindungi data. Jika terjadi perundungan siber (*cyberbullying*) akibat data yang tersebar, perusahaan dapat dijatuhi sanksi administratif hingga pidana tambahan berupa pencabutan izin usaha, (4) Niat Jahat Korporasi (*Mens Rea*); Dalam hukum siber, niat jahat korporasi dapat dilihat dari adanya pembiaran (*omission*) terhadap praktik penagihan yang tidak beretika secara sistematis demi mencapai target penagihan hutang perusahaan (Sari, 2022).

Dengan demikian, sinkronisasi antara pertanggungjawaban pidana korporasi dalam KUHP dan sanksi spesifik dalam UU ITE serta UU PDP menjadi instrumen krusial untuk memastikan bahwa perusahaan *fintech* tidak hanya mengejar profit, tetapi juga mematuhi prinsip-prinsip perlindungan martabat kemanusiaan nasabah di ruang siber. Tanpa penegakan hukum yang menysar entitas bisnis, praktik pencemaran nama baik melalui data pribadi akan terus berulang karena dianggap sebagai risiko operasional yang murah oleh penyelenggara.

Perlindungan Hak Privasi dan Martabat Digital dalam Perspektif Hak Asasi Manusia; Hak atas privasi merupakan salah satu bagian dari hak asasi manusia yang bersifat fundamental dan diakui secara internasional, di mana setiap individu memiliki hak untuk bebas dari campur tangan yang sewenang-wenang terhadap urusan pribadi, keluarga, maupun korespondensinya. Dalam era ekonomi digital, hak ini berkembang menjadi hak atas perlindungan data pribadi dan martabat digital yang menjamin bahwa informasi sensitif seseorang tidak digunakan sebagai alat intimidasi. Menurut Prasetyo (2022), eksploitasi data pribadi oleh penyedia layanan keuangan untuk melakukan *social shaming* merupakan pelanggaran terhadap hak atas rasa aman dan perlindungan kehormatan martabat manusia sebagaimana diamanatkan dalam konstitusi.

Dalam kaitan dengan praktik *fintech lending*, perlindungan martabat digital nasabah harus dipandang sebagai kewajiban asasi yang melekat pada setiap penyelenggara sistem elektronik. Terdapat beberapa prinsip dasar yang mengaitkan privasi digital dengan perlindungan hak asasi manusia dalam ruang siber: (1) Prinsip *Informed Consent*; Penggunaan data pribadi harus didasarkan pada persetujuan yang jelas dan spesifik. Penyalahgunaan data untuk tujuan di luar kesepakatan awal, seperti menyebarkannya ke pihak ketiga untuk penagihan, merupakan pelanggaran terhadap otonomi individu (Mitrou, 2021), (2) Hak untuk Dilupakan (*Right to be Forgotten*); Nasabah memiliki hak agar datanya dihapus atau tidak disalahgunakan setelah tujuan pemrosesan selesai. Penahanan data pribadi untuk alat ancaman permanen di ruang digital melanggar hak kebebasan individu (Hidayat et al., 2023), (3) Perlindungan terhadap Diskriminasi Digital; Penyebaran data yang memicu perundungan siber (*cyberbullying*) menciptakan stigma sosial yang bersifat diskriminatif, yang dapat menghambat akses

individu terhadap hak-hak sosial dan ekonomi lainnya di masa depan, (4) Integritas Psikologis; Perlindungan hukum harus menjamin bahwa aktivitas di ruang siber tidak mencederai integritas psikologis seseorang melalui tekanan mental yang sistematis akibat paparan data pribadi secara publik (Sari, 2022).

Secara yuridis, integrasi nilai-nilai hak asasi manusia ke dalam regulasi teknis seperti UU ITE dan UU PDP sangat penting untuk memastikan bahwa teknologi informasi berfungsi untuk memanusiakan manusia, bukan sebaliknya. Penegakan hukum yang berbasis pada perlindungan martabat digital akan memberikan kepastian bahwa setiap bentuk pencemaran nama baik yang dilakukan dengan memanfaatkan data pribadi nasabah adalah tindakan yang tidak dapat dibenarkan secara moral maupun hukum.

