

LETTER of ACCEPTANCE (LoA)

Nomor: 063/Wathan/LoA/VIII/2026

Tim penyunting WATHAN: Jurnal Ilmu Sosial dan Humaniora menerangkan bahwa:

ID Artikel/Judul : 647 / Problematika Kepolisian Resor Kota Banda Aceh
Dalam Penanganan Tindak Pidana Penipuan Berbasis
Elektronik
Penulis : Raja Aulia¹, Edi Yuhermansyah², Amrullah³, Badrun Munir⁴
Afiliasi : 1,2,3,4 Universitas Islam Negeri Ar-Raniry Banda Aceh, Aceh,
Indonesia
Email Koresponden : 220104018@student.ar-raniry.ac.id

Berdasarkan hasil review tim WATHAN: Jurnal Ilmu Sosial dan Humaniora status **diterima**, Jurnal akan publish di Volume 3 Nomor 3 Oktober Tahun 2026, dengan alamat web OJS: <https://jurnal.fanshurinstitute.org/index.php/wathan>

Untuk menghindari adanya duplikasi terbitan dan pelanggaran etika publikasi ilmiah terbitan berkala, kami berharap agar naskah/artikel tersebut tidak dikirimkan dan dipublikasikan ke penerbit/ jurnal lain.

Demikian surat ini kami sampaikan, atas partisipasi dan kerjasamanya, kami ucapkan terimakasih.

Meulaboh, 29 Agustus 2026
Chief Editor


Sumardi Efendi. S.H.I., M.Ag
Scopus ID: 60006218300



*Konfirmasi Keaslian LoA WA 0852-6008-3890 (Sumardi Efendi)

ALAMAT REDAKSI

Jl. Daud Dariah Gampong Paya Peunaga Perumahan Cinta Kasih
Kecamatan Meureubo Kabupaten Aceh Barat - Indonesia
HP/WA. 0852-6008-3890



PROBLEMATIKA KEPOLISIAN RESOR KOTA BANDA ACEH DALAM PENANGANAN TINDAK PIDANA PENIPUAN BERBASIS ELEKTRONIK

Raja Aulia¹, Edi Yuhermansyah², Amrullah³, Badrun Munir⁴

¹Universitas Islam Negeri Ar-Raniry, Aceh, Indonesia

²Universitas Islam Negeri Ar-Raniry, Aceh, Indonesia

³Universitas Islam Negeri Ar-Raniry, Aceh, Indonesia

⁴Universitas Islam Negeri Ar-Raniry, Aceh, Indonesia

Email Koresponden: 220104018@student.ar-raniry.ac.id

No WhatsApp (WA): 081265033108

ABSTRACT

The development of Indonesia's digital economy has significantly increased electronic transactions while simultaneously escalating online fraud crimes. In the jurisdiction of Banda Aceh City Police (Polresta Banda Aceh), this phenomenon is reflected in the high number of public reports that are not followed by case completion, in which none of the perpetrators were arrested. In law enforcement practice, police investigators tend to apply Article 492 of the Indonesian Criminal Code (KUHP) concerning conventional fraud rather than specific provisions under the Electronic Information and Transactions Law (ITE Law). This study examines how the handling of online fraud cases by Polresta Banda Aceh contributes to case stagnation and analyzes the role of the Financial Services Authority (OJK) in this context. This research employs an empirical juridical method using statutory and sociolegal approaches, with qualitative analysis of normative and empirical data obtained through literature review and interviews with police officers. The findings reveal that the stagnation of online fraud cases is primarily caused by limited investigative authority at the district police level, layered bureaucratic procedures, and dependency on financial data access beyond police control. Meanwhile, OJK conducts independent investigations related to financial sector violations based on Article 49 paragraph (5) of the Law on Financial Sector Development and Strengthening (P2SK Law), without intervening in criminal investigations conducted by the police. This study concludes that the absence of case resolution indicates weak institutional integration, emphasizing the need for strengthened functional coordination between the police and OJK to enhance the effectiveness of cybercrime law enforcement.

