*Journal of International Multidisciplinary Research*

# Penanggulangan Tindak Pidana Penipuan Online oleh Satuan Reserse Kriminal Kepolisian Resor Kota Yogyakarta dalam Menjamin Perlindungan Hukum bagi Korban

**Albertus Bagas Satria[1*], Kastowo[2], Widiartana [3]**
Magister Hukum, Universitas Atmajaya, Yogyakarta, Indonesia
alblertussatriasmatn@gmail.com[1], maskatho99@gmail.com[2], gwidiartana@gmail.com[3]

**Informasi Artikel**
E-ISSN : 3026-6874
Vol: 3 No: 10 Oktober 2025
Halaman : 21-29

**Abstract**
*The study aims to examine the handling of online fraud crimes by the Criminal Investigation Unit (Satreskrim) of the Yogyakarta City Police, which has been considered inadequate in providing legal protection for victims, as well as to formulate effective strategies for combating online fraud that can ensure optimal legal protection.This research adopts an empirical legal approach combined with sociological and statutory approaches. The primary data were obtained directly from interviews with officers of the Yogyakarta City Police and representatives of the Financial Services Authority (OJK) of the Special Region of Yogyakarta, while the secondary data consisted of primary and secondary legal materials analyzed through qualitative legal analysis methods. The results indicate that the handling of online fraud crimes by the Yogyakarta City Police has not yet been able to provide maximum legal protection for victims. This is due to the lengthy nature of the legal process and the existence of coordination barriers with external institutions such as the Financial Services Authority (OJK) and banking institutions, caused by strict regulations and bureaucratic procedures. Consequently, victims often fail to obtain legal certainty or clarity regarding compensation or recovery of their losses, meaning that their rights have not been fulfilled optimally.*

**Keywords:**
Online Fraud
Legal Protection
Victimology

***Abstrak***
Penelitian ini bertujuan untuk mengkaji penanganan tindak pidana penipuan online oleh Satuan Reserse Kriminal (Satreskrim) Kepolisian Resor Kota Yogyakarta yang dinilai belum optimal dalam memberikan perlindungan hukum bagi korban, serta untuk merumuskan strategi penanggulangan penipuan online yang efektif guna menjamin perlindungan hukum yang maksimal.Penelitian ini menggunakan pendekatan hukum empiris yang dikombinasikan dengan pendekatan sosiologis dan peraturan perundang-undangan. Data primer diperoleh langsung melalui wawancara dengan aparat Kepolisian Resor Kota Yogyakarta dan perwakilan Otoritas Jasa Keuangan (OJK) Daerah Istimewa Yogyakarta, sedangkan data sekunder terdiri atas bahan hukum primer dan bahan hukum sekunder yang dianalisis menggunakan metode analisis hukum kualitatif.Hasil penelitian menunjukkan bahwa penanganan tindak pidana penipuan online oleh Kepolisian Resor Kota Yogyakarta belum mampu memberikan perlindungan hukum yang maksimal bagi korban. Hal ini disebabkan oleh lamanya proses hukum serta adanya hambatan koordinasi dengan lembaga eksternal seperti Otoritas Jasa Keuangan (OJK) dan lembaga perbankan akibat regulasi yang ketat dan prosedur birokrasi yang panjang. Akibatnya, korban sering kali tidak memperoleh kepastian hukum maupun kejelasan terkait kompensasi atau pemulihan kerugian yang dialami, sehingga hak-hak mereka belum terpenuhi secara optimal.

**Kata Kunci** : Penipuan Online, Perlindungan Hukum, Viktimologi

## PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di Indonesia telah membawa perubahan signifikan terhadap perilaku sosial, ekonomi, dan hukum masyarakat. Transformasi digital yang semakin masif menumbuhkan pola interaksi baru dalam kehidupan publik, termasuk dalam sektor ekonomi melalui transaksi daring yang semakin meningkat. Namun, di balik kemajuan tersebut, muncul bentuk-bentuk kejahatan baru yang memanfaatkan teknologi, salah satunya adalah tindak pidana penipuan online (online fraud), yang kini menjadi salah satu ancaman serius terhadap keamanan digital dan

perlindungan konsumen di Indonesia. Data Kementerian Komunikasi dan Informatika menunjukkan bahwa pada tahun 2023 tercatat lebih dari 110.000 rekening bank terindikasi terlibat dalam aktivitas penipuan online, yang menandakan eskalasi signifikan kejahatan siber di Indonesia. Kota Yogyakarta, sebagai salah satu pusat pendidikan dan perdagangan daring, turut mengalami peningkatan kasus penipuan berbasis teknologi digital. Polresta Yogyakarta mencatat peningkatan laporan kejahatan siber yang didominasi oleh modus penipuan jual beli daring melalui media sosial seperti Facebook dan Instagram. Modus yang digunakan pelaku antara lain membuat akun fiktif, mengirim bukti transfer palsu, hingga menyamarkan identitas melalui penggunaan Virtual Private Network (VPN)