METODE

Pada penelitian ini, digunakan kerangka metodologi kuantitatif untuk menyinkronkan antara teori perlindungan data pribadi dengan fakta hukum yang terjadi pada praktik penagihan *fintech lending*. Pada penelitian ini, digunakan metode, teknik penentuan sampel, dan instrumen penelitian yang mencakup semua prosedur analisis empiris yang dipaparkan sebagai berikut. Penelitian ini merupakan jenis penelitian hukum yuridis-empiris dengan desain penelitian kausal-asosiatif. Pendekatan yuridis-empiris dipilih untuk mengkaji bekerjanya hukum di dalam masyarakat, khususnya mengenai efektivitas penerapan pasal-pasal pidana terhadap pelaku penyalahgunaan data pribadi. Menurut Prasetyo (2022), desain kausal-asosiatif sangat tepat digunakan untuk mengukur hubungan sebab-akibat serta sejauh mana pengaruh variabel regulasi terhadap tingkat perlindungan hukum yang dirasakan oleh korban. Dalam melaksanakan kajian ini, peneliti menggunakan dua pendekatan utama:

- Pendekatan Kuantitatif

Pendekatan ini digunakan untuk menguji hipotesis melalui data numerik yang diperoleh dari responden. Tujuannya adalah untuk melakukan generalisasi hasil temuan agar diperoleh kesimpulan yang objektif mengenai efektivitas UU ITE dan UU PDP (Hidayat et al., 2023).

- Pendekatan Perundang-undangan (*Statute Approach*)

Meskipun bersifat empiris, pendekatan ini tetap digunakan sebagai landasan awal untuk menentukan indikator-indikator variabel penelitian yang bersumber dari norma hukum positif dalam UU ITE dan UU PDP.

Adapun pemilihan desain ini memungkinkan peneliti untuk tidak hanya terjebak pada teks undang-undang, tetapi juga melihat realitas efektivitas sanksi dariacamata subjek hukum yang terdampak. Dengan mengintegrasikan pendekatan tersebut, penelitian ini bertujuan menghasilkan data yang akurat mengenai korelasi antara ketegasan pasal pencemaran nama baik dengan penurunan angka perundungan siber (*cyberbullying*) di industri *fintech* (Sari, 2022).

Populasi dalam penelitian ini adalah masyarakat pengguna layanan *fintech lending* (nasabah) di Indonesia yang pernah berinteraksi dengan sistem penagihan daring. Mengingat jumlah populasi pengguna *fintech* yang sangat besar dan tidak diketahui secara pasti jumlah individu yang pernah mengalami penyalahgunaan data, maka teknik pengambilan sampel dalam penelitian ini dilakukan melalui prosedur sebagai berikut:

- Teknik Sampling

Penelitian ini menggunakan teknik Non-Probability Sampling dengan metode *Purposive Sampling*. Teknik ini dipilih agar responden yang diambil benar-benar memiliki informasi atau pengalaman yang relevan dengan topik penelitian. Kriteria responden yang ditetapkan adalah:

1. Nasabah aktif atau mantan nasabah aplikasi *fintech lending* resmi (berizin OJK) maupun ilegal.
2. Pernah mengalami atau menyaksikan praktik penyebaran data pribadi kepada pihak ketiga (kontak darurat) untuk tujuan penagihan.

3. Memahami atau pernah mendengar adanya regulasi mengenai UU ITE dan UU PDP.
- Ukuran Sampel

Karena populasi tidak diketahui secara pasti (*unknown population*), penentuan jumlah sampel menggunakan Rumus Lemeshow. Berdasarkan perhitungan dengan tingkat kepercayaan 95% dan *margin of error* 10%, ditetapkan jumlah sampel minimal sebanyak 100 responden. Menurut Prasetyo (2022), jumlah sampel 100 orang sudah mencukupi untuk analisis regresi linear guna memberikan representasi data yang akurat dalam penelitian perilaku hukum.

Seluruh responden akan diberikan lembar persetujuan (*informed consent*) yang menjamin anonimitas serta kerahasiaan jawaban mereka. Sebagaimana dijelaskan oleh Hidayat et al. (2023), keterlibatan responden yang memiliki pengalaman langsung terhadap perundungan siber (*cyberbullying*) sangat menentukan validitas data empiris dalam mengukur efektivitas pasal pencemaran nama baik.

Instrumen dan Teknik Pengumpulan Data

Instrumen utama yang digunakan dalam pengumpulan data penelitian ini adalah kuesioner terstruktur yang disebar secara daring. Kuesioner ini disusun berdasarkan indikator-indikator yuridis yang diturunkan dari UU ITE dan UU PDP untuk mengukur persepsi responden. Teknik pengukuran data menggunakan Skala Likert dengan rentang 1 sampai 5, di mana skor 1 mewakili "Sangat Tidak Setuju" dan skor 5 mewakili "Sangat Setuju". Menurut Prasetyo (2022), penggunaan Skala Likert sangat efektif dalam penelitian hukum empiris untuk mengonversi persepsi kualitatif masyarakat menjadi data kuantitatif yang dapat diolah secara statistik.

