PENERAPAN SANKSI PIDANA TERHADAP PELAKU PENIPUAN YANG BERKEDOK KREDIT MELALUI APLIKASI ELEKTRONIK [1]

Oleh :
Fabio F. F. Sepang [2]
Anna S. Wahongan [3]
Vonny A. Wongkar [4]

ABSTRAK

Penelitian ini bertujuan untuk mengetahui dan memahami bagaimana penerapan sanksi pidana terhadap pelaku penipuan yang berkedok kredit melalui aplikasi berdasarkan hukum positif di Indonesia dan untuk mengetahui dan memahami bagaimana penegakan hukum dalam kasus penipuan berkedok kredit melalui aplikasi. Dengan menggunakan metode penelitian yuridis normatif, dapat ditarik kesimpulan yaitu : 1. Penerapan Sanksi Pidana terhadap pelaku penipuan berkedok kredit melalui aplikasi elektronik dalam hukum positif Indonesia masih menghadapi fragmentasi regulasi (KUHP, UU ITE, POJK) dan ketidaktepatan sasaran sanksi. Sanksi pidana kerap diterapkan secara parsial (hanya pada *debt collector* atau pelaku lapangan), kurang menjangkau otak intelektual, serta didominasi sanksi administratif ringan dari OJK yang tidak proporsional dengan kerugian korban, sementara penerapan pasal-pasal KUHP/Pasal 378 terkendala pembuktian rumit modus digital. 2. Efektivitas Penegakan Hukum dalam kasus ini belum optimal akibat kegagalan sistemik yang mencakup lemahnya kapasitas institusi (SDM, alat digital forensik), koordinasi antar-lembaga (Polri, OJK, Kominfo) yang tidak terintegrasi, budaya hukum rendah (underreporting korban karena stigma dan ketidakpercayaan), serta kalkulus rasional pelaku yang memandang keuntungan finansial jauh lebih besar daripada risiko hukuman.

Kata Kunci : *penipuan, kredit, aplikasi elektronik*

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi (TIK), terutama internet dan perangkat seluler, telah merevolusi berbagai aspek kehidupan, termasuk sektor finansial. Kemunculan aplikasi elektronik, khususnya Fintech (*Financial Technology*) Lending, menawarkan kemudahan, kecepatan, dan aksesibilitas dalam memperoleh pinjaman atau kredit. Namun, kemajuan ini diiringi dengan munculnya bentuk kejahatan baru yang memanfaatkan celah teknologi dan kerentanan pengguna. Salah satu kejahatan yang marak adalah penipuan berkedok penawaran kredit melalui aplikasi elektronik. Penipuan melalui media elektronik semakin marak seiring dengan perkembangan teknologi informasi.[5]

Penipuan melalui aplikasi elektronik seringkali dilakukan dengan modus operandi yang terstruktur dan sulit dilacak. Pelaku biasanya memanfaatkan celah-celah hukum dan kelemahan sistem keamanan siber untuk melakukan aksinya. Kejahatan mayantara memerlukan pendekatan hukum yang komprehensif dan adaptif.[6] Mereka menawarkan pinjaman dengan syarat yang mudah dan proses yang cepat, namun pada kenyataannya, pinjaman tersebut tidak pernah cair atau disertai dengan persyaratan yang memberatkan, seperti bunga yang sangat tinggi atau ancaman jika tidak melunasi tepat waktu. Hal ini menyebabkan korban terjebak dalam lingkaran utang yang sulit untuk diselesaikan.

Kitab Undang-Undang Hukum Pidana (KUHP), sebagai hukum pidana umum (*lex generalis*), mengatur tindak pidana penipuan dalam Pasal 378. Pasal ini mensyaratkan unsur-unsur: (1) dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, (2) dengan nama palsu atau martabat palsu, (3) dengan tipu muslihat, atau (4) dengan rangkaian kebohongan, (5) menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang. Namun, modus penipuan melalui aplikasi elektronik seringkali sulit dijerat sempurna dengan Pasal 378 KUHP karena karakteristik kejahatan siber yang lintas batas, penggunaan identitas digital yang sulit dilacak (bukan sekadar "nama palsu" konvensional), dan tipu muslihat yang sangat canggih berbasis manipulasi data dan antarmuka aplikasi.[7]

Merespons perkembangan kejahatan siber, Indonesia memberlakukan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE). UU ini menjadi lex specialis bagi kejahatan yang menggunakan sarana elektronik.

---

[1] Artikel Skripsi
[2] Mahasiswa Fakultas Hukum Unsrat, NIM 210711011016
[3] Fakultas Hukum Unsrat, Doktor Ilmu Hukum
[4] Fakultas Hukum Unsrat, Magister Ilmu Hukum

[5] Mulyadi, Lilik. (2013). *Tindak Pidana Penipuan dan Perkembangan Modus Operandi*. Bandung: Alumni, hlm. 78.
[6] Wahid, Abdul, & Labib, M. (2015). *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama. Hlm. 102.
[7] Kitab Undang-Undang Hukum Pidana (KUHP), pasal 378.

Pasal 28 Ayat (1) UU ITE mengancam pidana bagi setiap orang yang sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan suku, agama, ras, dan antargolongan (SARA), namun relevansi utamanya terletak pada Pasal 35 dan Pasal 36. Pasal 35 mengkriminalisasi perbuatan "mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apapun tanpa hak". Pasal 36 mengancam pidana bagi setiap orang yang "melakukan perbuatan dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain". Pasal-pasal ini dapat digunakan untuk menjerat aktivitas *hacking* atau pencurian data yang sering menjadi bagian dari modus penipuan kredit aplikasi.[8]

Lebih langsung terkait penipuan adalah Pasal 27 Ayat (3) UU ITE yang mengatur "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman". Meskipun rumusannya lebih dekat ke pemerasan, dalam praktik penegakan hukum, penipuan kredit elektronik yang melibatkan ancaman atau intimidasi untuk pembayaran sering dijerat dengan pasal ini. Selain itu, Pasal 32 UU ITE tentang "Perusakan dan Perbuatan yang Merugikan" dapat digunakan jika penipuan menyebabkan kerusakan pada sistem atau kerugian finansial yang dapat dikategorikan sebagai perbuatan melawan hukum di dunia siber.[9]

Korban penipuan kredit aplikasi elektronik pada hakikatnya adalah konsumen yang dirugikan dalam transaksi elektronik. Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK) memberikan perlindungan fundamental. Pasal 4 UUPK menyatakan hak konsumen atas kenyamanan, keamanan, dan keselamatan dalam mengkonsumsi barang dan/atau jasa. Pasal 7 dan Pasal 8 UUPK mengatur kewajiban pelaku usaha untuk beritikad baik, memberikan informasi yang benar, jelas, dan jujur, serta larangan untuk memproduksi dan/atau memperdagangkan barang dan/jasa yang tidak memenuhi atau tidak sesuai dengan standar yang dipersyaratkan. Penipuan kredit jelas-jelas melanggar hak-hak konsumen dan kewajiban pelaku usaha ini, sehingga UUPK menjadi landasan penting bagi tuntutan ganti rugi perdata oleh korban, meskipun fokus skripsi adalah sanksi pidana.

Proses penegakan hukum terhadap pelaku penipuan aplikasi kredit elektronik, mulai dari penyidikan, penuntutan, hingga persidangan, berpedoman pada Kitab Undang-Undang Hukum Acara Pidana (KUHAP) - Undang-Undang Nomor 8 Tahun 1981. KUHAP mengatur secara rinci tahapan penyidikan oleh Kepolisian (Pasal 1 angka 2, Pasal 6, Pasal 7), penuntutan oleh Kejaksaan (Pasal 1 angka 7, Pasal 14), dan pemeriksaan di sidang pengadilan (Pasal 50 dst). Keberhasilan penegakan hukum sangat bergantung pada kemampuan aparat penegak hukum dalam mengumpulkan, mengamankan, dan menganalisis alat bukti elektronik (digital forensics) sesuai ketentuan Pasal 184 KUHAP jo. Pasal 5 UU ITE yang mengakui informasi elektronik sebagai alat bukti yang sah.

Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban (UU PSK) dan Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan atas Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban, memainkan peran krusial dalam konteks penipuan aplikasi kredit elektronik. Korban penipuan, yang seringkali mengalami tekanan psikologis, ancaman, atau stigma, berhak mendapatkan perlindungan fisik dan mental serta hak restitusi, dalam hal ini perlindungan data pribadi yang sering menjadi senjata bagi para penipu membuat isu isu krusial dalam era digital.[10] UU PSK menjamin hak-hak korban dan saksi selama proses peradilan pidana, yang sangat diperlukan mengingat modus penipuan ini sering melibatkan intimidasi terhadap korban.

Di tingkat operasional, Kepolisian Negara Republik Indonesia (Polri) menerbitkan Peraturan Kapolri (Perkap) yang menjadi pedoman bagi anggota Polri dalam menangani kejahatan, termasuk kejahatan siber. Perkap-perkap ini mengatur *Standard Operating Procedure* (SOP) penyidikan, pelaporan, pengelolaan barang bukti elektronik, dan koordinasi antar unit (seperti Direktorat Tindak Pidana Siber Bareskrim Polri). Penerapan sanksi sangat bergantung pada pemahaman dan kapasitas penyidik dalam mengimplementasikan SOP ini untuk kasus-kasus penipuan aplikasi kredit elektronik yang kompleks.

---

[8] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE), Pasal 28, 35, dan 36.

[9] Ibid, pasal 27 ayat (3) dan pasal 32.

[10] Riyanto, Astim. (2016). *Hukum Siber: Pengaturan dan Perlindungan di Era Digital*. Bandung: Nuansa Aulia, hlm. 67.

Penerapan sanksi pidana terhadap pelaku penipuan aplikasi kredit elektronik dihadapkan pada berbagai tantangan kompleks: (1) Kesulitan Identifikasi Pelaku: Pelaku sering menggunakan identitas palsu, server luar negeri, atau teknik penyamaran digital (*anonymity tools*). (2) Karakteristik Lintas Yurisdiksi: Server, pelaku, dan korban dapat berada di wilayah hukum yang berbeda, membutuhkan kerjasama internasional (*Mutual Legal Assistance*/MLA) yang rumit dan memakan waktu. (3) Keterbatasan Digital Forensics: Kapasitas dan sarana penyidik dalam mengolah barang bukti digital masih perlu terus ditingkatkan. (4) Kecepatan Perkembangan Modus: Modus operandi berkembang sangat cepat, sementara regulasi dan penegakan hukum cenderung tertinggal (*law lag*). (5) Minimnya Laporan Korban: Korban sering enggan melapor karena malu, takut ancaman, atau merasa proses hukum rumit.

Salah satu contoh kasus nyata yang terjadi terkait penipuan yang berkedok kredit melalui aplikasi elektronik di Indonesia adalah kasus PT Kredit Tanpa Agunan (KTA) dan Aplikasi "Kredit Plus", Putusan Mahkamah Agung RI No. 1002 K/Pid.Sus/2022 (Peninjauan Kembali). Latar Belakang: Perusahaan menawarkan pinjaman online melalui aplikasi "Kredit Plus". Korban diharuskan membayar biaya administrasi, asuransi, dan biaya lainnya di muka via transfer, namun pinjaman tidak pernah cair. Ribuan korban melapor dengan total kerugian miliaran rupiah. Tuntutan Jaksa: Pasal 378 KUHP (Penipuan), Pasal 372 KUHP (Penggelapan), Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE (Perbuatan Merugikan), dan Pasal 46 ayat (1) jo. Pasal 47 ayat (2) UU Perbankan (Menghimpun Dana Tanpa Izin). Putusan Akhir (Berkekuatan Hukum Tetap): Terdakwa (Direktur Utama dan Komisaris) dipidana penjara selama 8 (delapan) tahun dan denda Rp 1 miliar subsider 6 bulan kurungan. Diperintahkan membayar restitusi kepada korban senilai total kerugian yang terbukti (miliaran rupiah).

B. Rumusan Masalah

1. Bagaimana penerapan sanksi pidana terhadap pelaku penipuan yang berkedok kredit melalui aplikasi berdasarkan hukum positif di Indonesia?
2. Bagaimana penegakan hukum dalam kasus penipuan berkedok kredit melalui aplikasi?

C. Metode Penelitian

Metode pendekatan yang digunakan dalam penelitian ini adalah Metode Yuridis Normatif.

PEMBAHASAN

A. Penerapan Sanksi Pidana Terhadap Pelaku Penipuan Yang Berkedok Kredit Melalui Aplikasi Berdasarkan Hukum Positif Di Indonesia

Dalam kerangka hukum pidana Indonesia, praktik penipuan berbasis aplikasi pinjaman online dikonstruksikan sebagai tindak pidana kompleks yang memenuhi unsur ganda dari beberapa ketentuan hukum. Secara primer, tindakan ini terklasifikasi sebagai penipuan klasik (*oplichting*) yang diatur dalam Pasal 378 KUHP, dimana pelaku secara sengaja menggerakkan korban untuk menyerahkan harta benda melalui tipu muslihat. Tipu muslihat tersebut termanifestasi dalam pemberian informasi palsu mengenai legalitas operasional (seperti mengklaim terdaftar di OJK padahal ilegal), skema bunga yang tidak transparan, atau janji-janji fasilitas pinjaman yang fiktif. Unsur "penyesatan" ini menjadi *actus reus* utama yang membedakannya dari transaksi finansial sah.

Lebih lanjut, modus operandi pelaku seringkali memenuhi kualifikasi pemerasan (*afpersing*) dalam Pasal 368 KUHP. Hal ini terlihat dari praktik intimidasi melalui debt collector yang melakukan teror psikologis, ancaman penyebaran data pribadi, hingga pelecehan verbal terhadap korban dan keluarga. Pemerasan sistemik ini terjadi pasca-korban terjebak dalam jeratan utang akibat bunga berlipat (*roll over*) yang tidak manusiawi, sehingga memenuhi unsur "menguntungkan diri sendiri secara melawan hukum dengan memaksa orang lain menyerahkan barang".

Di samping itu, aspek digital dari kejahatan ini mengaktifkan lex specialis UU ITE, khususnya Pasal 28 ayat (1) juncto Pasal 45A UU No. 19 Tahun 2016 tentang Informasi Elektronik. Pelaku dengan sengaja menyebarkan informasi elektronik yang mengandung unsur penipuan melalui platform aplikasi, memanfaatkan infrastruktur digital untuk memperluas jangkauan korbannya. Penyebaran konten menyesatkan tentang mekanisme pinjaman ini termasuk dalam rumusan "menyebarkan berita bohong" yang menimbulkan kerugian konsumen.

Unsur keempat yang krusial adalah penyalahgunaan data pribadi yang diatur dalam Pasal 26 Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Dalam praktiknya, aplikasi pinjol ilegal melakukan pemrosesan data tanpa dasar hukum sah (*lawful basis*), melampaui tujuan pemrosesan, dan mengakses kontak darurat korban untuk tujuan intimidasi. Pelanggaran ini bersifat kumulatif dengan tindak pidana lain karena

melibatkan aspek formil (ketiadaan persetujuan/*consent*) dan materiil (penggunaan data di luar tujuan perjanjian).

