Begawan Abioso
(Volume 17, Nomor 1, Juni 2026)
P-ISSN: 1858-2990 I E-ISSN: 2810-0727
Open access at: https://ejournal.hukumunkris.id/index.php/abioso

Kebijakan Hukum Pidana Penipuan Penyalahgunaan Teknologi Dalam Pengajuan Pinjaman Bank di Indonesia

[a] **Sherly Tan,** [a] **Abdurrakhman Alhakim**[*], [a] **Emiliya Febriyani**
[a] Universitas Internasional Batam, Batam, Indonesia

Submitted: 11-05-2026 Revised: 28-05-2026 Accepted: 09-06-2026 Published: 13-06-2026

Abstrak

Penelitian ini bertujuan untuk menganalisis kebijakan hukum pidana di Indonesia dalam menanggulangi tindak pidana penipuan pada pengajuan pinjaman bank yang dilakukan melalui penyalahgunaan teknologi, serta mengkaji efektivitas pendekatan preventif dan represif dalam praktik penegakan hukum. Metode penelitian yang digunakan adalah yuridis normatif dengan menelaah ketentuan hukum positif, antara lain Kitab Undang-Undang Hukum Pidana (KUHP) Baru, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta regulasi sektor perbankan yang berkaitan dengan pinjaman berbasis teknologi. Kebaruan penelitian ini terletak pada evaluasi kritis terhadap keterbatasan Pasal 492 KUHP Baru dalam menjangkau kejahatan siber, serta analisis penerapan prinsip *lex specialis* melalui Pasal 35 dan Pasal 51 UU ITE dalam menangani manipulasi data elektronik pada proses pengajuan pinjaman bank. Selain itu, penelitian ini menawarkan pendekatan kebijakan pidana yang terintegrasi antara hukum pidana, regulasi perbankan, sistem verifikasi digital, dan literasi digital masyarakat. Hasil penelitian menunjukkan bahwa modus penipuan umumnya melibatkan manipulasi identitas, pemalsuan dokumen elektronik, serta penyalahgunaan data pribadi. Penegakan hukum masih menghadapi kendala teknis dan yurisdiksional, sedangkan upaya preventif terhambat oleh rendahnya literasi digital dan lemahnya sistem verifikasi. Oleh karena itu, diperlukan kebijakan yang komprehensif melalui penguatan keamanan siber, peningkatan kapasitas aparat penegak hukum, dan kolaborasi lintas sektor.

Kata Kunci: Bank; Hukum Pidana; Penipuan; Teknologi.

Abstract

This study aims to analyze Indonesia's criminal law policy in addressing fraudulent practices in bank loan applications committed through the misuse of technology, as well as to examine the effectiveness of preventive and repressive approaches in law enforcement practices. The research employs a normative juridical method by examining relevant positive legal provisions, including the New Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law (ITE Law), and banking regulations related to technology-based lending. The novelty of this study lies in its critical evaluation of the limitations of Article 492 of the New Criminal Code in addressing cybercrime, as well as its analysis of the application of the lex specialis principle through Articles 35 and 51 of the ITE Law in dealing with the manipulation of electronic data during the bank loan application process. Furthermore, this study proposes an integrated criminal policy approach that combines criminal law, banking regulations, digital verification systems, and public digital literacy. The findings reveal that fraudulent schemes commonly involve identity manipulation, falsification of electronic documents, and the misuse of personal data. Law enforcement efforts continue to face technical and jurisdictional challenges, while preventive measures are hindered by low levels of digital literacy and weaknesses in verification systems. Therefore, a comprehensive policy framework is required through the strengthening of cybersecurity measures, the enhancement of law enforcement capacity, and cross-sectoral collaboration.

Keywords: *Banking; Criminal Law; Fraud; Technology.*

* **Email koresponden:** alhakim@uib.ac.id

A. Pendahuluan

Perkembangan teknologi informasi selain memberikan berbagai manfaat, juga menimbulkan dampak negatif berupa meningkatnya tindak pidana yang dilakukan melalui media elektronik. Kondisi tersebut menuntut adanya pengaturan hukum yang mampu memberikan perlindungan hukum bagi masyarakat (Alhakim & Sofia, 2021). Laporan Otoritas Jasa Keuangan melalui Indonesia Anti-Scam Centre menunjukkan bahwa angka penipuan berbasis transaksi elektronik telah mencapai tingkat yang mengkhawatirkan. Data resmi mencatat sebanyak 42.257 laporan penipuan yang berkaitan dengan manipulasi identitas, pemalsuan dokumen elektronik, dan pengambilalihan akses akun keuangan. Angka tersebut menunjukkan bahwa perkembangan teknologi telah memberikan ruang bagi pelaku untuk memanfaatkan celah keamanan digital pada sektor keuangan.

Sistem pendataan IASC mengungkapkan adanya 70.390 rekening yang terindikasi terlibat dalam tindak penipuan, sementara 19.980 rekening telah diblokir sebagai langkah mitigasi guna mencegah meluasnya kerugian yang dialami korban. Fenomena ini menunjukkan bahwa pola kejahatan semakin terstruktur, sistematis, dan memanfaatkan teknologi sebagai instrumen utama. Oleh karena itu, lembaga keuangan menghadapi tantangan serius dalam menjaga integritas sistem perbankan. Total kerugian finansial yang dialami korban mencapai sekitar Rp700,2 miliar, yang menunjukkan bahwa dampak penipuan berbasis teknologi tidak hanya bersifat individual, tetapi juga memiliki dimensi sistemik terhadap stabilitas sektor keuangan.

Dalam konteks tersebut, lembaga penegak hukum dituntut memiliki kemampuan analitis dan teknis yang memadai karena tindak penipuan elektronik melibatkan bukti digital yang kompleks serta sering kali bersifat lintas yurisdiksi. Situasi ini menuntut hadirnya kebijakan hukum pidana yang mampu memberikan perlindungan yang efektif bagi masyarakat serta mewujudkan kepastian hukum bagi seluruh pihak yang melakukan kegiatan perbankan (Yulenrivo dkk., 2023). Dengan demikian, sistem hukum dituntut untuk menyesuaikan perangkat normatif maupun mekanisme penegakannya agar mampu merespons kejahatan modern yang bersifat dinamis dan berkembang dengan sangat cepat (Putri, 2025).

Dalam perspektif hukum pidana, penipuan merupakan perbuatan tipu daya yang merugikan harta kekayaan pihak lain. Pengaturan mengenai tindak pidana penipuan dalam hukum positif Indonesia saat ini tercantum dalam Pasal 492 Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (selanjutnya disebut KUHP Baru). Ketentuan tersebut merumuskan penipuan sebagai perbuatan melawan hukum yang dilakukan melalui penggunaan nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kebohongan yang mengakibatkan penyerahan barang, pemberian utang, pembuatan pengakuan utang, atau penghapusan piutang sehingga menimbulkan kerugian, termasuk dalam konteks kejahatan berbasis teknologi. Oleh karena itu, muncul kebutuhan yang mendesak untuk mengkaji sejauh mana kebijakan hukum pidana saat ini mampu mengakomodasi bentuk-bentuk baru tindak pidana penipuan, terutama yang berkaitan dengan pemanfaatan teknologi dalam sektor perbankan (Anggun, 2022).