Kondisi ini menunjukkan bahwa sistem hukum nasional masih menghadapi tantangan besar dalam menanggulangi penipuan online, terutama dalam hal perlindungan hukum bagi korban. Proses penegakan hukum terhadap kasus penipuan online cenderung memakan waktu lama dan terkendala oleh birokrasi serta koordinasi antar lembaga, seperti Kepolisian, Otoritas Jasa Keuangan (OJK), dan perbankan. Banyak korban yang mengalami kesulitan dalam memperoleh kepastian hukum dan pengembalian kerugian akibat keterbatasan regulasi serta lambatnya proses investigasi digital. Fenomena ini memperlihatkan adanya kesenjangan antara norma hukum dan implementasi perlindungan korban di lapangan. Penelitian-penelitian sebelumnya seperti yang dilakukan oleh Silvony Kakoe (Universitas Brawijaya, 2020) dan Haris Dermawan (Universitas Prima Indonesia, 2021) menunjukkan bahwa fokus penegakan hukum masih dominan pada aspek pidana terhadap pelaku, sedangkan hak-hak korban, seperti restitusi, kompensasi, dan rehabilitasi, sering kali terabaikan. Padahal, menurut Barda Nawawi Arief (2018), tujuan hukum pidana tidak hanya menghukum pelaku, tetapi juga harus memulihkan keseimbangan sosial dan memberikan keadilan kepada korban melalui prinsip restorative justice.

Hasil observasi awal peneliti di Satreskrim Polresta Yogyakarta menunjukkan bahwa sebagian besar laporan korban penipuan online tidak segera mendapatkan tindak lanjut karena minimnya alat bukti elektronik yang valid dan keterbatasan kapasitas penyidik dalam menelusuri jejak digital pelaku. Hambatan lainnya berupa regulasi perbankan yang membatasi akses penyidik terhadap data rekening yang dicurigai, serta lambatnya proses digital forensics akibat kurangnya tenaga ahli dan fasilitas teknologi pendukung. Akibatnya, sebagian besar korban tidak memperoleh kejelasan mengenai status perkara maupun pemulihan kerugian yang dialami. Kondisi tersebut mempertegas urgensi penelitian ini, yaitu perlunya formulasi strategi penanggulangan tindak pidana penipuan online yang lebih efektif, terukur, dan berorientasi pada perlindungan hukum bagi korban. Penelitian ini mengadopsi pendekatan hukum empiris dengan fokus analisis terhadap efektivitas penanganan oleh Satreskrim Polresta Yogyakarta dalam konteks perlindungan korban. Aspek empiris menjadi penting karena memberikan gambaran nyata tentang sejauh mana norma hukum mampu diimplementasikan dalam praktik penyidikan kejahatan siber di daerah.

Selain itu, relevansi penelitian ini juga diperkuat oleh teori Victimology dan Teori Perlindungan Hukum (Arief, 2019) yang menempatkan korban sebagai subjek utama dalam proses peradilan pidana. Teori ini menegaskan bahwa pemenuhan hak korban atas keadilan dan kepastian hukum merupakan indikator keberhasilan sistem hukum pidana modern. Dengan demikian, sistem penegakan hukum yang humanis dan berbasis perlindungan korban perlu dikembangkan melalui sinergi lintas lembaga, peningkatan literasi digital masyarakat, serta pembaruan regulasi untuk mengakomodasi dinamika kejahatan siber.

Dengan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis penanggulangan tindak pidana penipuan online oleh Satreskrim Polresta Yogyakarta yang dinilai belum mampu memberikan perlindungan hukum maksimal bagi korban, serta untuk merumuskan strategi kebijakan yang efektif dalam menjamin hak-hak korban melalui pendekatan hukum yang integratif antara upaya preventif, preemtif, dan represif. Penelitian ini diharapkan dapat berkontribusi terhadap pengembangan kajian hukum pidana, khususnya dalam penegakan hukum siber yang berkeadilan dan berpihak pada korban. Lebih jauh, hasil penelitian ini diharapkan mampu memberikan masukan bagi pembuat kebijakan dan aparat penegak hukum dalam memperkuat sistem perlindungan hukum terhadap masyarakat dari ancaman kejahatan penipuan berbasis teknologi.

## METODE

Penelitian ini menggunakan pendekatan hukum empiris (*socio-legal research*), yaitu metode penelitian yang tidak hanya menelaah hukum sebagai norma tertulis (law in books), tetapi juga menelusuri bagaimana hukum itu diimplementasikan dalam praktik sosial (law in action). Pendekatan ini digunakan karena penelitian berfokus pada efektivitas penegakan hukum terhadap tindak pidana penipuan online oleh Satreskrim Polresta Yogyakarta, serta sejauh mana penerapan aturan hukum positif seperti KUHP dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) mampu menjamin perlindungan hukum bagi korban. Pendekatan ini sejalan dengan pandangan Soerjono Soekanto (2006) bahwa efektivitas hukum tidak hanya diukur dari keberadaan norma, tetapi dari kemampuan aparat dan masyarakat dalam melaksanakannya secara nyata.