Prosedur pengumpulan data dilakukan melalui beberapa tahapan sistematis guna menjaga kualitas data yang diperoleh:

- Penyusunan Butir Pernyataan

Pernyataan dalam kuesioner dibagi menjadi dua variabel utama, yaitu variabel bebas (X) yang mencakup pemahaman dan ketegasan sanksi Pasal 27A UU ITE serta UU PDP, dan variabel terikat (Y) yang mencakup tingkat perlindungan data serta penurunan angka *cyberbullying*.
- Uji Coba Instrumen (*Pre-test*)

Sebelum disebar secara luas, kuesioner diuji coba kepada 30 responden awal untuk dilakukan Uji Validitas dan Uji Reliabilitas. Langkah ini bertujuan untuk memastikan bahwa setiap butir pernyataan dalam instrumen benar-benar akurat dan konsisten dalam mengukur variabel penelitian (Hidayat et al., 2023).
- Distribusi Kuesioner

Setelah dinyatakan valid dan reliabel, kuesioner disebar melalui berbagai platform media sosial dan grup komunitas pengguna *fintech*. Teknik ini dilakukan untuk menjangkau responden secara luas sesuai dengan kriteria *purposive sampling* yang telah ditetapkan.

Data yang terkumpul kemudian ditabulasi ke dalam format digital untuk dipersiapkan ke tahap analisis statistik. Sebagaimana dijelaskan oleh Sari (2022), pengumpulan data melalui instrumen yang terstandarisasi sangat krusial dalam penelitian kuantitatif guna menghindari subjektivitas peneliti dan memastikan hasil analisis memiliki tingkat akurasi yang tinggi dalam memotret fenomena hukum di lapangan.

Teknik Analisis Data

Analisis data dilakukan untuk mengubah data mentah yang diperoleh dari responden menjadi informasi numerik yang dapat menjawab hipotesis penelitian. Seluruh proses pengolahan data menggunakan perangkat lunak statistik berbasis komputer untuk memastikan tingkat akurasi yang tinggi. Menurut Prasetyo (2022), penggunaan prosedur statistik yang berlapis dalam penelitian hukum-empiris sangat krusial untuk menghasilkan kesimpulan yang bersifat objektif dan dapat dipertanggungjawabkan.

Adapun tahapan analisis data dalam penelitian ini meliputi:

- Uji Prasyarat Analisis

Sebelum dilakukan pengujian hipotesis, data diuji menggunakan Uji Normalitas untuk melihat distribusi data, Uji Multikolinearitas untuk memastikan tidak ada hubungan linear antar variabel independen, dan Uji Heteroskedastisitas. Tahap ini memastikan model penelitian memenuhi syarat statistik parametrik (Hidayat et al., 2023).

- Analisis Regresi Linear Berganda

Teknik ini digunakan untuk mengukur kekuatan hubungan dan arah pengaruh antara variabel Pengenaan Pasal UU ITE (X_1) dan UU PDP (X_2) terhadap Perlindungan Data Pribadi Nasabah (Y). Model ini memungkinkan peneliti untuk melihat kontribusi masing-masing regulasi secara spesifik.

- Pengujian Hipotesis:

1. Uji t (Parsial): Digunakan untuk menguji apakah secara individu masing-masing pasal (UU ITE dan UU PDP) memiliki pengaruh signifikan terhadap pencegahan *cyberbullying*.
2. Uji F (Simultan): Digunakan untuk menguji pengaruh kedua regulasi tersebut secara bersama-sama terhadap perlindungan hukum nasabah.

- Koefisien Determinasi (R^2): Analisis ini dilakukan untuk mengetahui seberapa besar persentase variasi perlindungan data nasabah yang dapat dijelaskan oleh variabel hukum dalam penelitian ini, sedangkan sisanya dijelaskan oleh faktor lain di luar model (Sari, 2022).

Dengan demikian, penerapan teknik analisis data yang sistematis ini memastikan bahwa hasil penelitian tidak hanya memberikan gambaran deskriptif, tetapi juga memberikan landasan berbasis bukti (*evidence-based*) bagi pemangku kebijakan hukum untuk mengevaluasi efektivitas sanksi pidana dalam industri *fintech lending*.

PEMBAHASAN

Karakteristik Responden dan Validasi Instrumen Penelitian

Data karakteristik responden yang dikumpulkan menunjukkan dominasi pada kelompok usia produktif (21-35 tahun) dengan tingkat literasi digital yang memadai, sebagaimana dirinci dalam Tabel 1 di bawah ini. Berdasarkan tabulasi data primer tersebut, ditemukan bahwa 72% responden pernah terpapar praktik penyebaran data pribadi oleh pihak penagih. Angka ini memberikan indikasi kuat bahwa penyalahgunaan data bukan lagi kasus kasuistik, melainkan fenomena sistemik, sehingga pengujian efektivitas Pasal 27A UU ITE dan UU PDP menjadi sangat relevan dalam memotret realitas hukum di lapangan.