Selain KUHP, Indonesia juga memiliki regulasi khusus yang relevan, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya melalui Undang-Undang Nomor 19 Tahun 2016. Pasal 35 UU ITE mengatur bahwa setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum memanipulasi, menciptakan, mengubah, menghilangkan, atau merusak informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi atau dokumen

tersebut dianggap sebagai data yang autentik dapat dipidana. Ketentuan ini memiliki relevansi yang kuat terhadap praktik penipuan pinjaman bank secara daring yang dilakukan melalui pemalsuan data digital. Meskipun demikian, penerapan ketentuan tersebut dalam praktik peradilan tidak selalu mudah karena memerlukan pembuktian teknis yang kompleks, serta kemampuan penyidik dan aparat penegak hukum dalam memahami aspek forensik digital (*digital forensic*) (Gurning, 2022).

Bank sebagai lembaga keuangan yang menjadi sasaran tindak pidana memiliki tanggung jawab besar untuk menerapkan teknologi verifikasi ganda (*two-factor authentication*), kecerdasan buatan (*artificial intelligence*/AI) untuk mendeteksi *fraud*, serta sistem perlindungan data yang memadai (Pakpahan dkk., 2020). Upaya tersebut perlu dilakukan sebagai bentuk penerapan prinsip kehati-hatian berbasis AI dalam mencegah terjadinya penipuan melalui penyalahgunaan teknologi pada pengajuan pinjaman bank. Sistem evaluasi hukum pidana juga harus menyesuaikan diri dengan kompleksitas kejahatan siber yang terus berkembang.

Hal ini selaras dengan teori kebijakan hukum pidana yang dikemukakan oleh Marc Ancel dan Barda Nawawi Arief, bahwa hukum pidana tidak hanya berfungsi sebagai alat pembalasan, tetapi juga sebagai instrumen pengendalian sosial yang adaptif dan fungsional. Oleh karena itu, hukum pidana harus senantiasa berkembang mengikuti dinamika sosial dan kemajuan teknologi serta mampu memberikan kepastian hukum, keadilan, dan kemanfaatan secara seimbang (Permata & Haryanto, 2022).

Penipuan yang dilakukan melalui penyalahgunaan teknologi dalam pengajuan pinjaman bank memerlukan penegakan hukum pidana yang tegas guna melindungi sistem perbankan, memberikan efek jera kepada pelaku, serta mencegah terjadinya penyalahgunaan teknologi keuangan. Penelitian ini bertujuan untuk menganalisis kebijakan hukum pidana Indonesia dalam merespons tindak penipuan yang dilakukan melalui penyalahgunaan teknologi dalam pengajuan pinjaman bank dengan menggunakan pendekatan yuridis normatif melalui kajian terhadap peraturan perundang-undangan, doktrin, dan putusan pengadilan. Hasil penelitian ini diharapkan dapat memberikan kontribusi bagi reformulasi hukum pidana yang lebih responsif, efektif, dan berkeadilan, serta menjadi masukan bagi akademisi, praktisi hukum, dan pembuat kebijakan di bidang perbankan dan teknologi informasi (Kristian, 2022).

Adapun orisinalitas penelitian ini ditunjukkan melalui kajian terhadap penelitian terdahulu sebagai pembanding untuk menegaskan bahwa penelitian yang dilakukan memiliki gagasan dan fokus kajian yang berbeda. Penelitian pertama dilakukan oleh Fasa Muhamad Hapid, Ija Suntana, dan Muhammad Yayan Royani pada tahun 2024 dengan judul *"Penerapan Asas Geen Straf Zonder Schuld dalam Penindakan terhadap Kejahatan Penyalahgunaan Teknologi Deepfake"*. Penelitian tersebut membahas respons hukum pidana terhadap penyalahgunaan teknologi *deepfake* dengan menekankan penerapan asas *geen straf zonder schuld* sebagai dasar pertanggungjawaban pidana pelaku. Hasil penelitian menunjukkan bahwa asas kesalahan tetap menjadi landasan utama dalam penindakan terhadap pelaku penyalahgunaan teknologi kecerdasan artifisial. Selain itu, penelitian tersebut menyoroti peran Surat Edaran Menteri Komunikasi dan Informatika Nomor 9 Tahun 2023 sebagai pedoman etika dalam penggunaan kecerdasan artifisial (Hapid dkk., 2024).

Penelitian kedua dilakukan oleh Zainudin Hasan, Anisa Merti Ayu, Chinthia Dita M., Mayse Trisnawati, dan M. Ardan Aldika R.A. pada tahun 2024 dengan judul *"Penanggulangan*

Tindak Pidana Penipuan Melalui Transfer Mobile Banking". Penelitian tersebut mengkaji perkembangan teknologi informasi di sektor perbankan serta risiko kejahatan siber yang muncul akibat rendahnya tingkat kewaspadaan masyarakat terhadap keamanan data perbankan. Hasil penelitian menegaskan bahwa kemajuan teknologi memberikan kemudahan dalam transaksi keuangan, tetapi pada saat yang sama meningkatkan risiko pencurian data dan penipuan digital. Oleh karena itu, diperlukan implementasi hukum yang efektif guna memberikan perlindungan kepada masyarakat dari kerugian finansial yang ditimbulkan oleh kejahatan tersebut (Hasan dkk., 2024).

Penelitian ini mengkaji praktik manipulasi data elektronik, pemalsuan identitas digital, dan penyalahgunaan teknologi yang digunakan untuk memperoleh fasilitas kredit secara melawan hukum pada sektor perbankan. Kajian ini menelaah keterkaitan antara ketentuan dalam KUHP Baru, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), dan regulasi Otoritas Jasa Keuangan sebagai satu kesatuan sistem hukum dalam penanggulangan penipuan digital. Kebaruan penelitian ini terletak pada perumusan konsep kebijakan hukum pidana *digital banking fraud* yang terintegrasi sebagai kerangka konseptual dalam penanggulangan penipuan berbasis teknologi pada pengajuan pinjaman bank. Konsep tersebut mengintegrasikan pendekatan penal melalui penerapan hukum pidana, pendekatan regulatif melalui penguatan pengawasan sektor perbankan, pendekatan teknologis melalui optimalisasi verifikasi identitas dan keamanan digital, serta pendekatan kolaboratif melalui sinergi antarinstansi penegak hukum dan lembaga jasa keuangan.