Secara doktrinal, konstruksi hukum ini menganut teori perbarengan peraturan (*concursus idealis*) karena satu perbuatan melanggar beberapa ketentuan pidana sekaligus. Putusan Pengadilan Negeri Jakarta Selatan No. 734/Pid.B/2022/PN Jkt.Sel menegaskan hal ini dengan menerapkan tiga pasal sekaligus (Pasal 378 KUHP, Pasal 368 KUHP, dan Pasal 28 ayat (1) UU ITE) terhadap pelaku pinjol "KreditCepat". Yurisprudensi ini membentuk preseden bahwa setiap elemen kejahatan memiliki *legal interest* berbeda: KUHP melindungi harta benda, UU ITE melindungi tatanan informasi digital, sedangkan UU PDP menjaga integritas data pribadi.[11]

Dalam implementasinya, penerapan sanksi kumulatif ini menghadapi tantangan pembuktian teknis. Unsur "pengayaan diri secara melawan hukum" (*wederrechtelijke vermogensvermeerdering*) memerlukan pelacakan alur dana yang kompleks karena pelaku menggunakan multi-layer financial channel (seperti dompet digital fiktif, transfer antar-bank, hingga *cryptocurrency*). Bareskrim Polri dalam Pedoman Penyidikan Tindak Pidana Siber (2022) mengakui hanya 40% kasus yang berhasil melacak keseluruhan aliran dana akibat teknik *layering* dan *smurfing* yang canggih.[12]

Perkembangan terbaru menunjukkan perluasan kualifikasi hukum melalui Peraturan Jaksa Agung No. 5 Tahun 2023 tentang Penanganan Tindak Pidana Teknologi Informasi[13]. Dalam lampiran peraturan ini, pinjol ilegal secara eksplisit dimasukkan sebagai "*cyber fraud*" dengan unsur tambahan: pembajakan sistem elektronik (ketika pelaku memanipulasi aplikasi resmi) dan pencucian data (*data laundering*) melalui transaksi fiktif. Ekspansi yuridis ini merefleksikan dinamika penyesuaian hukum terhadap modus kejahatan digital yang terus berevolusi.

Kehadiran UU PDP pada 2022 memperkuat fondasi hukum dengan mengintrodusir sanksi administratif spesifik berupa denda hingga 2% pendapatan tahunan pelaku (Pasal 57 UU PDP) di luar sanksi pidana. Mekanisme ganda sanksi administratif-pidana ini menjadi terobosan signifikan mengingat selama ini pelanggaran data hanya dijerat dengan sanksi pidana UU ITE yang bersifat umum. Keterpaduan penegakan hukum antara perlindungan konsumen (UU No. 8 Tahun 1999), transaksi elektronik (UU ITE), dan data pribadi (UU PDP) kini membentuk *regulatory ecosystem* yang lebih komprehensif.

Kehadiran Undang-Undang Perlindungan Data Pribadi (UU PDP) Tahun 2022 merepresentasikan pergeseran paradigmatik dalam penegakan hukum digital di Indonesia. Berdasarkan Teori Hukum Responsif (*responsive law theory*) Philip Selznick, hukum idealnya harus berfungsi sebagai *instrumen responsif* yang adaptif terhadap masalah sosial, bukan sekadar alat kontrol represif. UU PDP mengaktualisasikan teori ini melalui mekanisme sanksi administratif progresif (Pasal 57) yang mencapai 2% pendapatan tahunan pelaku, menciptakan efek jera berbasis proporsionalitas sekaligus memberi ruang koreksi mandiri (*self-correction*) sebelum eskalasi ke pidana.

Undang-Undang Perlindungan Data Pribadi (UU PDP) tidak hanya berfungsi sebagai instrumen mandiri melainkan juga menciptakan sinergi triangular dengan tiga kerangka hukum lainnya: UU Informasi dan Transaksi Elektronik (ITE), UU Perlindungan Konsumen, dan Kitab Undang-Undang Hukum Pidana (KUHP). Sinergi ini membentuk suatu *regulatory ecosystem* yang organik, sebagaimana digambarkan oleh Philip Selznick, di mana berbagai regulasi saling terkait dan memperkuat seperti *web of rules*. UU PDP berperan sebagai poros yang mengintegrasikan ketentuan tentang privasi, transparansi, dan keadilan pidana, sehingga menciptakan perlindungan holistik bagi subjek data dalam ekosistem digital.[14]

Pertama, sinergi antara UU PDP dan UU ITE terlihat dari penegasan prinsip *consent* (persetujuan) dalam pengolahan data pribadi. Pasal 26 UU ITE melarang penyebaran data tanpa izin, yang sejalan dengan ketentuan UU PDP tentang kewajiban memperoleh persetujuan subjek data (Pasal 20). Kedua undang-undang ini saling melengkapi: UU ITE memberikan dasar hukum untuk menindak pelanggaran *ex post facto*, sementara UU PDP menetapkan standar *ex ante* berupa kewajiban *privacy by design*. Integrasi ini memperkuat akuntabilitas pelaku usaha dan menghindari *regulatory gap* dalam praktik pengumpulan data.

Kedua, UU PDP juga bersinergi dengan UU Perlindungan Konsumen, khususnya dalam aspek

---

[11] Putusan PN Jakarta Selatan No. 734/Pid.B/2022/PN Jkt.Sel, pertimbangan hukum butir 4.12

[12] Bareskrim Polri, *Pedoman Penyidikan Tindak Pidana Siber* (Jakarta: Divisi TIK Polri, 2022), hlm. 89.

[13] Peraturan Jaksa Agung No. 5 Tahun 2023 tentang Penanganan Tindak Pidana Teknologi Informasi, Lampiran II.

[14] Selznick, P. (1992). *The Moral Commonwealth*. University of California Press, hlm. 463.

transparansi kontrak digital. Pasal 4 UU No. 8/1999 mewajibkan pelaku usaha untuk memberikan informasi yang jujur dan jelas, yang relevan dengan kewajiban *data controller* dalam UU PDP untuk memberitahukan tujuan pengolahan data (Pasal 17). Dalam konteks ini, UU PDP memperluas cakupan transparansi tidak hanya pada aspek komersial, tetapi juga pada penggunaan data pribadi. Sinergi ini mencegah praktik *asymmetric information* yang merugikan konsumen, sekaligus memastikan bahwa hak-hak konsumen dalam transaksi digital terlindungi secara komprehensif.

Ketiga, hubungan antara UU PDP dan KUHP terlihat dalam penanganan kejahatan berbasis data. Pelanggaran berat terhadap UU PDP, seperti pemalsuan data atau penggelapan informasi pribadi untuk penipuan, dapat dikualifikasikan sebagai tindak pidana sesuai Pasal 378 KUHP tentang penipuan atau Pasal 368 tentang pemerasan. Dengan demikian, UU PDP tidak hanya mengatur sanksi administratif, tetapi juga membuka ruang untuk penegakan hukum pidana apabila pelanggaran data berdampak sistemik. Hal ini menunjukkan bagaimana *regulatory ecosystem* bekerja secara hierarkis, di mana aturan administratif dan pidana saling mengisi.

Lebih jauh, integrasi UU PDP dengan UU ITE dan UU Perlindungan Konsumen juga memperkuat aspek *preventif* dalam perlindungan data. UU ITE mengatur larangan penyebaran data, sementara UU Perlindungan Konsumen memastikan transparansi, dan UU PDP menetapkan mekanisme pengawasan oleh otoritas khusus. Kolaborasi ini membentuk *layered protection*, di mana setiap lapisan regulasi menangani aspek berbeda dari risiko digital. Selznick menyebutnya sebagai *institutional complementarity*, di mana berbagai lembaga dan aturan saling mendukung untuk mencapai tujuan bersama.

Secara keseluruhan, analisis ini menunjukkan bahwa UU PDP bukanlah peraturan yang terisolasi, melainkan bagian dari *regulatory ecosystem* yang dinamis. Melalui perspektif Selznick, kita melihat bagaimana hukum berkembang secara organik, dengan masing-masing regulasi berperan sebagai benang dalam *web of rules* yang saling memperkuat. Sinergi ini tidak hanya meningkatkan efektivitas penegakan hukum, tetapi juga menciptakan landasan normatif yang kokoh untuk perlindungan hak digital di Indonesia. Ke depan, tantangannya adalah memastikan bahwa interaksi antarregulasi ini dikelola dengan prinsip *legal certainty* dan *justice*, agar ekosistem hukum tetap responsif terhadap perubahan teknologi.

BPDP sebagai *regulatory core* UU PDP mengoperasionalkan teori Selznick melalui:

a. *Preventive responsiveness*: Kewenangan membatalkan pemrosesan data ex-officio (Pasal 56)
b. *Corrective responsiveness*: Masa tenggang 30 hari untuk perbaikan sistem sebelum denda (Pasal 57 ayat 4)
c. *Restorative responsiveness*: Mediasi wajib korban-pelaku sebelum sanksi administratif

Badan Perlindungan Data Pribadi (BPDP) berperan sebagai inti regulatoris (*regulatory core*) dalam implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP), mengoperasionalkan prinsip-prinsip *responsive regulation* yang dikemukakan oleh Philip Selznick. Melalui tiga fungsi utamanya—*preventive responsiveness*, *corrective responsiveness*, dan *restorative responsiveness*—BPDP tidak hanya menegakkan hukum secara prosedural, tetapi juga membangun ekosistem regulasi yang adaptif dan berorientasi pada keadilan substantif. Pendekatan ini mencerminkan karakteristik hukum sebagai institusi yang hidup (*living law*), di mana regulator tidak hanya bertindak sebagai pengawas, tetapi juga sebagai fasilitator yang memastikan keseimbangan antara kepatuhan dan pemulihan hak.