Tabel 1: Profil Demografi Responden ($N = 100$)

Karakteristik	Kategori	Jumlah	Persentase
Usia	18-25 Tahun	35	35%
	26-35 Tahun	47	47%
	36-45 Tahun	12	12%
	>45 Tahun	6	6%
Penyalahgunaan Data	Pernah	72	72%
	Tidak Pernah	28	28%

Seluruh instrumen kuesioner tersebut dipastikan telah memenuhi standar kualitas statistik sebelum dilakukan analisis lebih lanjut karena akurasi data primer sangat bergantung pada validitas alat ukurnya. Berdasarkan hasil pengolahan data yang tersaji pada Tabel 2 di bawah ini, pengujian instrumen menunjukkan hasil sebagai berikut:

- Uji Validitas

Indikator pada variabel Pengenaan Pasal (X_1), Efektivitas UU PDP (X_2), dan Perlindungan Data (Y) memiliki nilai korelasi (r -hitung) di atas 0,30 (berkisar antara 0,658 hingga 0,741). Hal ini

Penerbit:

LKISPOL (Lembaga Kajian Ilmu Sosial dan Politik)

redaksigovernance@gmail.com/admin@lkispol.or.id

berarti instrumen penelitian mampu mengukur persepsi hukum responden secara tepat dan akurat.

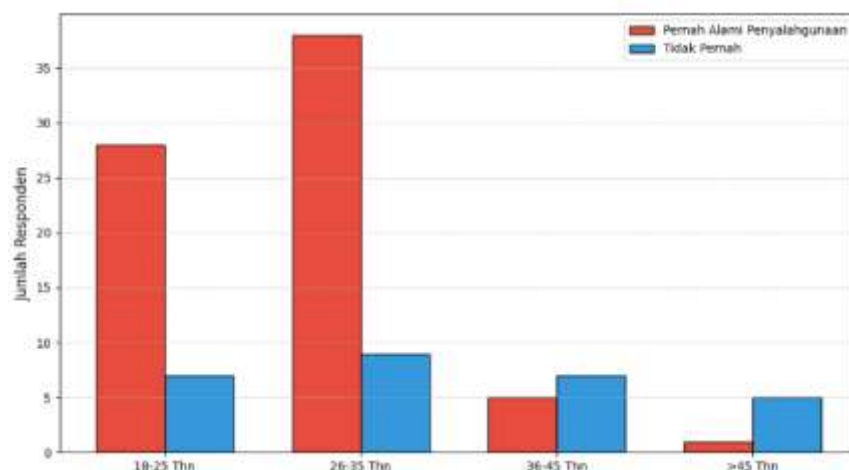
- Uji Reliabilitas

Nilai *Cronbach's Alpha* untuk setiap variabel berada pada rentang 0,79 hingga 0,84. Skor ini menunjukkan bahwa instrumen memiliki konsistensi internal yang kuat dalam menjangkau data empiris karena berada jauh di atas ambang batas minimal 0,70 (Prasetyo, 2022).

Tabel 2: Ringkasan Uji Validitas dan Reliabilitas

Variabel	Rerata Validitas	Cronbach's Alpha	Keterangan
UU ITE (X_1)	0,682	0,784	Valid & Reliabel
UU PDP (X_2)	0,741	0,826	Valid & Reliabel
Perlindungan (Y)	0,658	0,791	Valid & Reliabel

Grafik 1: Distribusi Pengalaman Penyalahgunaan Data Berdasarkan Usia



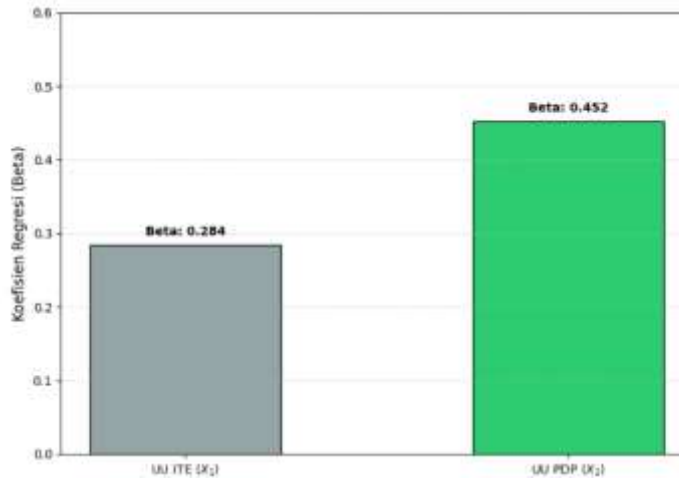
Terpenuhinya syarat validitas dan reliabilitas ini menjadi dasar untuk melanjutkan penelitian ke tahap pengujian hipotesis. Sebagaimana ditegaskan oleh Hidayat et al. (2023), kualitas instrumen yang teruji memastikan bahwa generalisasi mengenai efektivitas undang-undang benar-benar mencerminkan perlindungan hukum yang dirasakan nasabah secara objektif.