Konstruksi model tersebut dibangun melalui evaluasi terhadap keterbatasan Pasal 492 KUHP Baru dalam menjangkau karakteristik kejahatan digital serta melalui analisis relevansi Pasal 35 dan Pasal 51 UU ITE sebagai dasar pemidanaan atas manipulasi informasi elektronik dalam proses pengajuan pinjaman bank. Hasil penelitian ini tidak hanya memberikan analisis terhadap hukum positif yang berlaku, tetapi juga menawarkan formulasi kebijakan hukum pidana yang lebih adaptif terhadap perkembangan *digital banking fraud* di Indonesia.

B. Metode

Penelitian ini menggunakan pendekatan yuridis normatif dengan pengembangan yang lebih komprehensif untuk menganalisis kebijakan hukum pidana terkait penipuan melalui penyalahgunaan teknologi dalam pengajuan pinjaman bank. Selain mengkaji norma hukum positif, metode ini diperkaya dengan pendekatan perbandingan hukum (*comparative approach*) secara terbatas, khususnya untuk mengidentifikasi praktik terbaik (*best practices*) dari yurisdiksi lain yang relevan dalam menanggulangi kejahatan serupa. Pendekatan tersebut bertujuan untuk memberikan rekomendasi kebijakan hukum pidana yang lebih adaptif dan efektif di Indonesia.

Penelitian ini menitikberatkan pada analisis bahan hukum. Bahan hukum yang digunakan meliputi bahan hukum primer berupa peraturan perundang-undangan, bahan hukum sekunder berupa doktrin dan literatur hukum, serta bahan hukum yang memberikan penjelasan terhadap kedua jenis bahan hukum tersebut (Rishadi dkk., 2022). Penelitian ini mencakup pendekatan perundang-undangan (*statute approach*), pendekatan konseptual, pendekatan kasus, dan pendekatan perbandingan hukum untuk menganalisis perlindungan data pribadi dalam pengajuan pinjaman bank berbasis teknologi informasi.

Sumber data terdiri atas bahan hukum primer berupa Kitab Undang-Undang Hukum Pidana (KUHP), Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Pelindungan Data Pribadi (UU PDP), serta regulasi Otoritas Jasa Keuangan (OJK). Selain itu, penelitian ini juga menggunakan bahan hukum sekunder berupa buku, jurnal, dan hasil penelitian, serta bahan hukum tersier berupa kamus hukum dan ensiklopedia. Data dikumpulkan melalui studi kepustakaan (*library research*) dan dianalisis secara kualitatif normatif. Analisis difokuskan pada kejahatan pencurian data pribadi, upaya penanggulangannya, serta aspek yuridis dan teknis dalam penegakan hukum terkait pelindungan data pribadi pada layanan pinjaman berbasis teknologi informasi.

C. Hasil dan Pembahasan

C.1 Kebijakan Hukum Pidana Terkait Penipuan Penyalahgunaan Teknologi Dalam Pengajuan Pinjaman Bank di Indonesia

Perkembangan teknologi informasi telah meningkatkan risiko penipuan dalam layanan perbankan, termasuk melalui pemalsuan identitas, manipulasi data, dan rekayasa dokumen elektronik untuk memperoleh kredit secara melawan hukum. Dalam hukum positif Indonesia, perbuatan tersebut dapat dikualifikasikan sebagai tindak pidana berdasarkan Pasal 492 KUHP Baru karena memenuhi unsur tipu muslihat atau rangkaian kebohongan untuk menggerakkan pihak lain menyerahkan hak atau memberikan kredit (Sipayung & Amelya, 2022). Penipuan diatur dalam Pasal 492 KUHP Baru sebagai perbuatan memperoleh keuntungan secara melawan hukum melalui penggunaan nama palsu, kedudukan palsu, tipu muslihat, atau rangkaian kebohongan, dengan ancaman pidana penjara paling lama empat tahun atau pidana denda paling banyak kategori V sebesar Rp500.000.000. Dalam pengajuan pinjaman bank, pemalsuan identitas atau rekayasa dokumen, seperti slip gaji, laporan keuangan, atau bukti agunan, untuk memperoleh kredit memenuhi unsur tipu muslihat dan rangkaian kebohongan sehingga dapat dikualifikasikan sebagai tindak pidana penipuan (Muhammad & Harefa, 2023).

Seiring dengan berkembangnya penipuan berbasis teknologi, Pasal 492 KUHP Baru dinilai belum memadai sehingga diperlukan pengaturan yang lebih khusus melalui UU ITE. Dalam perspektif Teori Marc Ancel, kebijakan hukum pidana harus berorientasi pada perlindungan masyarakat dan mampu menyesuaikan diri dengan perkembangan teknologi. Oleh karena itu, pelaku yang mengajukan pinjaman menggunakan data elektronik palsu dapat dijerat dengan Pasal 35 UU ITE karena melakukan manipulasi dokumen elektronik agar dianggap autentik (Azis & Redi, 2023). Selain Pasal 35 UU ITE, pelaku juga dapat dijerat dengan Pasal 51 ayat (1) UU ITE yang mengancam pelaku dengan pidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp12 miliar. Ketentuan ini menunjukkan penerapan asas *lex specialis* dalam penanggulangan penipuan berbasis teknologi yang memiliki dampak luas dan relatif sulit dideteksi (Ayunda & Rusdianto, 2021).

Penggunaan identitas orang lain tanpa izin untuk mengajukan pinjaman bank merupakan bentuk penipuan yang dapat menimbulkan kerugian ekonomi dan memenuhi unsur Pasal 495 KUHP Baru, terutama apabila dilakukan melalui pemberian informasi yang tidak benar, penggunaan identitas palsu, atau pemalsuan dokumen yang memengaruhi proses penilaian kredit oleh bank. Apabila disertai dengan akses ilegal terhadap sistem elektronik, perbuatan tersebut juga dapat dijerat berdasarkan Pasal 30 UU ITE. Untuk mencegah terjadinya kejahatan ini, diperlukan penguatan sistem verifikasi digital melalui

penggunaan biometrik, verifikasi berlapis, pemanfaatan kecerdasan buatan (*artificial intelligence*/AI) untuk mendeteksi pengajuan yang mencurigakan, serta peningkatan literasi digital masyarakat (Utami & Astuti, 2023).

Namun, penegakan hukum terhadap tindak pidana tersebut masih menghadapi berbagai kendala, seperti manipulasi jejak digital, pelaku yang beroperasi lintas wilayah atau lintas negara, serta keterbatasan kemampuan forensik digital. Oleh karena itu, diperlukan penguatan kapasitas aparat penegak hukum, pengembangan infrastruktur digital, dan peningkatan kerja sama internasional dalam penanganan kejahatan siber (Satria & Handoyo, 2022).