Keyword: Online Fraud; Law Enforcement; KUHP; ITE



Creative Commons Attribution-ShareAlike 4.0
International License.

Published by Fanshur Institute: Research and Knowledge Sharing in Aceh

ABSTRAK

Perkembangan ekonomi digital di Indonesia telah mendorong peningkatan signifikan transaksi elektronik, namun secara simultan memicu eskalasi tindak pidana penipuan berbasis elektronik. Di wilayah hukum Polresta Banda Aceh, fenomena ini ditandai oleh tingginya jumlah laporan masyarakat yang tidak berbanding lurus dengan penyelesaian perkara, di mana tidak ada pelaku yang sampai pada tahap penangkapan. Dalam praktik penegakan hukum, aparat kepolisian cenderung menerapkan Pasal 492 Kitab Undang-Undang Hukum Pidana (KUHP) tentang penipuan konvensional, dibandingkan menggunakan ketentuan khusus dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Permasalahan yang dikaji dalam penelitian ini adalah bagaimana pola penanganan perkara penipuan berbasis elektronik oleh Polresta Banda Aceh sehingga perkara cenderung stagnan, serta bagaimana peran Otoritas Jasa Keuangan (OJK) dalam konteks tersebut. Penelitian ini menggunakan metode yuridis empiris dengan pendekatan perundang-undangan dan pendekatan sosiologis hukum. Analisis dilakukan secara kualitatif terhadap data normatif dan data empiris yang diperoleh melalui studi kepustakaan dan wawancara dengan aparat kepolisian. Hasil penelitian menunjukkan bahwa penanganan perkara oleh Polresta Banda Aceh menghadapi hambatan serius berupa keterbatasan kewenangan penyidikan, prosedur birokratis yang berlapis, serta ketergantungan pada akses data keuangan yang tidak sepenuhnya berada dalam kontrol kepolisian. Di sisi lain, Otoritas Jasa Keuangan menjalankan peran penyelidikan mandiri terhadap dugaan pelanggaran di sektor jasa keuangan berdasarkan Undang-Undang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) Pasal 49 ayat (5), tanpa bersifat mengintervensi proses penyidikan pidana. Kesimpulan penelitian ini menegaskan bahwa belum selesainya perkara penipuan berbasis elektronik mencerminkan lemahnya integrasi kelembagaan, sehingga diperlukan penguatan koordinasi fungsional antara kepolisian dan Otoritas Jasa Keuangan untuk meningkatkan efektivitas penegakan hukum pidana cyber.

Kata kunci: Penipuan Berbasis Elektronik; Penegakan Hukum; KUHP; ITE

Pendahuluan

Perkembangan teknologi informasi pada abad ke-21 telah mendorong transformasi signifikan dalam struktur sosial, ekonomi, dan hukum. Digitalisasi yang awalnya diharapkan menjadi instrumen peningkatan kesejahteraan justru memunculkan bentuk kejahatan baru, khususnya penipuan berbasis elektronik. Ruang cyber kini tidak lagi bersifat sekunder, melainkan menjadi bagian integral dari aktivitas sosial yang memiliki implikasi hukum nyata. Oleh karena itu, kejahatan di ranah digital menuntut pendekatan regulasi dan penegakan hukum yang adaptif dan terintegrasi.

Di Indonesia, pertumbuhan ekonomi digital yang pesat melalui e-commerce, fintech, dan layanan keuangan digital telah menggeser pola transaksi dari konvensional ke elektronik. Perubahan ini turut memunculkan kerentanan baru, seperti penipuan online melalui skema pembayaran digital dan investasi fiktif.

Kejahatan ini memanfaatkan anonimitas, asimetri informasi, serta kelemahan koordinasi antar-lembaga, sehingga berkembang menjadi kejahatan yang kompleks dan sering kali lintas yurisdiksi (Hanif, A. 2024).