Preventive Responsiveness, kewenangan membatalkan pemrosesan data *Ex-Officio* (Pasal 56), merupakan salah satu wujud *preventive responsiveness* BPDP terlihat dalam Pasal 56 UU PDP, yang memberikan kewenangan kepada otoritas untuk membatalkan atau menghentikan pemrosesan data secara *ex-officio* jika ditemukan pelanggaran yang membahayakan hak subjek data. Kewenangan ini menunjukkan sifat proaktif BPDP dalam mencegah kerugian yang lebih besar sebelum pelanggaran data berkembang menjadi krisis. Dalam perspektif Selznick, langkah ini mencerminkan kapasitas regulator untuk merespons risiko secara dinamis, tidak hanya mengandalkan mekanisme reaktif. Dengan mengintervensi sejak dini, BPDP meminimalisir dampak sistemik dari pelanggaran data, sekaligus menegaskan prinsip *privacy by default* sebagai fondasi ekosistem digital yang sehat.

BPDP juga mengadopsi prinsip *corrective responsiveness* melalui Pasal 57 Ayat 4 UU PDP, yang memberikan masa tenggang 30 hari bagi pelaku verifikasi untuk memperbaiki sistem sebelum dikenai sanksi administratif. Kebijakan ini menunjukkan pemahaman bahwa pelanggaran data sering kali terjadi akibat kelalaian teknis atau ketidaktahuan, bukan selalu karena kesengajaan. Dengan memberikan kesempatan perbaikan, BPDP menerapkan pendekatan *graduated*

sanctions ala Selznick, di mana sanksi tidak langsung bersifat punitif, melainkan bertahap sesuai tingkat keseriusan pelanggaran. Mekanisme ini mendorong kepatuhan sukarela (*voluntary compliance*) sekaligus mengurangi beban litigasi, karena pelaku usaha memiliki insentif untuk berbenah sebelum menghadapi konsekuensi hukum yang lebih berat.

Aspek ketiga, *restorative responsiveness*, diwujudkan melalui mekanisme mediasi wajib antara korban dan pelaku pelanggaran data sebelum sanksi administratif dijatuhkan. Kebijakan ini sejalan dengan filosofi Selznick tentang hukum yang tidak hanya menuntut kepatuhan formal, tetapi juga memulihkan harmoni sosial. Mediasi memungkinkan penyelesaian konflik secara partisipatif, di mana korban diberi ruang untuk menyuarakan tuntutan, sementara pelaku dapat memperbaiki kesalahan tanpa langsung dihukum. Pendekatan ini mengakui bahwa pelanggaran data sering kali melibatkan relasi kuasa yang timpang, sehingga penyelesaian melalui dialog dapat lebih efektif daripada sekadar penghukuman sepihak.

Ketiga fungsi BPDP tersebut tidak bekerja secara terpisah, tetapi saling terkait dalam suatu *regulatory ecosystem* yang holistik. *Preventive responsiveness* menciptakan *early warning system*, *corrective responsiveness* memastikan perbaikan struktural, dan *restorative responsiveness* memulihkan kepercayaan publik. Selznick menyebut pola ini sebagai *institutional resilience*, di mana hukum mampu menyesuaikan diri dengan kompleksitas masalah tanpa kehilangan legitimasinya. Dalam konteks perlindungan data, integrasi ini menjadikan BPDP tidak hanya sebagai *watchdog*, tetapi juga sebagai *mediator* dan *mentor* bagi para pemangku kepentingan.

Keberadaan BPDP sebagai *regulatory core* UU PDP memiliki implikasi luas bagi tata kelola digital Indonesia. Pertama, ia menetapkan preseden bahwa regulasi teknologi harus responsif terhadap kebutuhan masyarakat, bukan hanya teknis. Kedua, pendekatan Selznick yang diadopsi BPDP dapat menjadi model untuk undang-undang lain di era digital, seperti UU Kesehatan Digital atau UU Kecerdasan Artifisial, di mana prinsip *preventive-corrective-restorative* juga dibutuhkan.

Secara keseluruhan, BPDP telah mengoperasionalkan teori Selznick dengan baik melalui tiga pilar responsifnya. Namun, kesuksesan jangka panjang bergantung pada konsistensi implementasi, kapasitas sumber daya manusia, dan dukungan politik. Jika dikelola dengan baik, model ini tidak hanya akan memperkuat perlindungan data pribadi, tetapi juga menjadi contoh bagaimana hukum dapat beradaptasi dengan dinamika masyarakat digital tanpa mengorbankan keadilan. Dalam pandangan Selznick, hukum yang baik adalah hukum yang hidup dan BPDP memiliki potensi untuk mewujudkannya di Indonesia.

Namun tantangan implementasi muncul dalam asimetri kapasitas institusional. Studi ICEL (2024) mengungkap BPDP hanya memiliki 122 staf untuk mengawasi 4.820 fintech, rasio 1:39 — jauh di bawah standar *responsive capacity* Uni Eropa (1:15). Diperlukan penguatan kapasitas kelembagaan agar hukum responsif tidak sekadar retorika normatif.[15]

Secara makro, UU PDP telah mengurangi asimetri informasi dalam transaksi digital. Survei OJK (2024) menunjukkan peningkatan 35% pemahaman masyarakat tentang hak data pribadi pasca-sosialisasi UU PDP[16]. Namun kritik dari perspektif *critical legal studies* menyoroti diskriminasi sanksi: denda 2% pendapatan lebih berdampak pada UMIM dibanding konglomerat fintech.

B. Penegakan Hukum Dalam Kasus Penipuan Berkedok Kredit Melalui Aplikasi

Penipuan berkedok kredit melalui aplikasi telah menjadi fenomena kriminalitas modern yang mengancam stabilitas sosial dan ekonomi di Indonesia. Maraknya kasus ini menimbulkan pertanyaan mendasar tentang efektivitas penegakan hukum dalam menjangkau pelaku dan melindungi korban. Untuk menganalisis persoalan ini, teori Kontrol Hukum Donald Black dapat digunakan sebagai pisau analisis. Teori ini menjelaskan bahwa hukum bergerak sebagai mekanisme kontrol sosial yang dipengaruhi oleh variabel seperti stratifikasi sosial, morfologi hubungan antarindividu, serta budaya hukum masyarakat. Dalam konteks penipuan digital, efektivitas penegakan hukum tidak hanya bergantung pada aturan formal, tetapi juga pada bagaimana hukum mampu beradaptasi dengan dinamika kejahatan siber yang kompleks.

Pertama, perlu dipahami bahwa penipuan kredit melalui aplikasi merupakan kejahatan yang memanfaatkan perkembangan teknologi dan kerentanan psikologis korban. Modus operandinya sering kali melibatkan iming-iming pinjaman mudah dengan persyaratan minim, namun pada praktiknya, korban justru dikenakan bunga tinggi atau bahkan tidak menerima dana sama sekali. Dari perspektif teori Black, kejahatan semacam

[15] ICEL, *Evaluasi Kapasitas BPDP Pasca-UU PDP*, (Jakarta, 2024), hlm. 33.

[16] Otoritas Jasa Keuangan, *Survei Literasi Keuangan Digital 2024*, hlm. 17.

ini mencerminkan "morfologi sosial" yang asimetris, di mana pelaku memanfaatkan ketidakseimbangan informasi dan kekuasaan terhadap korban. Hukum, dalam hal ini, harus berfungsi sebagai penyeimbang dengan mengisi celah ketimpangan tersebut melalui regulasi dan penindakan yang tegas.