Fenomena tersebut terlihat pada kasus kredit fiktif di bank digital, ketika pelaku menggunakan identitas orang lain atau mengeksploitasi celah keamanan sistem untuk memperoleh dana kredit secara melawan hukum. Perbuatan tersebut pada akhirnya berujung pada pemidanaan oleh pengadilan (Wardhana, 2023).

Dari perspektif Teori *Deterrence*, kebijakan pemidanaan terhadap penipuan berbasis teknologi bertujuan menciptakan efek jera melalui ancaman pidana dan kepastian penegakan hukum, dengan asumsi bahwa individu akan menghindari kejahatan apabila risiko hukuman yang dihadapi lebih besar daripada keuntungan yang diperoleh (Rivanie dkk., 2022). Oleh karena itu, keberadaan Pasal 35 jo. Pasal 51 ayat (1) UU ITE yang mengancam pelaku dengan pidana penjara paling lama 12 tahun dan denda paling banyak Rp12 miliar harus didukung oleh penegakan hukum yang konsisten serta penguatan sistem verifikasi digital. Dengan demikian, kebijakan hukum pidana terhadap penipuan berbasis teknologi dalam pengajuan pinjaman bank perlu dilaksanakan secara terpadu melalui regulasi yang adaptif, penegakan hukum yang profesional, dan pelaksanaan pidana yang efektif guna melindungi sistem perbankan serta menjaga stabilitas sektor keuangan (Rivanie dkk., 2022).

Kebijakan hukum pidana terhadap penipuan digital dalam pengajuan pinjaman bank harus menjunjung tinggi keadilan dan kepastian hukum dengan menindak tegas pelaku tanpa mengabaikan perlindungan bagi korban penyalahgunaan identitas. Oleh karena itu, proses penyidikan, penuntutan, dan pemidanaan harus dilakukan secara cermat untuk mencegah terjadinya kriminalisasi yang tidak tepat (Yuwono & Hoesein, 2022). Dalam menghadapi transformasi ekonomi digital, harmonisasi antara KUHP Baru, UU ITE, dan regulasi perbankan, seperti POJK, menjadi suatu keharusan dalam mewujudkan perlindungan hukum yang menyeluruh. Oleh karena itu, penguatan kebijakan hukum pidana perlu dilakukan melalui regulasi yang adaptif, kolaborasi antarlembaga, serta peningkatan edukasi dan literasi digital agar mampu menanggulangi kejahatan siber secara efektif dan berkelanjutan (Ramadhani, 2022).

C.2 Upaya Penanggulangan Tindak Pidana Penipuan Penyalahgunaan Teknologi Dalam Pengajuan Pinjaman Bank di Indonesia

Perkembangan teknologi informasi telah mempermudah proses pengajuan pinjaman bank secara digital sehingga nasabah dapat mengakses layanan melalui telepon seluler tanpa harus melakukan tatap muka secara langsung. Meskipun meningkatkan efisiensi layanan, digitalisasi juga membuka peluang terjadinya penipuan berbasis teknologi, seperti penggunaan identitas palsu, pemalsuan dokumen, rekayasa data, dan manipulasi sistem perbankan digital. Oleh karena itu, diperlukan upaya penanggulangan yang efektif, sistematis, dan terintegrasi agar tindak kejahatan tersebut dapat dicegah serta ditindak

secara tegas sesuai dengan ketentuan hukum yang berlaku di Indonesia (Habibi & Liviani, 2020).

Penanggulangan penipuan berbasis teknologi dalam pengajuan pinjaman bank meliputi pendekatan preventif (pencegahan) dan represif (penindakan). Kedua pendekatan tersebut harus dilaksanakan secara seimbang dan sinergis dalam kerangka sistem peradilan pidana serta pengawasan terhadap teknologi keuangan di Indonesia. Namun demikian, efektivitas upaya preventif dan represif masih menghadapi berbagai kendala regulatif, khususnya yang berkaitan dengan perlindungan data pribadi. Thiara Dewi Purnama dan Abdurrakhman Alhakim menyatakan bahwa "perlindungan terhadap data pribadi di Indonesia belum diatur secara khusus, melainkan diatur secara terpisah dalam berbagai peraturan perundang-undangan" (Purnama & Alhakim, 2021). Kondisi tersebut berpotensi melemahkan kepastian hukum dan membuka peluang terjadinya penyalahgunaan data pribadi dalam proses pengajuan pinjaman bank digital.

Penanggulangan penipuan berbasis teknologi dalam pengajuan pinjaman bank memerlukan landasan teori kebijakan pidana yang tepat. Pemikiran Marc Ancel, A. Mulder, dan Sudarto relevan karena menempatkan hukum pidana sebagai bagian dari kebijakan sosial yang rasional, adaptif, dan berorientasi pada perlindungan masyarakat. Kerangka pemikiran tersebut menegaskan bahwa penanggulangan kejahatan digital tidak cukup dilakukan melalui tindakan represif, melainkan memerlukan kebijakan pidana yang komprehensif, terencana, dan berkelanjutan (Rohmy dkk., 2022).

Marc Ancel memandang hukum pidana sebagai *instrument of social policy* untuk mewujudkan ketertiban dan keamanan negara melalui pengaturan yang efektif. Pandangan tersebut sejalan dengan pemikiran A. Mulder dan diperkuat oleh Sudarto yang menyatakan bahwa kebijakan hukum pidana bertujuan membentuk peraturan yang sesuai dengan kebutuhan masyarakat, baik pada masa kini maupun masa yang akan datang. Konsep tersebut menegaskan bahwa kebijakan pidana harus mampu memilih norma dan sanksi yang adil serta efektif dalam menghadapi perkembangan kejahatan berbasis teknologi.

Selanjutnya, Marc Ancel dan A. Mulder membagi kebijakan pidana ke dalam tiga tahap, yaitu tahap legislatif (formulasi), yudikatif (aplikasi), dan eksekutif (eksekusi), yang harus saling mendukung agar penanggulangan penipuan berbasis teknologi dapat berlangsung secara efektif. Pada tahap formulasi, diperlukan peraturan yang mampu mengantisipasi manipulasi identitas digital, pemalsuan dokumen, dan penyalahgunaan data. Pada tahap aplikasi, diperlukan penegakan hukum yang konsisten dan berorientasi pada kepastian hukum. Adapun pada tahap eksekusi, pelaksanaan pidana harus dilakukan secara profesional, efektif, dan humanistis.