Dalam konteks hukum pidana Islam, penipuan memang belum dibahas secara eksplisit melainkan masih digeneralisasikan atau diqiyaskan sama dengan mengambil barang atau hak yang bukan miliknya, berlandaskan Al-Qur'an surat Al-Baqarah ayat 188 yang artinya:

“Dan janganlah sebagian kamu memakan harta sebagian yang lain di antara kamu dengan jalan yang batil. Dan (janganlah) kamu membawa (urusan) harta itu kepada hakim, supaya kamu dapat memakan sebagian dari harta benda orang lain itu dengan (jalan berbuat) dosa, padahal kamu mengetahui” (QS. al-Baqarah: 188).

Tegas dijelaskan bahwa harta memiliki peran krusial dalam kehidupan manusia. Harta dan Agama adalah hak Allah SWT dan tidak diperkenankan manusia mengelolanya melainkan atas seizin-Nya, oleh karena itu Allah SWT menegaskan kedudukan harta secara tegas untuk diperoleh ataupun digunakan dengan sebaik-baiknya.

Aceh sebagai daerah otonomi khusus yang menerapkan Syariat Islam berlandaskan Al-Qur'an dan Hadist melalui Qanun Jinayah Nomor 6 Tahun 2024 tentang Hukum Jinayat, Aceh dituntut memiliki kerangka penegakan hukum yang responsif. Namun, Qanun Jinayat saat ini masih terbatas pada jarimah tradisional dan belum memuat kodifikasi khusus mengenai jarimah *cyber* (*Al-khad'ah Al-iliktruniyyah*).

Oleh karena itu, kerangka Fiqh Jinayah dan Maqashid Syariah khususnya prinsip *Hifz al-Mal* (penjagaan harta) diperlukan sebagai fondasi normatif dan filosofis. Hal ini menegaskan bahwa penanganan kejahatan digital membutuhkan kebijakan hukum yang berorientasi pada pencegahan kemudharatan dan pemulihan hak korban, bukan sekadar pemenuhan aspek formalitas pemidanaan atau pemblokiran administratif yang pasif.

Fenomena kejahatan *cyber* berupa pencurian atau penipuan dalam ranah elektronik dapat dipahami sebagai pelanggaran terhadap prinsip amanah serta bentuk *zulm* karena menimbulkan kerugian bagi korban dan masyarakat. Perbuatan tersebut secara umum termasuk jarimah *ta'zīr*, yaitu tindak pidana yang jenis dan kadar hukumannya tidak ditetapkan secara rinci dalam Nas, sehingga penentuannya berada pada kewenangan hakim atau ulil amri. Sanksi yang diberikan dapat berupa denda sesuai tingkat kerugian, hukuman penjara, atau pengasingan sementara dengan mempertimbangkan dampak dan tingkat kesalahan pelaku. Selain berfungsi sebagai tindakan pencegahan dan pemberian efek jera, pendekatan ini juga menekankan rehabilitasi moral serta pemulihan integritas pelaku agar dapat kembali berperan secara baik dalam masyarakat.

Mengenai sanksi *ta'zīr*, para ulama memiliki perbedaan pendapat mengenai batas maksimal dan minimal hukuman. Imam Abu Yusuf berpendapat bahwa

hukuman *ta'zīr* tidak boleh melebihi tiga puluh sembilan kali, sedangkan batas minimumnya harus ditentukan berdasarkan kebutuhan untuk memberikan efek jera dan mencegah terulangnya tindak pidana. Ulama Syafi'iyah berpendapat bahwa batas maksimal hukuman tersebut tidak boleh melebihi sepuluh kali. Sementara itu, Imam Malik membolehkan hukuman *ta'zīr* melampaui satu kali hukuman *had* apabila tindakan tersebut dipandang memiliki kemaslahatan dan relevan dengan tingkat kejahatan yang dilakukan (Fernando, Y., 2022).