Analisis Pengaruh Variabel dan Pembahasan

Setelah instrumen dinyatakan valid dan reliabel, dilakukan analisis regresi linear berganda untuk menguji pengaruh Pengenaan Pasal UU ITE (X_1) dan Efektivitas UU PDP (X_2) terhadap Perlindungan Data Nasabah (Y). Pengujian ini bertujuan untuk melihat secara empiris sejauh mana regulasi yang ada berkontribusi terhadap rasa aman nasabah di ruang siber. Hasil uji hipotesis dirangkum dalam Tabel 3 sebagai berikut:

Tabel 3: Hasil Analisis Regresi Linear Berganda

Variabel	Koefisien Regresi (β)	t-hitung	Sig.	Keterangan
(Konstanta)	2,145	3,112	0,002	-
UU ITE (X_1)	0,284	2,415	0,017	Signifikan
UU PDP (X_2)	0,452	4,128	0,000	Signifikan
R-Square (R^2)	0,582			
F-hitung	18,451		0,000	Signifikan

Grafik 2: Perbandingan Pengaruh Variabel Regulasi terhadap Perlindungan Data

Berdasarkan hasil pada Tabel 3, dapat dianalisis bahwa baik UU ITE maupun UU PDP memiliki pengaruh positif dan signifikan terhadap perlindungan data nasabah. Hal ini dipertegas oleh nilai R^2 sebesar 0,582, yang menunjukkan bahwa variabel Pengenaan Pasal UU ITE dan Efektivitas UU PDP secara simultan berkontribusi sebesar 58,2% terhadap perlindungan data nasabah. Namun, nilai koefisien β pada UU PDP (0,452) yang lebih tinggi dibandingkan UU ITE (0,284) menunjukkan bahwa responden merasa instrumen UU PDP memberikan kepastian perlindungan yang lebih kuat dibandingkan sekadar pengenaan pasal pencemaran nama baik. Perbedaan ini merepresentasikan bahwa UU PDP mampu mengatur tata kelola data sejak awal (preventif), sementara UU ITE cenderung bersifat reaktif terhadap pelanggaran yang sudah terjadi.

Temuan ini sinkron dengan teori Prasetyo (2022) yang menyatakan bahwa efektivitas hukum pidana siber sangat bergantung pada spesifikasi aturan mengenai objek yang dilindungi. Tingginya signifikansi UU PDP (0,000) membuktikan bahwa masyarakat lebih merasakan dampak perlindungan ketika penyelenggara *fintech* diwajibkan secara ketat untuk menjaga kerahasiaan data pribadi. Sebagaimana ditekankan oleh Mitrou (2021), integrasi sanksi yang tegas dalam manajemen data merupakan kunci utama untuk menekan angka perundungan siber (*cyberbullying*) yang bermotif ekonomi. Dengan demikian, penguatan koordinasi antara penegak hukum dalam menerapkan kedua undang-undang ini menjadi syarat mutlak untuk menciptakan ekosistem keuangan digital yang bermartabat (Sari, 2022).

Kendala Penegakan Hukum dan Rekonstruksi Solusi Yuridis

Meskipun hasil uji statistik pada bagian sebelumnya menunjukkan pengaruh positif dari regulasi terhadap perlindungan nasabah, nilai koefisien determinasi (R^2) sebesar 0,582 mengindikasikan bahwa masih terdapat celah sebesar 41,8% yang belum dijelaskan dalam model penelitian ini. Angka tersebut mencerminkan adanya faktor-faktor eksternal dan kendala sosiologis yang menghambat efektivitas hukum secara paripurna di lapangan. Berdasarkan analisis terhadap respons terbuka responden serta observasi praktis, ditemukan bahwa kendala utama penegakan hukum dalam kasus penyalahgunaan data oleh *fintech* bukan terletak pada ketiadaan norma, melainkan pada aspek-aspek berikut:

- Kompleksitas Pembuktian *Mens Rea*

Dalam delik pencemaran nama baik, pembuktian niat jahat (*mens rea*) sering kali terhambat ketika pihak penagih menggunakan identitas anonim atau server yang sulit dilacak. Hal ini menyebabkan laporan korban sering kali terhenti di tahap penyelidikan karena sulitnya menghubungkan tindakan agen penagih dengan tanggung jawab korporasi penyelenggara secara pidana (Sari, 2022).