Pandangan Marc Ancel menekankan pentingnya pendekatan multidisipliner karena kejahatan berbasis teknologi melibatkan aspek hukum, teknologi informasi, ekonomi, dan manajemen risiko. Pandangan tersebut menegaskan bahwa efektivitas penanggulangan kejahatan digital bergantung pada sinergi antarpemangku kepentingan serta keseimbangan antara upaya preventif dan represif. Dalam konteks ini, pencegahan melalui penguatan keamanan digital, peningkatan literasi masyarakat, dan perlindungan data dinilai lebih efektif daripada mengandalkan penindakan semata. Kerangka pemikiran Marc Ancel, A. Mulder, dan Sudarto menegaskan bahwa kebijakan pidana harus bersifat menyeluruh, adaptif, preventif, humanistik, dan efektif. Kerangka tersebut menunjukkan bahwa penanggulangan penipuan pinjaman bank berbasis teknologi memerlukan kebijakan pidana

yang responsif terhadap dinamika perkembangan teknologi serta mampu menjaga keseimbangan antara perlindungan masyarakat dan penegakan hukum yang tegas.

Langkah preventif dan represif dalam penanggulangan penipuan melalui penyalahgunaan teknologi pada pengajuan pinjaman bank perlu dianalisis dari perspektif perlindungan hukum sebagaimana dikemukakan oleh Philipus M. Hadjon (Ahmad & Utari, 2025). Teori perlindungan hukum menempatkan negara sebagai pihak yang bertanggung jawab menjamin keamanan hak-hak masyarakat melalui mekanisme pencegahan dan penindakan. Penipuan digital di sektor perbankan tidak hanya menimbulkan kerugian ekonomi bagi lembaga keuangan, tetapi juga mengancam hak masyarakat atas keamanan data pribadi, kepastian hukum, dan perlindungan dari penyalahgunaan identitas. Karakteristik kejahatan yang memanfaatkan teknologi informasi menyebabkan perlindungan hukum tidak lagi dapat bergantung pada pendekatan represif semata, melainkan harus dibangun melalui sistem pencegahan yang mampu mengurangi peluang terjadinya kejahatan sejak tahap awal pengajuan pinjaman.

Efektivitas perlindungan hukum preventif pada sektor perbankan digital sangat bergantung pada kualitas regulasi dan kemampuan lembaga keuangan dalam menerapkan mekanisme verifikasi identitas yang memadai. Regulasi perbankan telah mewajibkan penerapan prinsip *Know Your Customer* (KYC) dan *Customer Due Diligence* (CDD) sebagai instrumen untuk memastikan keabsahan identitas nasabah (Nur Hasanah dkk., 2024). Selain itu, penegakan keadilan mengharuskan aparat penegak hukum menindak pelaku secara konsisten berdasarkan KUHP, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta ketentuan mengenai pemalsuan identitas atau dokumen guna memberikan kepastian hukum bagi korban. Pandangan tersebut sejalan dengan prinsip perlindungan hukum represif menurut Philipus M. Hadjon yang menekankan penyelesaian sengketa dan penindakan sebagai instrumen untuk melindungi masyarakat dari dampak kejahatan (Anindya & Subiyanto, 2025).

Kondisi tersebut menunjukkan adanya kesenjangan antara norma hukum dan implementasinya. Pelaku kejahatan kerap memanfaatkan data pribadi yang diperoleh melalui kebocoran data, *phishing*, *social engineering*, maupun pembelian data secara ilegal pada platform digital tertentu. Situasi ini menyebabkan proses verifikasi identitas yang secara administratif telah memenuhi ketentuan hukum tetap berpotensi ditembus oleh pelaku yang menguasai data korban secara lengkap. Fakta tersebut menunjukkan bahwa efektivitas perlindungan preventif tidak hanya ditentukan oleh keberadaan regulasi, tetapi juga oleh kualitas sistem keamanan digital yang diterapkan oleh lembaga keuangan dan penyelenggara sistem elektronik.

Pemanfaatan autentikasi biometrik, *two-factor authentication*, kecerdasan buatan, serta teknologi pendeteksi *fraud* merupakan langkah yang relevan untuk memperkuat perlindungan preventif (Hutauruk dkk., 2024). Namun demikian, implementasi teknologi tersebut masih menghadapi sejumlah kendala karena belum seluruh lembaga keuangan memiliki kapasitas teknologi yang setara dalam mendeteksi pola penipuan digital yang semakin kompleks. Perbedaan kemampuan teknologi antarlembaga tersebut menyebabkan tingkat perlindungan hukum yang diterima masyarakat menjadi tidak seragam. Kondisi ini menunjukkan bahwa kebijakan pencegahan tidak cukup hanya dibangun melalui kewajiban normatif, tetapi juga memerlukan standardisasi sistem keamanan digital yang dapat diterapkan secara nasional.

Persoalan lain yang perlu mendapat perhatian adalah harmonisasi regulasi mengenai perlindungan data pribadi. Kehadiran UU PDP memberikan landasan normatif yang lebih

kuat bagi perlindungan informasi pribadi masyarakat. Namun, efektivitas perlindungan tersebut masih menghadapi tantangan dalam implementasinya karena mekanisme pengawasan, penegakan sanksi administratif, dan koordinasi antarlembaga belum sepenuhnya berjalan optimal. Kondisi ini menyebabkan kebocoran data pribadi masih kerap terjadi dan kemudian dimanfaatkan sebagai sarana untuk melakukan penipuan dalam pengajuan pinjaman bank.

Analisis terhadap hubungan antara KUHP Baru, UU ITE, UU PDP, dan regulasi OJK menunjukkan bahwa masing-masing instrumen hukum memiliki fungsi yang berbeda, tetapi saling berkaitan. KUHP Baru berfungsi sebagai dasar pemidanaan terhadap tindak pidana penipuan. UU ITE berfungsi menjangkau manipulasi informasi elektronik dan penyalahgunaan sistem digital. UU PDP berfungsi melindungi data pribadi sebagai objek yang kerap disalahgunakan dalam kejahatan digital. Sementara itu, regulasi OJK berfungsi mengatur tata kelola serta manajemen risiko pada sektor jasa keuangan. Keterkaitan tersebut menunjukkan bahwa penanggulangan penipuan digital memerlukan pendekatan lintas regulasi yang terintegrasi (Pardosi & Primawardani, 2020).

Permasalahan muncul ketika masing-masing instrumen hukum masih bekerja secara sektoral. Aparat penegak hukum sering kali memfokuskan proses penegakan hukum pada unsur penipuan atau manipulasi data elektronik tanpa mengoptimalkan instrumen perlindungan data pribadi yang sesungguhnya memiliki relevansi langsung dengan modus kejahatan tersebut. Akibatnya, perlindungan hukum terhadap korban lebih berorientasi pada penghukuman pelaku, sedangkan aspek pencegahan kebocoran data belum memperoleh perhatian yang memadai. Situasi ini menunjukkan bahwa sinkronisasi regulasi masih memerlukan penguatan agar seluruh instrumen hukum dapat berfungsi sebagai satu sistem perlindungan yang utuh.