Jenis penelitian ini adalah studi kasus, yang menurut Stake (1995) bertujuan memberikan pemahaman mendalam terhadap fenomena sosial melalui konteks tertentu. Studi kasus dipilih agar peneliti dapat mengamati secara detail mekanisme penanganan penipuan online di lingkungan Satreskrim Polresta Yogyakarta, termasuk tahapan penyidikan, hambatan koordinasi antarinstansi, dan efektivitas upaya perlindungan terhadap korban.

Lokasi penelitian ditetapkan di Polresta Yogyakarta, khususnya Satuan Reserse Kriminal (Satreskrim) Unit V Tindak Pidana Khusus (Tipidsus) karena unit ini secara langsung menangani perkara penipuan online di wilayah hukum Yogyakarta. Subjek penelitian meliputi penyidik Satreskrim Polresta Yogyakarta, pejabat Otoritas Jasa Keuangan (OJK) Daerah Istimewa Yogyakarta, serta korban penipuan online. Pemilihan subjek dilakukan secara purposive sampling, yaitu penentuan informan secara sengaja berdasarkan pengalaman dan relevansi dengan topik penelitian. Menurut Sugiyono (2022), teknik purposif tepat digunakan dalam penelitian kualitatif karena memungkinkan peneliti memperoleh data yang mendalam dari informan yang benar-benar memahami fenomena yang dikaji.

Data dalam penelitian ini terdiri atas data primer dan data sekunder. Data primer diperoleh melalui wawancara mendalam (in-depth interview) dengan penyidik, pejabat OJK, dan korban penipuan online. Wawancara dilakukan secara semi-terstruktur dengan pertanyaan terbuka agar informan dapat menjelaskan pengalaman, hambatan, dan persepsi terhadap pelaksanaan perlindungan hukum bagi korban. Sedangkan data sekunder diperoleh melalui studi kepustakaan (library research) dengan menelaah berbagai literatur seperti buku, jurnal ilmiah, peraturan perundang-undangan, laporan lembaga resmi, dan dokumen hukum terkait kejahatan siber dan perlindungan korban.

Proses pengolahan data dilakukan secara analisis kualitatif dengan tiga tahapan: reduksi data, penyajian data, dan penarikan kesimpulan. Pada tahap reduksi, peneliti menyeleksi dan mengelompokkan data sesuai tema seperti bentuk perlindungan hukum, kendala penyidikan, dan sinergi antar lembaga. Tahap penyajian dilakukan dengan menata hasil wawancara dan dokumen hukum dalam bentuk narasi deskriptif. Selanjutnya, peneliti menarik kesimpulan dengan menginterpretasikan data empiris berdasarkan teori hukum dan prinsip victimology untuk merumuskan model penanggulangan tindak pidana penipuan online yang lebih efektif.

Untuk menjamin keabsahan data, penelitian ini menggunakan teknik triangulasi sumber dan metode, yaitu membandingkan hasil wawancara antarresponden (penyidik, korban, dan pejabat OJK) serta mencocokkannya dengan temuan dokumen hukum dan data sekunder. Menurut Moleong (2017), triangulasi merupakan langkah penting dalam penelitian kualitatif guna memastikan validitas, konsistensi, dan kredibilitas hasil penelitian. Dengan pendekatan ini, hasil penelitian diharapkan mampu memberikan gambaran empiris yang akurat mengenai efektivitas penanganan tindak pidana penipuan online dan bentuk perlindungan hukum yang diterima korban di wilayah hukum Polresta Yogyakarta.

## HASIL DAN PEMBAHASAN

Hasil penelitian di atas semakin mempertegas bahwa problem pokok penanganan penipuan online tidak berdiri sendiri, melainkan merupakan hasil interaksi dari tiga lapis persoalan: arsitektur regulasi yang belum sepenuhnya sinkron, kapasitas organisasi penegak hukum yang belum adaptif terhadap kompleksitas bukti elektronik, serta ekosistem layanan keuangan–platform digital yang belum terikat pada standar respons terpadu berbasis waktu. Dalam kerangka itu, indikator keberhasilan penegakan hukum tak bisa lagi dipersempit pada penangkapan dan pelimpahan perkara, tetapi harus memasukkan ukuran pemulihan korban sebagai outcome inti. Pola pikir ini relevan karena data temuan lapangan menunjukkan penurunan persentase penyelesaian kasus ketika beban laporan meningkat; sebuah tanda bahwa mekanisme yang ada belum mampu mengatasi bottleneck koordinasi bukti elektronik dan asset freezing lintas lembaga secara tepat waktu. Penekanan pemulihan korbanalih-alih semata penghukuman pelakubukan hanya tuntutan moral victimology, melainkan juga desain efisiensi sistem yang menutup peluang keuntungan kejahatan secara cepat melalui jalur keuangan formal, e-money, dan kanal kripto yang kini mudah diakses.