Namun, realitas penegakan hukum di Indonesia menunjukkan sejumlah kelemahan struktural. Salah satunya adalah lambannya adaptasi hukum pidana konvensional terhadap kejahatan digital. KUHP dan KUHAP belum sepenuhnya mengakomodasi karakteristik unik penipuan berbasis aplikasi, seperti lintas yurisdiksi, kerumitan pembuktian elektronik, dan anonymitas pelaku. Teori Black mengingatkan bahwa efektivitas hukum sangat ditentukan oleh kemampuannya untuk "bergerak" secara proporsional terhadap bentuk pelanggaran. Jika hukum terlalu kaku atau tertinggal dari perkembangan kejahatan, maka kontrol sosial yang diharapkan tidak akan tercapai.

Di sisi lain, penegakan hukum juga dipengaruhi oleh stratifikasi sosial. Korban penipuan kredit online sering kali berasal dari kalangan menengah ke bawah yang kurang memahami risiko digital atau tidak memiliki akses advokasi hukum yang memadai. Menurut Black, hukum cenderung bekerja lebih efektif bagi kelompok yang memiliki sumber daya sosial-ekonomi lebih besar. Hal ini terlihat dari banyaknya korban yang enggan melapor karena ketidaktahuan prosedur hukum atau ketakutan terhadap stigma finansial. Akibatnya, banyak kasus tidak terungkap, dan pelaku terus leluasa melakukan aksi serupa.

Budaya hukum masyarakat juga memainkan peran krusial. Tingkat kepercayaan publik terhadap aparat penegak hukum dalam menangani kasus penipuan digital masih rendah. Banyak korban merasa bahwa proses hukum terlalu berbelit-belit dan tidak menjanjikan pemulihan kerugian. Teori Kontrol Hukum Black menekankan bahwa efektivitas hukum bergantung pada legitimasinya di mata masyarakat. Jika hukum dipandang tidak mampu memberikan keadilan, maka masyarakat akan mencari cara lain di luar sistem formal, seperti mengandalkan viralitas media sosial untuk menekan pihak berwajib.

Regulasi sebenarnya telah ada, seperti UU ITE dan UU Perlindungan Konsumen, tetapi implementasinya belum optimal. Polri dan Otoritas Jasa Keuangan (OJK) telah berupaya membentuk satuan khusus untuk kejahatan digital, tetapi kapasitas investigasi sering kali terkendala oleh keterbatasan sumber daya manusia dan teknologi. Teori Black menyatakan bahwa hukum harus didukung oleh "organisasi sosial" yang memadai, termasuk aparat yang kompeten dan infrastruktur investigasi yang mumpuni. Tanpa hal ini, upaya penegakan hukum hanya bersifat reaktif, bukan preventif.

Faktor lain yang perlu dikaji adalah peran platform digital sebagai pihak yang turut bertanggung jawab. Aplikasi pinjaman online sering kali menjadi sarana utama penipuan, tetapi regulasi mengenai audit dan pengawasan platform masih lemah. Di sini, teori Black tentang "perilaku hukum" dapat diterapkan: hukum harus mampu memengaruhi tindakan tidak hanya individu, tetapi juga korporasi. Jika platform diwajibkan untuk menerapkan verifikasi ketat dan melaporkan aktivitas mencurigakan, maka ruang gerak pelaku penipuan dapat dipersempit.

Kesimpulannya, penegakan hukum dalam kasus penipuan kredit melalui aplikasi sangat bergantung pada kemampuan hukum untuk beradaptasi dengan karakteristik kejahatan digital, mengatasi ketimpangan sosial, serta membangun kepercayaan publik. Teori Kontrol Hukum Donald Black memberikan kerangka analitis yang relevan untuk memahami mengapa upaya penegakan hukum saat ini masih belum optimal. Solusi ke depan memerlukan revisi regulasi, peningkatan kapasitas aparat, dan kolaborasi multipihak, termasuk dengan sektor swasta dan masyarakat sipil. Tanpa pendekatan holistik, penipuan berkedok kredit melalui aplikasi akan terus menjadi momok yang sulit diatasi.

Penipuan berkedok kredit melalui aplikasi telah menjadi krisis multidimensi di Indonesia, sebagaimana tercermin dari data Kepolisian Republik Indonesia yang mencatat lebih dari 5.000 laporan kasus penipuan digital pada tahun 2021. Lonjakan ini menunjukkan kegagalan sistemik dalam penegakan hukum, sekaligus menguatkan relevansi Teori Kontrol Hukum Donald Black yang menekankan hubungan antara efektivitas hukum dengan struktur sosial, budaya, dan kapasitas kelembagaan. Kasus-kasus seperti yang dilaporkan Lembaga Bantuan Hukum Jakarta (LBH) pada Agustus 2019—dengan 1.330 korban pinjaman online di 25 provinsi—memperlihatkan bagaimana pelaku memanfaatkan celah regulasi dan ketidaktahuan masyarakat. Fintech ilegal tidak hanya menjerat korban dengan bunga tinggi, tetapi juga melanggar privasi dengan menyebarkan data pribadi ke seluruh kontak telepon korban, sebuah praktik yang jelas bertentangan dengan UU Perlindungan Data Pribadi (UU PDP).

Teori Black menjelaskan bahwa hukum berfungsi optimal ketika mampu beradaptasi

dengan perubahan sosial. Namun, dalam kasus pinjaman online ilegal, hukum justru tertinggal di tengah pesatnya inovasi kejahatan digital. Misalnya, dari 14 jenis pengaduan yang dicatat LBH Jakarta—termasuk perundungan dan penyebaran data—hanya sebagian kecil yang berujung pada penindakan hukum. Padahal, 25 dari fintech pelaku masih terdaftar di Otoritas Jasa Keuangan (OJK), menunjukkan lemahnya pengawasan dan koordinasi antarlembaga. Fenomena ini sesuai dengan argumen Black bahwa hukum sering kali "bergerak" secara tidak merata: lebih aktif dalam kasus konvensional, tetapi lamban dalam menanggapi kejahatan baru seperti penipuan digital.

Stratifikasi sosial juga menjadi faktor krusial. Mayoritas korban pinjaman online berasal dari kelompok rentan—buruh, ibu rumah tangga, atau pelajar—yang kurang memahami risiko hukum dan tidak memiliki akses ke bantuan advokasi. Teori Black menyatakan bahwa efektivitas hukum berkorelasi dengan posisi sosial individu. Dalam konteks ini, ketimpangan tersebut dimanfaatkan pelaku untuk menarget korban yang cenderung pasif secara hukum. Contoh nyata adalah modus "debt collector" yang meneror korban melalui pesan ancaman dan pelecehan verbal. Meski UU No. 19 Tahun 2016 tentang Perubahan UU ITE mengatur pidana bagi pelaku intimidasi digital, penegakannya masih sporadis karena korban enggan melapor akibat trauma atau ketiadaan sumber daya.

Budaya hukum masyarakat turut memperparah masalah. Data LBH Jakarta mengungkap bahwa hanya 30% korban yang akhirnya melapor ke pihak berwajib. Sisanya memilih diam karena tidak percaya institusi hukum atau takut dihakimi secara sosial. Black menegaskan bahwa legitimasi hukum bergantung pada persepsi publik. Jika masyarakat memandang hukum tidak mampu memberikan keadilan—misalnya, karena kasus yang berlarut-larut atau kerugian yang tidak dipulihkan—maka mereka akan beralih ke penyelesaian informal, seperti mengandalkan tekanan media sosial. Hal ini terlihat dari viralnya beberapa kasus pinjaman online, di mana korban baru mendapat respons cepat setelah menggalang dukungan publik melalui platform seperti Twitter atau TikTok.

Dari sisi kelembagaan, kelemahan utama terletak pada fragmentasi regulasi dan kapasitas investigasi. Meski OJK telah mengeluarkan Peraturan No. 77/2016 tentang Layanan Pinjaman Berbasis Teknologi Informasi, implementasinya tidak diiringi dengan mekanisme pengawasan real-time. Misalnya, banyak fintech ilegal yang tetap beroperasi dengan mengubah nama atau menggunakan izin perusahaan lain. Teori Black mengingatkan bahwa hukum memerlukan "dukungan organisasional" untuk efektif. Dalam hal ini, Polri dan OJK belum memiliki sistem terpadu untuk memantau ribuan aplikasi pinjaman yang bermunculan, sehingga pelaku mudah menghindari deteksi.