Dalam ranah pembuktian, perkara pidana cyber memiliki karakteristik yang lebih kompleks dibandingkan tindak pidana konvensional. Perbuatan pidana dapat dilakukan tanpa kehadiran fisik pelaku di tempat kejadian, menggunakan identitas atau akun palsu, serta melibatkan server, perangkat, dan jaringan yang berada di wilayah berbeda. Selain itu, bukti digital bersifat mudah diubah, dihapus, disalin, atau dipindahkan, sehingga keaslian dan integritasnya harus diuji secara cermat. Dalam konteks Aceh, Qanun Aceh Nomor 7 Tahun 2013 tentang Hukum Acara Jinayat telah mengakui bukti elektronik sebagai salah satu alat bukti. Bukti tersebut mencakup informasi mengenai terjadinya jarimah dan pihak yang melakukannya yang dihasilkan melalui perangkat elektronik atau optik serta dapat dibaca, dilihat, atau didengar. Pengakuan ini menunjukkan bahwa hukum acara jinayat memiliki ruang untuk merespons perkembangan teknologi, tetapi penerapannya tetap memerlukan pemeriksaan terhadap sumber, cara memperoleh, keutuhan, dan keterkaitan bukti dengan perbuatan pidana. Kesulitan pembuktian tersebut harus dikaitkan dengan prinsip kehati-hatian dalam fiqh jinayah. Salah satu kaidah yang sering dijadikan dasar sebagai mana di jadikan dalam jurnal (Bego, K. C., et al., 2025) ialah:

ادْرَأُوا الْحُدُودَ بِالشُّبُهَاتِ

Idra'ū al-hudūd bi al-syubuhāt

"Hindarkanlah hukuman had karena adanya syubhat atau keraguan."

Kaidah tersebut menegaskan bahwa hukuman yang berat tidak boleh dijatuhkan apabila masih terdapat keraguan yang substansial mengenai peristiwa pidana, identitas pelaku, unsur kesengajaan, atau keabsahan alat bukti. Prinsip ini sejalan dengan gagasan bahwa kesalahan pidana harus dibuktikan secara meyakinkan, sedangkan keraguan yang beralasan harus dipertimbangkan untuk melindungi seseorang dari penghukuman yang keliru.

Namun, kaidah tersebut perlu diterapkan secara tepat. Dalam perkara *cyber* yang dikategorikan sebagai jarimah *ta'zīr*, tidak semua keraguan otomatis menghapus seluruh kemungkinan penegakan hukum (Putra & Lubis, 2024). Keraguan yang tidak terpenuhi untuk menjatuhkan sanksi berat tetap harus mendorong hakim untuk menilai kembali konstruksi perkara, memilih sanksi yang proporsional, atau mengutamakan pemulihan korban. Dengan kata lain, prinsip *dar'ū al-hudūd bi al-syubuhāt* terutama berfungsi sebagai jaminan agar hukuman tidak dijatuhkan berdasarkan bukti yang lemah, ambigu, atau tidak autentik

(Putra, R., & Lubis, S. D., 2024). Oleh karena itu, pembuktian kejahatan cyber harus memperhatikan beberapa aspek utama:

- Keaslian, yaitu memastikan bahwa data benar-benar berasal dari sumber yang diklaim.
- Integritas, yaitu memastikan bahwa bukti tidak mengalami perubahan sejak diperoleh.
- Keterkaitan, yaitu menunjukkan hubungan antara bukti digital, peristiwa pidana, korban, dan terdakwa.
- Legalitas perolehan, yaitu memastikan bukti dikumpulkan melalui prosedur yang sah dan tidak melanggar hak privasi.
- Kecukupan pembuktian, yaitu memastikan bukti digital didukung oleh keterangan saksi, ahli, dokumen, jejak transaksi, atau alat bukti lainnya.