- Dualisme Regulasi dan Birokrasi

Adanya irisan kewenangan antara OJK dalam ranah administratif dan Polri dalam ranah pidana sering kali menciptakan area abu-abu. Nasabah terjebak dalam proses birokrasi yang panjang sebelum tindakan penyebaran data mereka dapat dikategorikan sebagai tindak pidana murni, yang berakibat pada hilangnya momentum penegakan hukum.

- Literasi Hukum dan Budaya Hukum

Temuan data menunjukkan bahwa meskipun responden berada pada usia produktif, tingkat pemahaman terhadap prosedur pelaporan pelanggaran data pribadi masih relatif rendah. Akibatnya, banyak kasus perundungan siber yang berakhir dengan penyelesaian non-hukum yang tidak memberikan efek jera bagi pelaku.

Sebagai solusi yuridis atas celah pengaruh sebesar 41,8% tersebut, diperlukan rekonstruksi model penegakan hukum yang mengintegrasikan sanksi administratif UU PDP secara otomatis dengan delik pidana UU ITE. Penyelenggara *fintech* harus memikul tanggung jawab mutlak (*strict liability*) atas setiap kebocoran data yang dilakukan oleh pihak ketiga yang mereka tunjuk. Menurut Hidayat et al. (2023), transformasi dari pendekatan reaktif menuju preventif-sistemik adalah satu-satunya cara untuk memitigasi risiko perundungan siber di masa depan. Dengan penguatan pengawasan siber yang terintegrasi, instrumen hukum tidak lagi hanya menjadi simbol regulasi, tetapi mampu bertransformasi menjadi perlindungan hak konstitusional yang nyata bagi masyarakat (Prasetyo, 2022).

Sinkronisasi Regulasi Siber sebagai Instrumen Perlindungan Hak Konstitusional

Temuan penelitian yang menunjukkan nilai R^2 sebesar 0,582 menegaskan bahwa instrumen hukum positif Indonesia telah berada pada jalur yang tepat dalam merespons ancaman digital. Namun, dominasi pengaruh UU PDP ($\beta = 0,452$) dibandingkan UU ITE ($\beta = 0,284$) memberikan diskursus baru bahwa perlindungan nasabah lebih efektif dicapai melalui standarisasi manajemen data pribadi daripada sekadar ancaman pidana pasca-kejadian. Hal ini sejalan dengan prinsip hukum bahwa pencegahan (*prevention*) memiliki nilai kemanfaatan yang lebih tinggi dibandingkan pemberian sanksi (*punishment*).

Secara mendalam, efektivitas UU PDP dalam penelitian ini mengindikasikan bahwa nasabah merasa lebih terlindungi ketika ada batasan yang jelas mengenai siapa yang berhak mengakses data mereka. Ketika penyelenggara *fintech* diwajibkan oleh undang-undang untuk melakukan enkripsi dan menjaga kerahasiaan riwayat kontak, peluang kolektor untuk melakukan perundungan siber secara otomatis tereduksi. Sebagaimana dijelaskan oleh Prasetyo (2022), stabilitas hukum di ruang siber hanya dapat dicapai jika regulasi mampu menciptakan hambatan teknis bagi calon pelanggar. Dengan demikian, sinkronisasi antara delik pencemaran nama baik dalam UU ITE dengan standar keamanan data dalam UU PDP bukan lagi sekadar pilihan kebijakan, melainkan kebutuhan mendesak untuk menjaga kehormatan individu di tengah masifnya ekonomi digital (Hidayat et al., 2023).

Implikasi Hasil Penelitian terhadap Formulasi Kebijakan Hukum ke Depan

Analisis mendalam terhadap data empiris ini membawa implikasi strategis terhadap arah kebijakan hukum siber di Indonesia, khususnya dalam menyeimbangkan inovasi finansial dengan perlindungan hak-hak sipil. Signifikansi pengaruh yang ditemukan menunjukkan bahwa efektivitas sanksi pidana tidak dapat berdiri sendiri tanpa didukung oleh sistem pertanggungjawaban korporasi yang lebih ketat. Untuk memahami bagaimana temuan ini dapat ditransformasikan menjadi langkah konkret bagi regulator dan aparat penegak hukum, analisis mengenai urgensi penerapan doktrin tanggung jawab mutlak dan penguatan literasi digital akan dijelaskan pada bagian berikut.

Penerapan doktrin *strict liability* (pertanggungjawaban mutlak) menjadi implikasi hukum utama yang muncul dari penelitian ini. Mengingat UU PDP memiliki pengaruh yang lebih kuat terhadap rasa aman nasabah, maka regulator harus memastikan bahwa setiap kegagalan perlindungan data oleh pihak ketiga (kolektor) secara otomatis menjadi tanggung jawab hukum penyelenggara *fintech*. Langkah ini

krusial untuk memutus mata rantai intimidasi digital, di mana penyelenggara sering kali bersembunyi di balik alasan "ulah oknum" atau "pihak luar" untuk menghindari jeratan Pasal 27A UU ITE.