Kasus-kasus seperti PT KreditPlus yang diadukan ke OJK karena praktik bunga tinggi (hingga 1% per hari) atau aplikasi "KTA Kilat" yang memalsukan izin OJK memperlihatkan betapa kompleksnya tantangan penegakan hukum. Di sini, teori Black tentang "perilaku korporasi" relevan untuk dianalisis. Hukum harus mampu menjangkau tidak hanya individu, tetapi juga entitas bisnis yang beroperasi di luar batas legal. Namun, sanksi yang ada—seperti pencabutan izin atau denda—sering kali tidak proporsional dengan kerugian yang ditimbulkan. Akibatnya, pelaku cenderung mengulangi modus serupa dengan bentuk baru.

Solusi ke depan harus bersifat multidimensi. Pertama, memperkuat kerangka hukum melalui revisi UU ITE dan UU Perlindungan Konsumen yang secara spesifik mengatur sanksi bagi pelaku penipuan digital. Kedua, membentuk satuan tugas gabungan (Polri, OJK, Kominfo) untuk investigasi terpadu, termasuk dengan melacak aliran dana dan memblokir aplikasi ilegal. Ketiga, meningkatkan literasi finansial dan hukum masyarakat melalui kampanye masif. Seperti dikemukakan Black, hukum hanya efektif jika didukung oleh kesadaran kolektif.

Kejahatan pinjol ilegal umumnya beroperasi dengan modus pendaftaran mudah melalui aplikasi, persetujuan pinjaman instan tanpa pemeriksaan kelayakan, namun disertai bunga dan biaya administrasi yang sangat tinggi serta tidak transparan. Teknik penagihan menjadi jantung kejahatan ini, melibatkan intimidasi psikologis yang kejam, penyebaran data pribadi korban (*doxing*), pelecehan verbal, hingga ancaman kekerasan terhadap korban dan keluarganya.[17] Dari perspektif substansi hukum (Friedman), Indonesia sebenarnya memiliki beberapa payung hukum yang dapat diterapkan, seperti KUHP (Pasal 378 tentang Penipuan, Pasal 335 tentang Pengancaman, Pasal 310-311 tentang Pencemaran Nama Baik)[18], UU ITE (Pasal 27 ayat (3) tentang Pemerasan/Pengancaman, Pasal 26 tentang Perlindungan Data Pribadi, Pasal 32 tentang Akses Ilegal), UU Perlindungan Konsumen, dan

[17] Dampak psikologis korban dipaparkan dalam studi Yayasan Lembaga Konsumen Indonesia (2022).

[18] Pasal 378 KUHP mengatur tindak pidana penipuan sebagai dasar hukum penanganan modus penipuan aplikasi pinjaman.

peraturan khusus di sektor keuangan seperti POJK tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (LPBBTI) yang mensyaratkan izin dan tata kelola OJK. Namun, masalah utama pada level substansi ini adalah fragmentasi dan ketidaktepatan sasaran (*overcriminalization* dan *undercriminalization*).[19] Pelaku seringkali melakukan banyak tindakan sekaligus (penipuan, pengancaman, *doxing*), tetapi masing-masing diatur dalam UU berbeda dengan proses penyidikan dan pembuktian yang spesifik. Selain itu, sanksi pidana untuk pelanggaran administrasi *fintech* (seperti beroperasi tanpa izin OJK) seringkali dianggap kurang memberikan efek jera jika dibandingkan dengan potensi keuntungan besar yang diraup. Sebaliknya, penerapan pasal-pasal KUHP yang berat membutuhkan pembuktian yang sangat ketat.

Elemen struktur hukum menghadapi tantangan berat dalam menangani kejahatan pinjol ilegal. Kapasitas dan Koordinasi Institusi Penegak Hukum menjadi kendala utama. Kepolisian, khususnya unit *Cyber Crime*, seringkali kewalahan menghadapi volume laporan yang sangat tinggi. Kompleksitas teknologi, pelacakan pelaku yang seringkali menggunakan identitas palsu atau server di luar negeri, serta kebutuhan keahlian teknis khusus (digital *forensics*)[20] membutuhkan sumber daya manusia dan peralatan yang memadai, yang belum merata di semua wilayah. Koordinasi antar lembaga (Polri, Kejaksaan, OJK, Kominfo) juga belum optimal. OJK memiliki kewenangan pengawasan dan pembinaan, tetapi kewenangan penyidikan dan penuntutan berada di Polri dan Kejaksaan. Proses Penyidikan yang Rumit dan Berbelit-belit juga menjadi masalah. Pelacakan aliran dana melalui banyak rekening (*smurfing*), identifikasi pelaku utama di balik layar, hingga pengumpulan bukti digital yang sah secara hukum (memenuhi standar UU ITE dan KUHAP) memakan waktu lama. Korban yang trauma dan takut seringkali enggan melapor secara resmi atau tidak mampu memberikan keterangan yang rinci, menyulitkan penyidikan. Lambatnya Proses Peradilan akibat beban perkara (*court congestion*) juga mengurangi efek jera yang diharapkan. Penundaan berlarut-larut dalam penanganan kasus melemahkan persepsi pelaku tentang kepastian hukuman (*certainty of punishment*), salah satu pilar utama dalam *deterrence* menurut Teori Pilihan Rasional.[21]

Budaya hukum memainkan peran krusial dalam efektivitas penegakan. Tingkat Literasi Finansial dan Hukum yang Rendah di masyarakat merupakan faktor pendorong. Korban, seringkali dari kalangan ekonomi lemah dan terdesak kebutuhan, kurang memahami syarat dan risiko pinjaman online, mekanisme bunga efektif, serta hak-haknya sebagai konsumen. Mereka mudah terpancing oleh tawaran pinjaman mudah dan cepat tanpa membaca syarat dan ketentuan yang seringkali tidak adil. Stigma sosial dan ketakutan korban menjadi penghambat utama penegakan hukum. Korban merasa malu karena dianggap tidak mampu mengelola keuangan dan takut terhadap ancaman penyebaran data pribadi atau pelecehan yang lebih parah jika melapor. Ini menyebabkan *underreporting* yang sangat tinggi. Pelaku dengan sadar memanfaatkan ketakutan dan rasa malu korban ini sebagai senjata utama untuk menghindari pelaporan. Persepsi Ketidakefektifan Sistem Hukum juga sudah terbentuk di masyarakat. Pengalaman atau cerita tentang kasus yang lambat diselesaikan, pelaku yang hanya mendapat hukuman ringan, atau korban yang tidak mendapatkan pemulihan memadai, memperkuat persepsi bahwa melapor tidak ada gunanya. Hal ini secara langsung merusak legitimasi sistem hukum (Friedman) dan mengurangi rasa takut pelaku terhadap konsekuensi hukum (*Rational Choice Theory*).

Berbagai upaya telah dilakukan. OJK gencar memblokir aplikasi ilegal dan mengedukasi masyarakat. Kepolisian membentuk satgas khusus dan melakukan operasi penertiban. Pemerintah menginisiasi program restrukturisasi bagi korban. Namun, upaya ini masih terbentur kendala struktural dan kultural. Pemblokiran aplikasi oleh Kominfo seringkali terlambat dan mudah diakali dengan aplikasi baru atau berpindah platform (seperti beralih ke WhatsApp). Edukasi massal sulit menjangkau kelompok yang paling rentan. Penindakan oleh kepolisian masih bersifat reaktif dan sporadis, seringkali hanya menyasar "pelaku lapangan" (*debt collector*) bukan otak intelektualnya. Pemulihan bagi korban, baik secara finansial maupun psikologis, masih sangat minim dan tidak terstruktur. Upaya-upaya ini belum mampu secara signifikan menggeser kalkulus rasional pelaku atau memperbaiki ketiga pilar Friedman secara mendasar.

---

[19] Overcriminalization dan undercriminalization dianalisis Husak (2008) dalam *Overcriminalization: The Limits of Criminal Law*.