Bagi lembaga peradilan yang berwenang, prinsip ini menuntut adanya keseimbangan antara perlindungan masyarakat dan perlindungan terhadap terdakwa (Kholiq et al., 2025). Hakim tidak boleh hanya mendasarkan putusan pada dugaan, alamat IP, kepemilikan perangkat, atau keberadaan akun tertentu tanpa bukti tambahan yang menghubungkan terdakwa dengan perbuatan pidana. Kepemilikan perangkat atau akun, misalnya, tidak selalu membuktikan bahwa orang tersebut adalah pihak yang melakukan penipuan atau pencurian data. Apabila bukti elektronik terbukti autentik dan saling bersesuaian dengan alat bukti lain, hakim dapat menyimpulkan adanya perbuatan pidana secara lebih kuat. Sebaliknya, apabila terdapat keraguan mengenai manipulasi data, akses pihak ketiga, rantai penguasaan bukti, atau identitas pelaku, keraguan tersebut harus ditafsirkan secara jelas dan tidak boleh digunakan untuk menjatuhkan hukuman secara sewenang-wenang, atau hanya berdasarkan perasaan semata (Kholiq, A., 2025).

Dalam kerangka hukum konvensional, penipuan diatur dalam Pasal 492 KUHP dan diperkuat melalui ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Namun, dalam praktiknya, aparat penegak hukum cenderung menggunakan Pasal 492 KUHP karena dianggap lebih sederhana dalam pembuktian. Hal ini menunjukkan adanya ketidakharmonisan antara perkembangan modus kejahatan dengan instrumen hukum yang digunakan. UU ITE sebagai *lex specialis* belum dimanfaatkan secara optimal karena kendala teknis, seperti kebutuhan keahlian forensik digital, keterbatasan alat bukti elektronik, serta kompleksitas pembuktian unsur “penyebaran informasi” (Syahril & Aris, 2021).

Selain persoalan normatif, keterbatasan kapasitas teknis penyidik di tingkat Polresta turut menjadi faktor penentu. Penerapan UU ITE menuntut penguasaan forensik digital, pengamanan alat bukti elektronik, serta koordinasi dengan unit cyber di tingkat Polda. Tidak semua kepolisian resort memiliki sumber daya manusia dan sarana yang memadai untuk memenuhi standar pembuktian

elektronik tersebut, sehingga penggunaan KUHP dipandang lebih efisien dan realistis dalam kerangka penyelesaian perkara (Masdi et al., 2022).

Persoalan akses terhadap data elektronik dan data keuangan pelaku juga menjadi hambatan. Dalam banyak kasus, penyidik membutuhkan data transaksi dari lembaga perbankan dan penyelenggara sistem elektronik, namun akses tersebut sering terkendala oleh rezim perlindungan data pribadi. Ketidakjelasan batas kewenangan antara kepentingan penyidikan pidana dan kewajiban perlindungan data pribadi menyebabkan aparat penegak hukum bersikap sangat berhati-hati, sehingga memperlambat proses penegakan hukum apabila menggunakan UU ITE sebagai dasar hukum utama (Mouzakiti, E., 2020).

Informasi elektronik, dokumen elektronik, dan hasil cetaknya diakui sebagai alat bukti hukum yang sah. Meskipun demikian, pengakuan formal tersebut tidak berarti bahwa setiap tangkapan layar, pesan, atau rekaman digital otomatis memiliki kekuatan pembuktian yang sempurna. Nilai pembuktiannya tetap bergantung pada autentikasi, kesinambungan penguasaan barang bukti (chain of custody), dan penilaian hakim.

Data empiris Kepolisian Resor Kota Banda Aceh menunjukkan adanya fluktuasi jumlah kasus penipuan online selama periode 2022–2025, dengan total 36 kasus, yang sebagian besarnya tidak dapat diproses lebih lanjut ke dalam tahapan penyidikan atau tahap penetapan tersangka. Kondisi ini mengindikasikan adanya hambatan dalam proses penegakan hukum, khususnya pada tahap penyelidikan.