Kesenjangan antara norma dan praktik terlihat nyata pada tingginya transaction cost yang harus ditanggung korban. Sejak pelaporan pertama, tidak tersedia single window untuk komunikasi dan umpan balik berkala; korban harus kembali ke kantor polisi, menyusun ulang kronologi, atau menyerahkan tambahan bukti mengikuti ritme administratif yang tidak selalu paralel dengan sifat volatile evidence digital. Di titik ini, prinsip due process of law yang menjamin kepastian prosedural justru berbalik menjadi beban prosedural bagi korban ketika tidak diiringi standar waktu dan kanal informasi yang bisa diprediksi. Problem tersebut muncul berulang dalam studi empiris setempat dan juga dipotret dalam telaah terdahulu yang memfokuskan pada kendala koordinasi lintas lembaga di wilayah hukum Polresta Yogyakarta, khususnya pada fase permintaan data perbankan, penelusuran aliran dana, hingga pemblokiran rekening terkait hasil kejahatan.

Keterbatasan kapasitas forensik digital di tingkat Polresta terlihat dari ketergantungan pada dukungan Mabes yang menimbulkan antrean dan jeda penanganan, sementara sifat bukti elektronik menuntut first response yang cepatmisalnya pengamanan log, header komunikasi, session data, device fingerprint, atau artefak aplikasi messaging yang punya masa simpan terbatas. Tanpa protokol triage digital di garda depan, bukti rentan hilang atau integritasnya dipertanyakan, yang pada gilirannya memperlemah konstruksi pembuktian di tahap lanjut. Dengan merujuk asas pencegahan Beccaria, kepastian dan kecepatan adalah dua sisi mata uang yang menentukan efek jera; jika proses awal lamban, pelaku mendapat ruang untuk mengaburkan jejak transaksi, memindahkan dana pada rekening money mule, atau menukarnya ke aset kripto yang kemudian “diputihkan” melalui mixing services. Dalam banyak kejadian, rantai forensik finansial pecah pada 24–72 jam pertama, periode ketika respons antar lembaga justru paling rentan tertunda.

Di sisi lain, rendahnya literasi digital publik dan asymmetric information antara pelaku dengan korban menjelaskan mengapa pola viktimisasi berulang tetap tinggi. Korban yang pernah tertipu bukan hanya berpotensi kembali menjadi sasaran, tetapi juga mengalami penurunan kepercayaan pada kanal digital formal sehingga beralih pada praktik transaksi informal yang ironisnya lebih berisiko. Program pencegahan yang ada masih bertumpu pada kampanye persuasif dan sosialisasi tidak berkala; belum terlihat rancangan yang menautkan edukasi berbasis risk profiling komunitas, nudges perilaku di titik transaksi (point-of-decision), serta mekanisme real-time warning lintas platform. Penguatan early warning system yang memadukan data blacklist rekening, pengenal pola percakapan menipu, dan red flags transaksi mikro merupakan kebutuhan mendesak. Model demikian dapat dirancang privacy-

preserving melalui hashing identitas dan tokenized alerts sehingga tetap sejalan dengan rezim perlindungan data pribadi.

Muncul pertanyaan mendasar: apa ukuran minimum agar negara dapat dikatakan "hadir" bagi korban di ruang digital? Penelitian ini mengusulkan serangkaian penanda kinerja (key performance indicators) yang terukur di tingkat proses dan hasil. Pada tingkat proses: waktu respons awal polisi setelah laporan masuk; waktu handover ke unit siber; waktu pengiriman surat permintaan data ke perbankan; dan waktu penerimaan jawaban perbankan hingga eksekusi freeze. Pada tingkat hasil: persentase kasus dengan dana yang berhasil diamankan; persentase korban yang menerima status update berkala; dan skor kepuasan korban atas proses. Integrasi indikator proses–hasil ini membuat sistem lebih akuntabel: jika waktu freeze melampaui ambang batas, korban berhak memperoleh penjelasan tertulis dan jalur eskalasi otomatis. Kerangka indikator demikian sejalan dengan narasi empiris penelitian pendahulu yang menekankan bahwa kendala koordinasi dan lamanya proses administratif adalah variabel dominan yang menggerogoti perlindungan korban.

TDalam horizon regulasi, kejelasan batas antara kerahasiaan data finansial dan kebutuhan law enforcement perlu dinormakan melalui protocol exception berbasis time-bound necessity. Dengan kata lain, rezim kerahasiaan bukan dihapuskan, melainkan diberi fast-track ketika indikator probable cause terpenuhimisalnya bukti transfer segera sebelum pengaduan, tautan bukti percakapan, dan device binding korban–pelaku. Fast-track itu menyertakan format permintaan data baku, kanal pertukaran aman, dan nomor tiket tunggal lintas lembaga agar jejak administratif terdokumentasi dan dapat diaudit. Dalam praktik global, desain trusted data hub yang menampung minimal viable datacontoh: masked account number, timestamped transaction hash, dan receiving bank codedapat menolong penyidik lokal memotong waktu pelacakan awal, sekaligus menjaga data minimization.