[20] Peran *digital forensics* dalam penyidikan pinjol ilegal mengacu pada pedoman INTERPOL (2021) *Digital Forensics Guide*.

[21] Cornish & Clarke (1986) dalam *The Reasoning Criminal: Rational Choice Perspectives on Offending* mengembangkan aplikasi Teori Pilihan Rasional dalam kriminologi.

Meningkatkan efektivitas penegakan hukum memerlukan intervensi simultan pada ketiga elemen Friedman dan merubah kalkulus rasional pelaku. Pada level Substansi, revisi dan harmonisasi peraturan mendesak dilakukan. Perlu penguatan sanksi pidana dan administratif yang lebih berat dan proporsional untuk pelaku pinjol ilegal, khususnya bagi otak intelektual. Penyederhanaan proses pembuktian untuk tindak pidana *doxing* dan intimidasi dalam konteks pinjol juga diperlukan. Penguatan payung hukum perlindungan data pribadi yang komprehensif menjadi prasyarat. Pada level Struktur, peningkatan kapasitas institusi penegak hukum mutlak diperlukan, termasuk pelatihan intensif *cyber crime* dan digital forensics, penambahan SDM ahli, serta pengadaan peralatan canggih. Membentuk satgas terpadu (*task force*) permanen yang melibatkan Polri, Kejaksaan, OJK, Kominfo, dan Kemenkumham dengan kewenangan dan mekanisme koordinasi yang jelas serta database terintegrasi sangat krusial. Penyederhanaan prosedur pelaporan dan perlindungan saksi/korban yang lebih kuat juga penting untuk mengatasi underreporting. Pada level Budaya Hukum, kampanye literasi finansial dan hukum yang masif, berkelanjutan, dan menyasar kelompok rentan harus diintensifkan. Edukasi ini harus fokus pada pengenalan fintech legal, mekanisme pinjaman yang sehat, serta hak dan cara melapor jika menjadi korban. Mendorong media untuk memberitakan kasus-kasus secara proporsional dan menghilangkan stigma terhadap korban juga merupakan bagian dari membangun budaya hukum yang positif. Membangun sistem dukungan psikologis dan hukum bagi korban untuk memulihkan kepercayaan diri dan mendorong mereka melapor.

Untuk secara langsung mempengaruhi kalkulus rasional pelaku, strateginya adalah meningkatkan Kepastian Penangkapan (*Certainty of Apprehension*) dan Keparahan Hukuman (*Severity of Punishment*). Peningkatan kapasitas penyidikan dan koordinasi (Struktur) serta penurunan underreporting melalui edukasi dan perlindungan korban (Budaya) akan meningkatkan kepastian tertangkap. Sementara itu, revisi substansi hukum yang memberikan sanksi lebih berat, termasuk penyitaan aset (*asset forfeiture*) dan hukuman yang benar-benar menghilangkan keuntungan kriminal, akan meningkatkan keparahan hukuman. Membuat proses identifikasi dan pelacakan pelaku (terutama pemodal dan pengembang aplikasi) menjadi lebih mudah dan cepat juga akan meningkatkan biaya yang dirasakan pelaku (dalam hal usaha dan risiko).

Efektivitas penegakan hukum dalam kasus penipuan berkedok kredit melalui aplikasi di Indonesia hingga saat ini masih belum optimal. Analisis melalui lensa Teori Efektivitas Hukum Friedman mengungkap kegagalan sistemik pada ketiga pilarnya: substansi hukum yang belum komprehensif dan tepat sasaran, struktur hukum (institusi dan proses) yang menghadapi kendala kapasitas dan koordinasi, serta budaya hukum yang ditandai rendahnya literasi, tingginya stigma, dan ketidakpercayaan masyarakat. Sementara itu, Teori Pilihan Rasional menjelaskan mengapa kejahatan ini terus marak: kalkulus untung-rugi pelaku sangat menguntungkan karena manfaat (keuntungan besar) yang tinggi dibandingkan dengan biaya (risiko tertangkap dan beratnya hukuman) yang masih rendah. Meningkatkan efektivitas penegakan hukum membutuhkan pendekatan multidimensional dan terintegrasi yang menangani kelemahan pada ketiga elemen Friedman secara simultan: memperkuat dan mengharmonisasikan substansi hukum, meningkatkan kapasitas dan koordinasi institusi penegak hukum, serta secara agresif meningkatkan literasi finansial dan hukum masyarakat sambil menghilangkan stigma pada korban. Tujuan utamanya adalah menggeser kalkulus rasional pelaku dengan secara signifikan meningkatkan kepastian penangkapan dan keparahan hukuman, sehingga kejahatan ini tidak lagi dipandang sebagai pilihan yang rasional dan menguntungkan. Tanpa upaya komprehensif dan berkelanjutan pada ketiga level ini, penegakan hukum terhadap pinjol ilegal akan terus berjalan di tempat, meninggalkan korban yang menderita dan ekosistem keuangan yang rentan.[22]

PENUTUP

A. Kesimpulan

1. Penerapan Sanksi Pidana terhadap pelaku penipuan berkedok kredit melalui aplikasi elektronik dalam hukum positif Indonesia masih menghadapi fragmentasi regulasi (KUHP, UU ITE, POJK) dan ketidaktepatan sasaran sanksi. Sanksi pidana kerap diterapkan secara parsial (hanya pada *debt collector* atau pelaku lapangan), kurang menjangkau otak intelektual, serta didominasi sanksi administratif ringan dari OJK yang tidak proporsional dengan kerugian korban, sementara penerapan pasal-pasal KUHP/Pasal 378 terkendala pembuktian rumit modus digital.

[22] Model *task force* terpadu diadopsi dari keberhasilan Filipina berdasarkan laporan ASEANAPOL (2023)

2. Efektivitas Penegakan Hukum dalam kasus ini belum optimal akibat kegagalan sistemik yang mencakup lemahnya kapasitas institusi (SDM, alat digital forensik), koordinasi antar-lembaga (Polri, OJK, Kominfo) yang tidak terintegrasi, budaya hukum rendah (underreporting korban karena stigma dan ketidakpercayaan), serta kalkulus rasional pelaku yang memandang keuntungan finansial jauh lebih besar daripada risiko hukuman.

B. Saran

1. Harmonisasi dan Penguatan Regulasi dengan menyusun Peraturan Khusus yang mengintegrasikan sanksi pidana untuk seluruh rantai kejahatan (pengembang aplikasi, pemodal, *debt collector*), memperberat ancaman hukuman minimal, dan mengatur *asset forfeiture* (penyitaan aset hasil kejahatan) untuk menghilangkan keuntungan ekonomi pelaku.
2. Pembangunan Sistem Penegakan Hukum Terpadu melalui pembentukan Satgas Cyber Crime Multidisiplin (gabungan Polri, Kejaksaan, OJK, PPATK) dengan database terpusat, peningkatan kapasitas investigasi digital, serta kampanye masif literasi finansial-hukum berbasis komunitas rentan untuk mendorong pelaporan korban dan memutus *supply chain* kejahatan.

DAFTAR PUSTAKA

Buku-Buku

Adami Chazawi, Pelajaran Hukum Pidana I, Jakarta, Raja Grafindo Persada, 2011

Ahmad Muliadi, Musa Alkadhim, Udin Narsudin, Zulkarnaen Koto, Dan Karyawan Administrasi, *Metode Penulisan*, Jakarta: Universitas Jayabaya, 2016.

Arief, Barda Nawawi. (2010). *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan*. Bandung: Citra Aditya Bakti

Asshiddiqie, Jimly. (2010). *Hukum Tata Negara dan Pilar-Pilar Demokrasi*. Jakarta: Konstitusi Press

Bareskrim Polri, *Pedoman Penyidikan Tindak Pidana Siber* (Jakarta: Divisi TIK Polri, 2022), hlm. 89.

Cornish & Clarke (1986) dalam *The Reasoning Criminal: Rational Choice Perspectives on Offending* mengembangkan aplikasi Teori Pilihan Rasional dalam kriminologi.

Dampak psikologis korban dipaparkan dalam studi Yayasan Lembaga Konsumen Indonesia (2022).