Efektivitas upaya represif juga menghadapi tantangan yang tidak sederhana. Penegakan hukum terhadap tindak pidana penipuan berbasis teknologi sangat bergantung pada kemampuan aparat dalam memperoleh, mengamankan, dan menganalisis bukti elektronik. Karakteristik bukti digital berbeda dengan alat bukti konvensional karena data elektronik dapat diubah, dihapus, dipindahkan, atau disembunyikan dalam waktu yang relatif singkat. Kesulitan tersebut semakin kompleks ketika pelaku memanfaatkan *virtual private network* (VPN), server yang berlokasi di luar negeri, identitas palsu, atau akun digital yang dibuat secara anonim.

Kapasitas forensik digital menjadi faktor yang sangat menentukan keberhasilan proses penegakan hukum. Namun, keterbatasan jumlah tenaga ahli forensik digital, perbedaan kualitas laboratorium forensik digital, serta perkembangan teknologi yang berlangsung sangat cepat sering kali menyebabkan proses pembuktian berjalan lebih lambat dibandingkan dengan perkembangan modus kejahatan. Kondisi tersebut meningkatkan risiko kegagalan pembuktian meskipun secara substantif telah terjadi tindak pidana. Situasi ini menunjukkan bahwa ancaman pidana yang berat tidak akan memberikan efek yang optimal apabila tidak didukung oleh kemampuan pembuktian yang memadai.

Penerapan Pasal 35 jo. Pasal 51 ayat (1) UU ITE memberikan dasar hukum yang kuat untuk menjerat pelaku manipulasi informasi elektronik dalam pengajuan pinjaman bank (Rasji & Budiman, 2023). Ancaman pidana yang relatif berat menunjukkan komitmen negara dalam menanggulangi kejahatan digital. Akan tetapi, efektivitas ketentuan tersebut tidak hanya ditentukan oleh beratnya ancaman pidana, melainkan juga oleh kepastian penegakan hukum. Perspektif teori *deterrence* menjelaskan bahwa pelaku akan

mempertimbangkan risiko melakukan kejahatan apabila meyakini bahwa perbuatannya dapat dideteksi, dibuktikan, dan dihukum secara konsisten. Sebaliknya, penegakan hukum yang tidak konsisten dapat mengurangi daya cegah meskipun ancaman pidana yang diatur tergolong berat. Hambatan lain yang sering muncul berkaitan dengan karakter lintas yurisdiksi dari kejahatan siber. Pelaku dapat beroperasi dari wilayah hukum yang berbeda dengan lokasi korban maupun lokasi server yang digunakan. Kondisi tersebut menyebabkan proses penyidikan sering kali memerlukan kerja sama antarlembaga, bahkan kerja sama internasional. Mekanisme pertukaran informasi digital dan bantuan hukum timbal balik juga masih memerlukan penguatan agar proses penegakan hukum dapat berjalan lebih efektif. Tantangan tersebut menunjukkan bahwa pendekatan nasional semata tidak lagi memadai untuk menghadapi perkembangan kejahatan digital yang bersifat transnasional.

Analisis terhadap berbagai permasalahan tersebut menunjukkan bahwa efektivitas penanggulangan penipuan berbasis teknologi tidak dapat diukur hanya berdasarkan keberadaan regulasi atau beratnya ancaman pidana. Efektivitas tersebut harus dinilai berdasarkan kemampuan sistem hukum dalam mengintegrasikan perlindungan data pribadi, keamanan sistem elektronik, pengawasan sektor perbankan, serta penegakan hukum berbasis forensik digital. Kelemahan pada salah satu aspek tersebut berpotensi menciptakan celah yang dapat dimanfaatkan oleh pelaku kejahatan. Berdasarkan kondisi tersebut, penting untuk membentuk konsep kebijakan hukum pidana *digital banking fraud* yang terintegrasi dengan memadukan empat komponen utama, yaitu komponen penal, komponen teknologis, komponen regulatif, dan komponen kolaboratif. Komponen penal berfungsi menjamin kepastian pemidanaan melalui penerapan KUHP Baru dan UU ITE secara efektif. Komponen teknologis berfungsi memperkuat sistem verifikasi digital, deteksi *fraud* berbasis kecerdasan buatan, dan keamanan siber perbankan. Komponen regulatif berfungsi menyelaraskan penerapan UU PDP, regulasi OJK, dan ketentuan di sektor jasa keuangan. Sementara itu, komponen kolaboratif berfungsi memperkuat koordinasi antara aparat penegak hukum, otoritas keuangan, penyelenggara sistem elektronik, dan lembaga perbankan. Integrasi keempat komponen tersebut diharapkan mampu mengatasi kelemahan implementasi regulasi yang selama ini menyebabkan penanggulangan penipuan digital pada sektor perbankan belum berjalan secara optimal.

Dalam rangka memperkuat penanggulangan tindak pidana penipuan berbasis teknologi, pemerintah perlu mengharmonisasikan berbagai regulasi, termasuk memperkuat Undang-Undang Pelindungan Data Pribadi (UU PDP), mengingat penipuan digital kerap berawal dari penyalahgunaan data pribadi. Penegakan UU PDP terhadap Penyelenggara Sistem Elektronik yang lalai merupakan upaya represif sekaligus preventif dalam mencegah terjadinya kejahatan tersebut (Debora, 2023). Selain itu, kerja sama internasional menjadi penting karena kejahatan siber bersifat lintas negara. Melalui Budapest Convention on Cybercrime dan Interpol Cybercrime Division, Indonesia dapat melakukan pelacakan pelaku, ekstradisi, serta pemulihan aset sehingga tidak menjadi ruang aman (*safe haven*) bagi pelaku kejahatan. Penanggulangan juga memerlukan reformasi sistem peradilan pidana yang adaptif terhadap pembuktian digital, seperti log aktivitas, metadata, dan analisis algoritma, serta penyesuaian terhadap KUHP Baru dan KUHAP melalui pendekatan preventif dan represif yang terintegrasi. Dengan sinergi antara pemerintah, aparat penegak hukum, industri keuangan, dan masyarakat, penipuan berbasis teknologi diharapkan dapat ditekan sehingga sistem perbankan digital dapat berjalan secara aman, transparan, dan akuntabel (Mahesa, 2023).

Singapura menempatkan penipuan berbasis teknologi sebagai ancaman serius terhadap stabilitas sektor keuangan dan merumuskan norma pidana yang mampu menjangkau berbagai modus operandi tanpa bergantung pada jenis teknologi tertentu. Tindak pidana penipuan diatur dalam *Section 415 Penal Code (Cap. 224)* mengenai *cheating*. Ketentuan tersebut mendefinisikan penipuan sebagai perbuatan curang yang mengakibatkan korban mengalami kerugian. Unsur-unsur tersebut menitikberatkan pada adanya perbuatan curang, kesengajaan, dan kerugian sehingga penggunaan teknologi digital tetap tercakup dalam delik *cheating*. Selanjutnya, *Section 420 Penal Code* mengatur pemberatan sanksi berupa pidana penjara paling lama 10 tahun dan/atau denda apabila penipuan tersebut mengakibatkan penyerahan harta atau pemberian fasilitas ekonomi, seperti pinjaman bank. Ketentuan ini juga mencakup penggunaan identitas palsu, manipulasi data digital, dan penyampaian informasi yang tidak benar dalam pengajuan kredit. Pendekatan tersebut menunjukkan bahwa hukum pidana Singapura memberikan penekanan pada perlindungan kepentingan ekonomi serta pemeliharaan kepercayaan publik terhadap sistem keuangan (Syahril & Aris, 2024).