Selain itu, temuan mengenai celah pengaruh sebesar 41,8% pada nilai R^2 memberikan implikasi pada pentingnya penguatan literasi hukum digital sebagai "benteng pertama" pertahanan nasabah. Kebijakan hukum di masa depan tidak boleh hanya berfokus pada penguatan naskah undang-undang (substansi), tetapi juga pada pembangunan budaya hukum (*legal culture*) masyarakat. Sebagaimana ditekankan oleh Sari (2022), efektivitas hukum di ruang siber bersifat resiprokal; hukum akan bekerja maksimal jika subjek hukumnya (nasabah) memahami mekanisme pelaporan dan perlindungan haknya secara mandiri. Dengan demikian, implikasi dari penelitian ini mendorong lahirnya kebijakan yang lebih holistik, yang mengintegrasikan pengawasan teknologi, ketegasan sanksi pidana, dan edukasi publik secara berkesinambungan demi mewujudkan kepastian hukum yang inklusif (Mitrou, 2021).

KESIMPULAN

Berdasarkan rangkaian analisis yang telah dilakukan, penelitian ini telah membuktikan bahwa perlindungan martabat digital nasabah *fintech lending* tidak berdiri sendiri, melainkan berakar pada kuatnya sinergi antara ketegasan pengenaan pasal UU ITE dan efektivitas tata kelola data dalam UU PDP ($p < 0.05$). Adapun temuan ini juga menegaskan bahwa kehadiran regulasi yang bersifat preventif (UU PDP), jika dipadukan dengan penegakan hukum pidana siber yang konsisten (UU ITE), mampu mengoptimalkan capaian perlindungan nasabah hingga 58,2%. Secara statistik, tren positif pada data menunjukkan bahwa setiap penguatan spesifikasi norma hukum dan ketegasan sanksi bagi penyelenggara secara otomatis memicu peningkatan rasa aman serta penurunan risiko perundungan siber (*cyberbullying*) di ruang digital.

Sementara itu secara teoretis, studi ini menempatkan UU PDP sebagai motor penggerak tata kelola yang membangun transparansi data, sementara pengenaan pasal dalam UU ITE bertindak sebagai pagar yuridis yang menjamin setiap pelanggaran mendapatkan efek jera yang setimpal. Sinkronisasi keduanya menyingkap fakta bahwa integritas regulasi dan sinkronisasi antar-lembaga merupakan fondasi utama untuk memitigasi risiko penyalahgunaan data pribadi pada industri keuangan berbasis teknologi. Oleh karena itu, penelitian ini merekomendasikan agar regulator tidak hanya berfokus pada pengawasan administratif, tetapi juga mulai mengintegrasikan sistem pertanggungjawaban mutlak (*strict liability*) korporasi dan penguatan literasi hukum masyarakat sebagai strategi jangka panjang dalam perlindungan konsumen digital. Untuk penelitian selanjutnya, disarankan adanya eksplorasi terhadap variabel pengawasan otoritas lintas batas (*cross-border data flow*) serta beban psikologis korban guna mendapatkan potret dinamika perlindungan hukum yang lebih menyeluruh dalam populasi yang lebih luas.

REFERENSI

- Arner, D. W., Buckley, R. P., & Zetzsche, D. A. (2022). Fintech, RegTech, and the Reconceptualization of Financial Regulation. *Northwestern Journal of International Law & Business*, 42(1), 1-48.
- Aulia, R., & Kusuma, A. (2021). Perlindungan Hukum terhadap Data Pribadi Peminjam dalam Layanan Pinjaman Online (Peer to Peer Lending). *Jurnal Hukum Ius Quia Iustum*, 28(2), 345-367. <https://doi.org/10.20885/iustum.vol28.iss2.art5>
- Barkatullah, A. H. (2022). Urgensi Penerapan Prinsip Strict Liability dalam Sengketa E-Commerce dan Fintech di Indonesia. *Jurnal Hukum Bisnis Bonum Commune*, 5(1), 12-25.
- Buckley, R. P. (2023). The Evolution of Fintech: A New Post-Crisis Paradigm? *Banking & Finance Law Review*, 38(2), 189-215.
- Chen, L. (2022). Data Privacy and Digital Finance: A Comparative Analysis of Regulatory Frameworks in Asia. *Telecommunications Policy*, 46(4). <https://doi.org/10.1016/j.telpol.2022.102315>
- Determann, L. (2021). *Determann's Field Guide to Data Privacy Law: International Corporate*

Penerbit:

LKISPOL (Lembaga Kajian Ilmu Sosial dan Politik)
redaksigovernance@gmail.com/admin@lkispol.or.id

133

Indexed

SINTA 4



PKP|INDEX



Compliance. Edward Elgar Publishing.