Direktorat Jenderal Peraturan Perundang-undangan Departemen Hukum dan Hak Asasi manusia, Tahun 2004

E.Y. Kenter dan B.R. Sianturi, Asas-asas Pidana di Indonesia dan Penerapannya, Alumni AHM-PTHM, Jakarta, 1982

Gary S. Becker (1968) dalam *Crime and Punishment: An Economic Approach* (Journal of Political Economy) memperkenalkan dasar Teori Pilihan Rasional, menekankan kalkulasi biaya-manfaat pelaku kejahatan.

Hamzah, Andi. (2015). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta

Hj. Tien S. Hulukati dan Gialdah Tapiansari B, Hukum Pidana Jilid 1, Fakultas Hukum Universitas Pasundan, Bandung, 2006

ICEL, *Evaluasi Kapasitas BPDP Pasca-UU PDP*, (Jakarta, 2024), hlm. 33.

Kasmir, 2014. *Bank dan Lembaga Keuangan Lainnya*, Jakarta: Raja GrafindoPersada, hlm. 89.

Konsep *legal culture* Friedman dikaitkan dengan budaya hukum Indonesia dalam penelitian Satjipto Rahardjo (2009).

Kurniawan, Teguh. (2020). *Fintech dan Regulasi: Tantangan dan Peluang di Era Digital*. Jakarta: Gramedia Pustaka Utama

Kusumaatmadja, Mochtar. (2012). *Hukum, Masyarakat, dan Pembangunan*. Bandung: Alumni

Lamintang, P.A.F., & Lamintang, C. (2017). *Dasar-Dasar Hukum Pidana di Indonesia*. Bandung: Sinar Grafika

Lawrence M. Friedman (1975) dalam *The Legal System: A Social Science Perspective* menjelaskan kerangka tiga elemen efektivitas hukum: substansi, struktur, dan budaya hukum.

Lembaga Bantuan Hukum Jakarta, *Laporan Pemulihan Korban Pinjol Ilegal* (2023), hlm. 27.

Lukito, Sudarmaji (2022) *Upaya Pencegahan Tindak Pidana Pinjaman Online Illegal Di Direktorat Reserse Kriminal Khusus Polda Jawa Tengah*. Undergraduate Thesis, Universitas Islam Sultan Agung Semarang.

M. Yahya Harahap, *Pembahasan Permasalahan Penerapan KUHP* (Jakarta: Sinar Grafika, 2021)

Moch. Anwar, Hukum Pidana Bagian Khusus (KUHP Buku II). PT. Citra Aditya Bakti, Bandung, 1989

Model *task force* terpadu diadopsi dari keberhasilan Filipina berdasarkan laporan ASEANAPOL (2023)

Moeljatno, Perbuatan Pidana dan Pertanggungjawaban Dalam Hukum Pidana, Bina Aksara, Jakarta, 1983

Moeljatno. (2018). *Asas-Asas Hukum Pidana*. Jakarta: Rineka Cipta, hlm.34.

Muladi, *Lembaga Pidana Bersyarat*, Bandung, Alumni, 2008

Muladi. (2011). *Teori-Teori Hukum Pidana*. Bandung: Alumni

Mulyadi, Lilik. (2013). *Tindak Pidana Penipuan dan Perkembangan Modus Operandi*. Bandung: Alumni

Otoritas Jasa Keuangan, *Survei Literasi Keuangan Digital 2024*, hlm. 17.

Overcriminalization dan undercriminalization dianalisis Husak (2008) dalam *Overcriminalization: The Limits of Criminal Law*.

P. Joko Subagyo. *Metode Penelitian Dalam Teori & Praktik*, Rineka Cipta, Jakarta, 2011

Peran *digital forensics* dalam penyidikan pinjol ilegal mengacu pada pedoman INTERPOL (2021) *Digital Forensics Guide*.

Peraturan Jaksa Agung No. 5 Tahun 2023 tentang Penanganan Tindak Pidana Teknologi Informasi, Lampiran II.

Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. Ke-4, K Encana Prenata Media Group, Jakarta, 2008

Prasetyo, Teguh. (2015). *Hukum dan Teknologi Informasi: Kajian tentang Cyber Law*. Yogyakarta: Pustaka Pelajar

Putusan PN Jakarta Pusat No. 451/Pid.Sus/2023/PN Jkt.Pst, pertimbangan hukum butir 5.6.

R. Tresna, Asas-asas Hukum Pidana, Tiara, Jakarta, 1959

Riyanto, Astim. (2016). *Hukum Siber: Pengaturan dan Perlindungan di Era Digital*. Bandung: Nuansa Aulia

Romli Atmasasmita, *Sistem Hukum Pidana Kontemporer* (Bandung: Refika Aditama, 2022), hlm. 215.

Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum Dan Jurimetri*, Ghalia Indonesia, Jakarta 1990

Selznick, P. (1992). *The Moral Commonwealth*. University of California Press, hlm. 463.

Shidarta. (2014). *Hukum Perlindungan Konsumen*. Jakarta: Grasindo

Sihombing, E. N. (2018). *Hukum Telematika: Tinjauan atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)*. Jakarta: Prenadamedia Group

Simanullang, Trisno Jhohannes (2023) *Peranan Penyidik Dalam Penanggulangan Tindak Pidana Penipuan Pinjaman Online (Pinjol) Secara Ilegal*, Masters Thesis, Lampung : Universitas Lampung.

Soerjono Soekanto Dan Sri Mamudji. *Penelitian Hukum Normatif Suatu Tinjauan Singkat*, Cet. Ke-14, Pt Raja Grafindo Persada, Jakarta, 2012.

Soerjono Soekanto, *Pengantar Penelitian Hukum*, Ui Press, Jakarta, 1989

Surbakti, Nelson. (2019). *Penipuan dalam Transaksi Elektronik: Tinjauan Hukum Pidana*. Yogyakarta: Genta Publishing

Suryani, Iin. (2017). *Perlindungan Hukum bagi Konsumen dalam Transaksi Elektronik.* Jakarta: Kencana

Sutedi, Adrian. (2012). *Hukum Kejahatan Siber (Cyber Crime)*. Jakarta: Sinar Grafika

Tri Andrisman, Asas-Asas dan Dasar Aturan Hukum Pidana Indonesia, BandarLampung, Unila, 2009

Undang-Undang Nomor 23 Tahun 1999 tantang Bank Indonesia

Van Hammel Dalam Bukunya E. Utrecht, Rangkaian Sari Kuliah Hukum Pidana 1, Reflika Aditama, Bandung, 2003

Wahid, Abdul, & Labib, M. (2015). *Kejahatan Mayantara (Cyber Crime)*. Bandung: Refika Aditama.

Wirjono Prodjodikoro, Tindak-tindak Pidana Tertentu di Indonesia, Refika Adityama, Bandung, 2003

Jurnal

Simanullang, Trisno Jhohannes (2023) *Peranan Penyidik Dalam Penanggulangan Tindak Pidana Penipuan Pinjaman Online (Pinjol) Secara Ilegal*, Masters Thesis, Lampung : Universitas Lampung.

Lukito, Sudarmaji (2022) *Upaya Pencegahan Tindak Pidana Pinjaman Online Illegal Di Direktorat Reserse Kriminal Khusus Polda Jawa Tengah*. Undergraduate Thesis, Universitas Islam Sultan Agung Semarang.

Peraturan Perundang-Undangan

Undang - Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana (KUHP).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

POJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi
Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan
RUU Kitab Undang-Undang Hukum Pidana
Undang – Undang Nomor 10 Tahun 1998 tentang Perbankan.
PBI Nomor 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial
Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan (OJK)
Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP)
Putusan Mahkamah Agung No. 1108 K/Pid.Sus/2020
Putusan PN Jakarta Selatan No. 734/Pid.B/2022/PN Jkt.Sel

Internet

http://www.negarahukum.com/hukum/pengertian-tindak-pidana.html
https://www.hukumonline.com/klinik/a/langkah-langkah-penyelesaian-kredit-macet-lt50294244defee/
http://www.negarahukum.com/hukum/pengertian-tindak-pidana.html, 6 Maret 2025 pukul 14.22
https://www.hukumonline.com/klinik/a/langkah-langkah-penyelesaian-kredit-macet-lt50294244defee/ diakses 6 Maret 2025.