Selain itu, Singapura memperkuat penanggulangan penipuan digital melalui *Computer Misuse and Cybersecurity Act* (CMCA), yang mengkriminalisasi akses tanpa izin, manipulasi data, dan penyalahgunaan sistem elektronik yang menimbulkan kerugian ekonomi (Sari, 2024). Di samping itu, *Monetary Authority of Singapore* (MAS) mewajibkan penerapan *Know Your Customer* (KYC), verifikasi identitas digital berlapis, serta sistem deteksi penipuan berbasis analisis data. Pendekatan tersebut menekankan kejelasan norma, ketegasan sanksi, dan sinergi antarlembaga berbasis teknologi, yang dapat dijadikan model dalam penguatan kebijakan hukum pidana di Indonesia.

D. Simpulan

Berdasarkan hasil pembahasan, dapat disimpulkan bahwa kebijakan hukum pidana terhadap penipuan melalui penyalahgunaan teknologi dalam pengajuan pinjaman bank di Indonesia telah didukung oleh KUHP Baru, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data Pribadi (UU PDP), serta regulasi di sektor jasa keuangan. Namun demikian, efektivitas penegakan hukum masih menghadapi berbagai kendala, antara lain belum optimalnya harmonisasi antarregulasi, tingginya risiko penyalahgunaan data pribadi, serta keterbatasan kapasitas forensik digital dalam pembuktian tindak pidana.

Konsep kebijakan hukum pidana yang terintegrasi dalam penanggulangan digital banking fraud, dengan menggabungkan dimensi penal, teknologis, regulatif, dan kolaboratif sebagai kerangka yang lebih adaptif terhadap kejahatan digital, menjadi penting untuk diterapkan. Reformasi kebijakan perlu diarahkan pada harmonisasi regulasi, penguatan sistem verifikasi digital, peningkatan kapasitas aparat penegak hukum, serta penguatan kerja sama antarinstansi guna mewujudkan perlindungan hukum yang efektif bagi sektor perbankan dan masyarakat.

Selain itu, penegakan hukum harus diarahkan secara tegas terhadap perbuatan manipulasi data elektronik, pemalsuan identitas digital, dan rekayasa dokumen dalam pengajuan kredit melalui penerapan kebijakan penal secara proporsional yang mencakup tahap legislasi, aplikasi, dan eksekusi pidana. Aparat penegak hukum juga memerlukan peningkatan kapasitas forensik digital untuk mendukung proses pembuktian yang akurat dan akuntabel. Upaya penanggulangan tersebut perlu disertai langkah-langkah preventif

melalui penguatan sistem verifikasi identitas digital, penerapan prinsip kehati-hatian perbankan, peningkatan keamanan siber, serta penguatan literasi digital masyarakat guna mencegah berkembangnya kejahatan berbasis teknologi di sektor perbankan.

Daftar Pustaka

Ahmad, M. R. A., & Utari, I. S. (2025). Perlindungan Hukum Pengguna E Commerce: Perspektif Viktimologi dalam Menghadapi Kejahatan Siber. *Bookchapter Hukum dan Lingkungan*, *1*. https://bookchapter.unnes.ac.id/index.php/hk/article/view/545

Alhakim, A. & Sofia. (2021). Kajian Normatif Penanganan Cyber Crime di Sektor Perbankan di Indonesia. *Jurnal Komunitas Yustisia*, *4*(2), 377–385. https://doi.org/10.23887/jatayu.v4i2.38089

Anggun, L. (2022). Perkembangan Kejahatan Tindak Pidana Pencucian Uang dan Tindak Pidana Pendanaan Terorisme (TPPU dan TPPT) di Masa Pandemi Covid-19. *Jurnal Hukum & Pembangunan*, *1*(1). https://doi.org/10.21143/TELJ.vol1.no1.1004

Anindya, R. P., & Subiyanto, A. E. (2025). Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(3), 1105–1112. https://doi.org/10.31004/riggs.v4i3.2105

Ayunda, R. & Rusdianto. (2021). Perlindungan Data Nasabah Terkait Pemanfaatan Artificial Intelligence dalam Aktifitas Perbankan di Indonesia. *Jurnal Komunikasi Hukum (JKH)*, *7*(2). https://doi.org/10.23887/jkh.v7i2.37995

Azis, M., & Redi, A. (2023). Rekonstruksi Perlindungan Hukum Bagi Konsumen Perbankan di Tengah Ancaman Kejahatan Teknologi. *Jurnal Retentum*, *5*(2). https://doi.org/10.46930/retentum.v7i1.5380

Debora. (2023). *Penegakan Hukum Pidana Terhadap Pelaku Tindak Pidana Penipuan Investasi Ilegal Dengan Cryptocurrency Pada Pasar Komoditi* [Skripsi, Universitas Medan Area]. https://repositori.uma.ac.id/jspui/handle/123456789/21291

Gurning, E. A. (2022). *Kebijakan Hukum Pidana Terhadap Penyalahgunaan Data Pribadi Pada Pinjaman Online* [Skripsi, Universitas Medan Area]. https://repositori.uma.ac.id/jspui/handle/123456789/18685

Habibi, M. R., & Liviani, I. (2020). Kejahatan Teknologi Informasi (Cyber Crime) dan Penanggulangannya dalam Sistem Hukum Indonesia. *Al-Qanun: Jurnal Pemikiran dan Pembaharuan Hukum Islam*, *23*(2), 400–426. https://doi.org/10.15642/alqanun.2020.23.2.400-426

Hapid, F. M., Suntana, I., & Royani, M. Y. (2024). Penerapan Asas Geen Straf Zonder Schuld Dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake. *Jurnal USM Law Review*, *7*(3), 1155–1174. https://doi.org/10.26623/julr.v7i3.9686

Hasan, Z., Ayu, A. M., M, C. D., Trisnawati, M., & R.A, M. A. A. (2024). Penaggulangan Tindak Pidana Penipuan Melalui Transfer Mobile Mbanking. *Humanitis: Jurnal Homaniora, Sosial dan Bisnis*, *1*(9). https://ecosemica.net/index.php/HUMANITIS/article/view/513

Hutauruk, R. H., Febriyani, E., Disemadi, H. S., Sudirman, L., Ayunda, R., & Agustianto. (2024). Meningkatkan Literasi Keuangan Digital Masyarakat Melalui Pemahaman

Hukum di Sektor Fintech. *Abdurrauf Journal of Community Service*, *1*(2). https://doi.org/10.70742/ajcos.v1i2.115

Kristian, O. Y. (2022). Perlindungan Hukum Pengguna Layanan Fintech P2P Lending dari Tindak Pidana Ekonomi dan Terhadap Penyedia Layanan Fintech P2P Lending Ilegal. *Majalah Hukum Nasional*, *52*(2). https://jdih.ppatk.go.id/storage/dokumen_produk_hukum/15b1b14a978f1118ab0abbb9c666241e.pdf

Mahesa, A. R. (2023). *Penegakan Hukum Terhadap Tindak Pidana Penipuan Jual Beli Online (E-Commerce) di Kota Yogyakarta*.