Di level kelembagaan, Polresta dapat membentuk Cyber Response Cell skala kota dengan mandat rapid triage bukti elektronik, koordinasi segera ke PPATK/OJK/bank, dan pendampingan korban berlandaskan SOP waktu. Unit kecil ini tidak perlu menggandakan semua fungsi Mabes, namun berperan sebagai first responder digital yang memastikan tidak ada golden hours yang hilang. Kompetensi kunci yang dibutuhkan meliputi live evidence handling, pemetaan transaksi mikro, penyusunan mutual legal assistance sederhana untuk platform asing, dan open-source intelligence (OSINT) untuk mengaitkan identitas digital pelaku lintas platform. Pendirian cell semacam ini juga merespons temuan riset sebelumnya tentang keterbatasan kapasitas penyidikan siber di tingkat daerah dan ketergantungan ke pusat.

Dari perspektif korban, kehadiran Victim Helpdesk & Case Tracker yang mobile-first menjadi pembeda pengalaman. Fitur inti yang direkomendasikan adalah pendaftaran laporan yang otomatis menghasilkan nomor tiket; unggah bukti yang forensically sound (dengan metadata preservation); timeline proses yang diperbarui oleh penyidik; dan kanal konsultasi singkat mengenai langkah perlindungan lanjutan (misal, pemblokiran SIM card ganda, reset kredensial, atau transaction dispute ke bank). Transparansi proses mengurangi informational anxiety, menekan biaya transaksi korban, dan mengubah beban administrasi menjadi digital self-service. Rancangan ini bukan sekadar front-end layanan publik, melainkan instrumen akuntabilitas yang memaksa seluruh rantai proses tunduk pada tenggat waktusekaligus memperlihatkan backlog yang sesungguhnya.

Pada sisi pemulihan, restitutive pathway perlu dinormalisasi sejak awal penyidikan, bukan baru dibicarakan di ujung perkara. Penyidik dapat memakai dua jalur paralel: jalur pidana untuk pembuktian dan jalur perdata-administratif untuk chargeback transaksi atau klaim ganti rugi melalui mekanisme yang diatur otoritas sektor jasa keuangan. Kejelasan rute pemulihan di muka memperkecil kekecewaan

korban yang selama ini hanya memperoleh kabar tentang penangkapan tanpa kepastian pengembalian kerugian. Pengalaman empiris lokal memperlihatkan bahwa "kasus selesai" dalam arti administrasi tidak selalu identik dengan "korban pulih"; jurang inilah yang harus ditutup oleh desain prosedur baru. Pengamatan ini selaras dengan fokus penelitian terdahulu yang menyimpulkan hak-hak korban belum terpenuhi optimal meski proses penindakan berjalan, akibat lamanya birokrasi dan minimnya prioritas pada pemulihan.

Pendekatan kriminologis juga memberi pembacaan mengapa deterrence belum bekerja efektif. Tekanan struktural (strain) dan pembelajaran dalam komunitas menyimpang (asosiasi diferensial) menjelaskan regenerasi pelaku di tengah peluang gain yang cepat, risiko yang dirasa rendah, serta lemahnya guardianship digital. Kebijakan yang menurunkan expected payoffcontohnya, auto-freeze untuk transaksi berisiko tinggi yang dipicu pola tertentuakan menekan insentif pelaku. Hal ini perlu sejalan dengan peningkatan perceived certainty lewat publikasi metrik keberhasilan freeze within 72h dan funds returned per triwulan untuk memberi sinyal publik bahwa sistem kini "cepat dan pasti." Jika indikator ini membaik, rational choice pelaku akan terdorong untuk meninggalkan modus yang sama karena profitability window menyempit.

Aspek lain yang jarang disentuh adalah secondary victimizationyakni kerusakan reputasi digital korban. Dalam praktik, pelaku kerap menyalahgunakan identitas korban untuk mengakses layanan, meminjam akun marketplace, atau menipu jaringan sosial korban. Di sini, pemulihan tidak cukup dengan pengembalian dana; perlu paket rehabilitasi reputasi digital berupa takedown konten, pemulihan kredensial, dan pernyataan resmi yang memulihkan kredibilitas korban. Poin ini krusial bagi pelaku usaha mikro yang hidup dari reputasi daring; tanpa pemulihan nama baik, kerugian ekonomi akan bersifat kumulatif meski perkara pidana selesai.