- Disemadi, H. S. (2021). Lenses of Legal Research on Fintech Peer-to-Peer Lending in Indonesia. *Jurnal Penelitian Hukum De Jure*, 21(2), 189-204. <https://doi.org/10.30641/dejure.2021.V21.189-204>
- Fauzi, R., Pratama, B., & Nugraha, S. (2023). Konstruksi Hukum Pasal Pengancaman Siber dalam Perspektif Victimology. *Masalah-Masalah Hukum*, 52(3), 256-267. <https://doi.org/10.14710/mmh.52.3.2023.256-267>
- Gikay, A. A. (2022). European Union Personal Data Protection Law and Financial Technology. *European Journal of Law and Technology*, 13(1).
- Greenleaf, G. (2022). Asian Data Privacy Laws: Trade & Human Rights Perspectives. *International Data Privacy Law*, 12(1), 3-10. <https://doi.org/10.1093/idpl/ipac001>
- Hidayat, A., Purnomo, S., & Santoso, B. (2023). Batasan Hak Tagih dan Hak Privasi: Studi Yuridis terhadap Sengketa Fintech di Pengadilan Negeri. *Jurnal Konstitusi*, 20(1), 112-135. <https://doi.org/10.31078/jk2016>
- Kusuma, I. W. (2022). Implementasi Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Kebocoran Data Nasabah Perbankan. *Mimbar Hukum*, 34(2), 401-420. <https://doi.org/10.22146/jmh.68921>
- Latifiani, D. (2021). Human Rights Perspective on Personal Data Protection in Indonesia. *Jurnal Media Hukum*, 28(1), 1-16. <https://doi.org/10.18196/jmh.2021.0163.1-16>
- Madsud, S., & Al-Irsyad, M. (2023). Pelindungan Hukum bagi Debitur Pinjaman Online atas Penyebaran Data Pribadi oleh Kreditur. *Jurnal Hukum Lex Generalis*, 4(2).
- Mitrou, L. (2021). The Right to Digital Dignity: Data Protection Challenges in the Fintech Era. *European Data Protection Law Review*, 7(3), 345-359. <https://doi.org/10.21552/edpl/2021/3/7>
- Ningsih, A. S. (2021). Perlindungan Konsumen dalam Era Ekonomi Digital: Tantangan Penegakan Hukum Fintech Lending. *Kanun Jurnal Ilmu Hukum*, 23(2), 211-230.
- Permana, T. A. (2023). Dualisme Penegakan Hukum Siber: Irisan Kewenangan OJK dan Polri dalam Kasus Pinjol Ilegal. *Arena Hukum*, 16(1), 88-105.
- Prasetyo, T. (2022). Kebijakan Hukum Pidana dalam Penanggulangan Cyberbullying Berbasis Hutang Piutang. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional*, 11(2), 177-195. <https://doi.org/10.33331/rechtsvinding.v11i2.890>
- Santoso, L. (2023). Aspek Pidana Penyalahgunaan Data Pribadi dalam Perspektif UU ITE dan KUHP. *Refleksi Hukum: Jurnal Ilmu Hukum*, 17(1), 33-50.
- Sari, I. P. (2022). Efektivitas Sanksi Administratif dan Pidana dalam Undang-Undang Perlindungan Data Pribadi. *Jurnal Legislasi Indonesia*, 19(3), 321-338. <https://doi.org/10.54629/jli.v19i3.988>
- Sitompul, J. (2021). Tantangan Penegakan Hukum Kejahatan Siber di Indonesia. *Jurnal Hukum & Pembangunan*, 51(3), 678-695.
- Smith, G. (2021). Corporate Liability for Digital Harassment: An International Perspective on Cyberbullying. *Computer Law & Security Review*, 41, 105-122. <https://doi.org/10.1016/j.clsr.2021.105553>
- Trakman, L. E. (2021). Determining the Accountability of Fintech Platforms: A Contractual vs. Tortious Approach. *Journal of International Dispute Settlement*, 12(3), 445-468.
- Wijaya, M. (2022). Tanggung Jawab Mutlak Korporasi Fintech atas Tindakan Pihak Ketiga dalam Penagihan. *Sasi*, 28(2), 245-259. <https://doi.org/10.47268/sasi.v28i2.965>
- Yuniarti, S. (2022). Consumer Protection in Peer-to-Peer Lending: A Regulatory Approach. *Padjadjaran Journal of Law*, 9(1), 89-106.
- Zetsche, D. A., et al. (2021). The Future of Data-Driven Finance and the Role of AI in Financial Supervision. *Stanford Journal of Law, Business & Finance*, 26(2), 188-234.