Muhammad, F. E., & Harefa, B. (2023). Pengaturan Tindak Pidana Bagi Pelaku Penipuan Phisning Berbasis Web. *Jurnal USM Law Review*, *6*(1), 226–241. https://doi.org/10.26623/julr.v6i1.6649

Nur Hasanah, V., Mustika Putri, N. K., Elsisi Suanti, E. A. Y., & Martia, V. (2024). Analisis Putusan Nomor 796 K Pid Sus 2015 tentang Penyalahgunaan Wewenang dalam Pengelolaan Keuangan di Bank Perkreditan Rakyat. *PENG: Jurnal Ekonomi dan Manajemen*, *2*(2), 1529–1547. https://doi.org/10.62710/g3nsnq86

Pakpahan, E. F., Chandra, K., & Tanjaya, A. (2020). Urgensi Pengaturan Financial Technology di Indonesia. *Jurnal Darma Agung*, *28*(3), 444. https://doi.org/10.46930/ojsuda.v28i3.807

Pardosi, R. O. A. G., & Primawardani, Y. (2020). Perlindungan Hak Pengguna Layanan Pinjaman Online dalam Perspektif Hak Asasi Manusia. *Jurnal HAM*, *11*(3), 353. https://doi.org/10.30641/ham.2020.11.353-368

Permata, S., & Haryanto, H. (2022). Perlindungan Hukum Terhadap Pengguna Aplikasi Shopee Pay Later. *Krisna Law : Jurnal Mahasiswa Fakultas Hukum Universitas Krisnadwipayana*, *4*(1), 33–47. https://doi.org/10.37893/krisnalaw.v4i1.13

Purnama, T. D., & Alhakim, A. (2021). Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi di Indonesia. *Jurnal Komunitas Yustisia*, *4*(3). https://ejournal.undiksha.ac.id/index.php/jatayu/article/view/44370

Putri, K. A. (2025). *OJK Terima 42.257 Laporan Penipuan, Total Kerugian Korban Tembus Rp700,2 M* [Infobanknews.com]. https://infobanknews.com/ojk-terima-42-257-laporan-penipuan-total-kerugian-korban-tembus-rp7002-m

Ramadhani, D. Y. (2022). Upaya Perlindungan Hukum Konsumen Terhadap Penyalahgunaan Data Pribadi Oleh Financial Technology Ilegal. *Dinamika*, *28*(6). https://jim.unisma.ac.id/index.php/jdh/article/view/14491

Rasji, & Budiman, M. A. (2023). Tinjauan Hukum terhadap Pengawasan dan Penyidikan oleh Otoritas Jasa Keuangan. *Jurnal Kewarganegaraan*, *7*(2). https://doi.org/10.31316/jk.v7i2.5423

Rishadi, A. A., M, M., & Simanjuntak, P. (2022). Model Penanganan Kejahatan Teknologi Finansial (Fintech) Dalm Upaya Mendukung Pembangunan Nasional di Sektor Ekonomi di Era Digital 4.0. *Jurnal Hukum Positum*, *7*(1), 25–42. https://doi.org/10.35706/positum.v7i1.6641

Rivanie, S. S., Muchtar, S., Muin, A. M., Prasetya, A. M. D., & Rizky, A. (2022). Perkembangan Teori-teori Tujuan Pemidanaan. *Halu Oleo Law Review*, *6*(2), 176–188. https://doi.org/10.33561/holrev.v6i2.4

Rohmy, A. M., Setiyono, S., & Nihayaty, A. I. (2022). Kebijakan Pidana Tindakan Kebiri Kimia Pelaku Kejahatan Seksual Berulang Pada Anak di Indonesia. *Jurnal Rechtens*, *11*(2), 161–184. https://doi.org/10.56013/rechtens.v11i2.1361

Sari, A. K. (2024). Tinjauan Hukum terhadap Kejahatan Siber dalam Transaksi Financial Technology. *Juris Sinergi Journal (JSJ)*, *1*(1). https://doi.org/10.70321/jsj.v1i1.27

Satria, M., & Handoyo, S. (2022). Perlindungan Hukum Terhadap Data Pribadi Pengguna Layanan Pinjaman Online Dalam Aplikasi Kreditpedia. *Journal De Facto*, *8*(2). https://jurnal.pascasarjana.uniba-bpn.ac.id/index.php/jurnaldefacto/article/view/113

Sipayung, B., & Amelya, A. (2022). Manajemen Risiko dalam Pertimbangan Pengajuan Pinjaman Dana Pemulihan Ekonomi Nasional (PEN) Daerah. *Kinerja*, *19*(4), 681–691.

Syahril, Muh. A. F., & Aris, A. (2024). Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act. *Journal of Law Justice (JLJ)*, *2*(3), 198–205. https://doi.org/10.33506/jlj.v2i3.3711

Utami, G., & Astuti, P. (2023). Analisis Yuridis Penggunaan Cryptocurrency (Bitcoin) Sebagai Sarana Tindak Pidana Pencucian Uang. *Novum: Jurnal Hukum*, *10*(1). https://doi.org/10.2674/novum.v0i0.50069

Wardhana, R. W. (2023). Kebijakan Hukum Pidana Terkait Penyalahgunaan Data Pribadi Pada Pelaksanaan Transaksi Pinjaman Online. *Dinamika*, *29*(2). https://jim.unisma.ac.id/index.php/jdh/article/view/20067

Yulenrivo, F., Azheri, B., & Yulfasni. (2023). Perlindungan Hukum Terhadap Konsumen Pengguna Pinjaman Online Berbasis Financial Technology oleh Otoritas Jasa Keuangan. *UNES Law Review*, *6*(1). https://doi.org/10.31933/unesrev.v6i1.927

Yuwono, M. S., & Hoesein, Z. A. (2022). Kekosongan Hukum Perlindungan Konsumen dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Retentum*, *4*(2). https://doi.org/10.46930/retentum.v7i1.5276