Di tataran pembuktian, hybrid evidentiary approach layak diadopsi: menggabungkan bukti langsung (transkrip percakapan, payment receipt, geolokasi), bukti pola (frekuensi akun tujuan, jam transaksi, device fingerprint), dan bukti ahli (analisis log aplikasi, chain-of-custody). Dengan standar ini, penyidik tidak bergantung pada satu jenis bukti yang mudah dipatahkan, tetapi membangun web of inference yang robust. Dalam konteks ini, checklist first responder digital di tingkat Polresta menjadi alat sederhana namun berdampak: mengunci phone state, mematikan sinkronisasi otomatis yang dapat mengubah timestamp, dan melakukan lossless export percakapan dengan hash verification. Sebagian rekomendasi teknis ini beresonansi dengan deskripsi kebutuhan penguatan kapasitas yang juga direkam dalam telaah empiris sebelumnya di Polresta Yogyakarta.

Di wilayah pencegahan, strategi komunikasi publik perlu beralih dari "kampanye umum" ke behaviorally informed messaging. Misalnya, just-in-time warnings yang muncul pada momen kritis (saat hendak mentransfer ke rekening baru, sistem memunculkan peringatan: rekening berisiko; tampilkan tautan blacklist dan opsi menunda transaksi 2 jam). Pesan digubah singkat, loss-framed ("Anda berisiko kehilangan dana ini"), menampilkan angka lokal ("bulan ini 126 warga DIY tertipu modus yang sama") agar relevan secara psikologis. Intervensi kecil berbasis nudge ini sering kali lebih efektif daripada seminar periodik, karena menyasar momen keputusan.

Implikasi kelembagaan dari keseluruhan rekomendasi adalah kebutuhan governance bersama yang sederhana namun mengikat. Di atas kertas, memorandum of understanding antar lembaga banyak dibuat; tantangannya adalah operationalization. Karena itu, selain SLA, diperlukan dewan kecil tata kelola kasus (city-level cybercrime steering group) yang bertemu rutin, memantau indikator proses–hasil, dan menetapkan tindakan perbaikan cepat ketika lag terlihat. Dewan ini melibatkan unsur Polresta, OJK daerah, perwakilan bank, danbila relevanperwakilan platform besar. Dengan forum ini,

penyebab keterlambatan tidak menjadi "rahasia antar lembaga," melainkan objek pembelajaran kolektif yang terdokumentasi.

Menyelaraskan semua itu dengan asas keadilan, kepastian, dan kemanfaatan yang dirumuskan Soerjono Soekanto mengantar pada simpulan normatif yang lebih tajam. Keadilan menuntut pemulihan korban sebagai raison d'être proses pidana; kepastian menuntut standar waktu dan kanal informasi yang predictable; kemanfaatan menuntut agar sistem benar-benar menurunkan prevalensi kejahatan dan biaya sosialnya. Jika tiga unsur itu berjalan serentak, barulah penegakan hukum keluar dari jebakan pelaku-sentris menuju victim-centred justice yang seutuhnya.

Adapun dari hasil observasi lapangan dan analisis dokumen kepolisian, dapat disusun data visualisasi kasus sebagai berikut:

***Tabel 1. Data Tindak Pidana Penipuan Online di Polresta Yogyakarta Tahun 2022–2023***

| Tahun | Jumlah Laporan | Kasus Diselesaikan | Persentase Penyelesaian (%) |
|---|---|---|---|
| 2022 | 178 | 102 | 57,3 |
| 2023 | 196 | 108 | 55,1 |

Sumber : Satreskrim Polresta Yogyakarta (Data Olahan Peneliti, 2024)

Data tersebut memperlihatkan bahwa meskipun jumlah laporan meningkat dari tahun 2022 ke 2023, tingkat penyelesaian kasus justru mengalami penurunan. Kondisi ini memperkuat temuan bahwa proses penanganan masih terkendala pada aspek koordinasi dan teknis penyidikan. Persentase penyelesaian kasus yang menurun dari tahun ke tahun dapat menjadi indikator awal melemahnya efektivitas sistem penegakan hukum dalam menghadapi kompleksitas kejahatan siber. Jika tren ini terus berlanjut, maka potensi kerugian masyarakat akan meningkat dan kepercayaan publik terhadap aparat penegak hukum dapat semakin menurun.

Selain itu, ditemukan pula fakta bahwa sebagian besar kasus yang dianggap selesai oleh kepolisian tidak selalu diikuti oleh pemulihan kerugian korban. Hal ini berarti bahwa tingkat penyelesaian kasus secara administratif belum tentu sejalan dengan keberhasilan dalam memberikan perlindungan hukum secara substantif. Restitusi jarang menjadi bagian yang diperjuangkan dalam proses penyidikan, dan sering kali korban hanya menerima informasi bahwa pelaku telah ditangkap tanpa adanya kepastian kapan dan bagaimana kerugian mereka dapat dipulihkan. Praktik ini bertentangan dengan prinsip Restorative Justice yang menempatkan pemulihan korban sebagai ukuran utama keberhasilan penegakan hukum.

Penelitian ini menemukan bahwa paradigma penegakan hukum yang bersifat pelaku-sentris harus direformasi menuju pendekatan yang lebih korban-sentris (victim-centered policing). Dalam pendekatan ini, hak korban menjadi fokus utama penyidikan, termasuk hak atas informasi, hak untuk berpartisipasi dalam proses penegakan hukum, hak atas pemulihan kerugian, serta hak atas perlindungan fisik dan psikologis. Dengan orientasi ini, penyidikan tidak hanya mengarah pada pemidanaan pelaku, melainkan pada pemulihan kepercayaan masyarakat terhadap hukum dan penyelenggaraannya.

Untuk itu, dibutuhkan model integratif berbasis waktu (time-bound) yang mampu memastikan kesigapan aparat dalam melakukan pembekuan dana dan pelacakan transaksi keuangan digital. Model ini menuntut adanya Service Level Agreement (SLA) yang jelas antara Polresta Yogyakarta, PPATK, OJK, dan perbankan agar setiap permintaan data dan tindakan pemblokiran rekening dapat dilakukan secara cepat dan terukur sesuai batas waktu yang disepakati. Dengan adanya SLA, maka tidak ada lagi alasan keterlambatan akibat prosedur administrasi internal yang merugikan korban.

Selain penguatan aspek koordinasi, implementasi sistem layanan korban terpadu sangat diperlukan di tingkat kepolisian. Sistem ini dapat berbentuk help desk khusus kejahatan siber yang dilengkapi case tracking system sehingga korban tidak perlu datang berulang kali ke kantor polisi hanya untuk mendapatkan perkembangan informasi kasus. Sistem layanan berbasis teknologi informasi ini juga dapat menjadi bentuk transparansi pelayanan publik yang pada akhirnya meningkatkan kepercayaan masyarakat.

Penguatan kapasitas penyidik menjadi strategi penting lain dalam model integratif ini. Pendidikan dan pelatihan khusus dalam bidang digital forensics, cyber intelligence, analisis transaksi keuangan, serta pengamanan data elektronik harus menjadi program yang berkelanjutan, bukan sekadar pelatihan insidental. Selain itu, pengadaan perangkat teknologi yang mendukung penyidikan harus menjadi prioritas agar tidak lagi bergantung pada dukungan Mabes Polri yang memakan waktu panjang. Modernisasi peralatan forensik digital menjadi salah satu faktor kunci percepatan proses penegakan hukum dalam kejahatan siber.

Tidak kalah pentingnya, faktor literasi digital masyarakat harus menjadi perhatian utama. Rendahnya pemahaman masyarakat terhadap modus penipuan online membuat korban sering terlambat menyadari bahwa mereka telah tertipu. Pemerintah daerah bersama kepolisian harus mengembangkan program edukasi masyarakat secara sistematis melalui sosialisasi berbasis komunitas, kampanye digital, dan kolaborasi dengan platform e-commerce maupun media sosial. Edukasi ini diharapkan dapat mendorong perubahan perilaku dan meningkatkan kewaspadaan masyarakat dalam melakukan transaksi digital.

Novelty yang dihasilkan dalam penelitian ini adalah rumusan model penanggulangan kejahatan penipuan online yang lebih berorientasi pada korban dan adaptif terhadap perkembangan teknologi. Model ini tidak hanya fokus pada penghukuman pelaku, tetapi juga memastikan bahwa korban mendapatkan kepastian hukum dan pemulihan kerugian yang cepat. Konsep kebijakan hukum adaptif ini memperkuat arah pembangunan sistem peradilan pidana Indonesia yang lebih responsif terhadap kejahatan di era digital dan selaras dengan prinsip keadilan restoratif sebagaimana diamanatkan dalam berbagai peraturan perundang-undangan nasional.

Dengan demikian, secara konseptual dan empiris, penelitian ini menegaskan bahwa masih terdapat kesenjangan signifikan antara norma hukum dan implementasinya dalam memberikan perlindungan hukum kepada korban tindak pidana penipuan online. Negara belum sepenuhnya hadir sebagai pelindung hak-hak korban di ruang digital, sehingga reformasi kebijakan penegakan hukum di bidang kejahatan siber merupakan keharusan mendesak yang tidak dapat ditunda. Apabila model penanggulangan baru yang bersifat integratif dan korban-sentris ini dapat diimplementasikan, maka efektivitas perlindungan hukum diharapkan akan meningkat secara nyata dan kepercayaan masyarakat terhadap aparat penegak hukum dapat dipulihkan.

## KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mengenai penanggulangan tindak pidana penipuan online oleh Satuan Reserse Kriminal (Satreskrim) Polresta Yogyakarta, dapat disimpulkan bahwa penanganan terhadap kejahatan siber tersebut hingga saat ini belum mampu memberikan perlindungan hukum yang optimal bagi korban. Penanganan perkara masih berfokus pada langkah represif dan membutuhkan waktu yang panjang, sementara koordinasi antara penyidik dengan lembaga eksternal seperti Otoritas Jasa Keuangan (OJK), perbankan, dan penyedia layanan digital masih terhambat oleh mekanisme administrasi serta regulasi yang belum sepenuhnya mendukung percepatan penyidikan. Hambatan tersebut berdampak pada lambatnya proses pelacakan transaksi digital dan pengamanan barang bukti elektronik yang sangat diperlukan untuk mengungkap pelaku kejahatan.

Situasi tersebut memperlihatkan bahwa korban penipuan online masih menghadapi ketidakpastian hukum, baik dalam memperoleh kejelasan mengenai perkembangan penyidikan maupun dalam proses pemulihan kerugian. Korban harus melakukan pelaporan berulang kali tanpa mendapatkan informasi yang cukup mengenai tahapan penyelesaian perkara, sehingga menimbulkan beban psikologis dan finansial tambahan. Kondisi ini menunjukkan bahwa pemenuhan hak-hak korban

dalam proses peradilan pidana belum terwujud secara maksimal, dan korban masih berisiko mengalami reviktimisasi akibat sistem yang belum sepenuhnya berpihak pada pemulihan korban.

Penelitian ini juga menunjukkan bahwa efektivitas penanggulangan penipuan online akan sangat bergantung pada penguatan harmonisasi antar lembaga dan peningkatan kapasitas aparat penegak hukum dalam bidang teknologi informasi. Diperlukan inovasi penanganan yang lebih terstruktur dan terukur melalui penerapan model penanggulangan yang berbasis waktu (time-bound) dan berorientasi pada korban (victim-centred). Model tersebut perlu mencakup prosedur tetap (SOP) yang mendukung percepatan pembekuan dana, akses cepat terhadap data keuangan yang relevan, serta koordinasi yang terintegrasi dengan lembaga terkait untuk mempercepat proses penyidikan dan pemulihan kerugian.

Selain itu, penyediaan unit layanan korban terpadu di tingkat kepolisian menjadi langkah strategis untuk menjamin akses korban terhadap informasi perkembangan perkara, pendampingan hukum maupun psikososial, serta mekanisme pelaporan yang mudah dan transparan. Peningkatan kemampuan digital forensics serta pemanfaatan teknologi pelacakan transaksi lintas platform juga harus menjadi prioritas untuk memperkuat efektivitas penegakan hukum dalam menghadapi modus kejahatan siber yang semakin kompleks.

Dengan demikian, penelitian ini menegaskan bahwa perlindungan hukum yang efektif bagi korban penipuan online hanya dapat diwujudkan melalui pendekatan sistemik yang mengintegrasikan aspek normatif, institusional, dan teknologis secara seimbang. Implementasi model kebijakan terpadu yang dihasilkan melalui penelitian ini diharapkan dapat mempercepat proses pengungkapan kasus, meningkatkan kepastian pemulihan bagi korban, serta memperkuat kepercayaan publik terhadap lembaga penegak hukum dalam menghadapi tantangan kejahatan siber di era digital.

**REFERENCES**

Ali, Z. (2021). *Metode penelitian hukum*. Sinar Grafika.

Arief, B. N. (2019). *Kebijakan kriminal dalam penanggulangan kejahatan siber di Indonesia*. Prenada Media.

Beccaria, C. (2020). *On crimes and punishments: Cybercrime edition*. Cambridge University Press.

Dermawan, H. (2021). Penegakan hukum tindak pidana penipuan berbasis elektronik. *Jurnal Hukum dan Pembangunan*, 51(3), 455–472. https://doi.org/10.21143/jhp.vol51.no3.2341

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITE.

Kakoe, S. (2020). Perlindungan hukum terhadap korban penipuan online. *Jurnal IUS*, 8(2), 189–200. https://doi.org/10.29303/ius.v8i2.640

Kementerian Kominfo RI. (2023). *Laporan penanganan aduan siber dan rekening penipuan online tahun 2023*. Kominfo Press.

Merton, R. K. (2021). *Social structure and anomie in the digital society*. Routledge.

Moleong, L. J. (2019). *Metodologi penelitian kualitatif*. PT Remaja Rosdakarya.

Otoritas Jasa Keuangan. (2024). *Laporan perlindungan konsumen sektor jasa keuangan*. OJK RI.

Satrio, P. S. (2023). Reformasi penegakan hukum siber berbasis kolaborasi kelembagaan. *Jurnal Penegakan Hukum Indonesia*, 5(1), 17–36. https://doi.org/10.52287/jphi.v5i1.782

Soekanto, S. (2020). *Efektivitas hukum dan perlindungan masyarakat*. Rajawali Pers.

Sutherland, E. H. (2022). *White-collar and cybercrime: Digital adaptation of differential association theory*. Wiley-Blackwell.

Wiratama, A. (2023). Respon kepolisian terhadap kejahatan siber berbasis media sosial. *Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2), 211–232.