NO	TAHUN	NAMA KASUS	JUMLAH KASUS	KET
1	2022	TP. Penipuan Online	8	-
2	2023	TP. Penipuan Online	12	-
3	2024	TP. Penipuan Online	7	-
4	2025	TP. Penipuan Online	9	-
		JUMLAH	36	

Selain itu, aparat masih memiliki keterbatasan dalam menangani bukti digital, termasuk pelacakan transaksi keuangan dan identifikasi pelaku yang menggunakan identitas anonim. Akses terhadap data perbankan dan data elektronik sering terkendala oleh undang-undang perlindungan data pribadi, sehingga memperlambat proses penyelidikan. Dalam konteks ini, koordinasi antara kepolisian dengan lembaga lain, yakni Otoritas Jasa Keuangan (OJK) dan penyelenggara sistem elektronik, menjadi krusial.

Namun demikian, koordinasi antar lembaga tersebut belum berjalan optimal. Otoritas Jasa Keuangan memiliki kewenangan dalam sektor jasa keuangan,

termasuk akses terhadap data transaksi, tetapi perannya lebih bersifat administratif dan tidak secara langsung mengintervensi proses penyidikan pidana. Di sisi lain, kepolisian sebagai penyidik utama menghadapi keterbatasan akses terhadap data tersebut. Kondisi ini menciptakan celah koordinasi yang berdampak pada lambatnya penyelesaian perkara (Khusnaeni, I., 2023).

Fenomena stagnasi perkara di mana banyak laporan tidak berlanjut ke tahap penetapan tersangka menunjukkan adanya persoalan dalam struktur, substansi, dan kultur hukum. Struktur birokrasi yang kompleks, substansi hukum yang belum sepenuhnya adaptif, serta kultur aparat yang masih berorientasi pada kejahatan konvensional menjadi faktor yang saling berkaitan. Akibatnya, pendekatan penegakan hukum cenderung reaktif dan belum mampu mengantisipasi karakteristik kejahatan cyber yang dinamis (Duarif & Saleh, M., 2023).

Selain itu, perlindungan hukum terhadap korban masih belum optimal. Korban penipuan online sering kesulitan memperoleh ganti rugi karena keterbatasan pengaturan normatif dan sulitnya pembuktian. Hal ini menunjukkan adanya kebutuhan untuk memperkuat regulasi yang tidak hanya berorientasi pada pemidanaan pelaku, tetapi juga pada pemulihan kerugian korban.

Dari perspektif teori sistem hukum, permasalahan ini mencerminkan ketidakseimbangan antara struktur, substansi, dan kultur hukum. Struktur penegakan hukum yang birokratis, substansi hukum yang multitafsir, serta kultur aparat yang masih berorientasi pada kejahatan konvensional membentuk kombinasi yang kurang adaptif terhadap karakteristik kejahatan *cyber*. Akibatnya, pendekatan hukum pidana yang digunakan cenderung reaktif dan kasuistik, bukan sistemik dan preventif.

Meskipun penggunaan Pasal 492 KUHP dapat memberikan kepastian hukum jangka pendek, pendekatan ini menyisakan persoalan konseptual dalam jangka panjang (Pangemanan, Suoth, & Ante, 2026). Kejahatan penipuan berbasis elektronik memiliki karakteristik khusus, seperti penggunaan identitas anonim, lintas yurisdiksi, dan pemanfaatan teknologi informasi secara intensif, yang tidak sepenuhnya dapat dijangkau oleh hukum pidana konvensional. Oleh karena itu, dominasi penggunaan KUHP justru berpotensi menghambat pengembangan kapasitas penegakan hukum *cyber* secara struktural (Sariani, 2023).

Penelitian mengenai penipuan daring telah dilakukan secara ekstensif oleh Kurnia et al. (2022) melalui riset monograf nasional yang memetakan spektrum modus operandi, medium komunikasi, dan dampak finansial penipuan digital di Indonesia. Fokus utama penelitian tersebut adalah pada identifikasi medium seperti WhatsApp dan Instagram sebagai kanal utama yang digunakan pelaku untuk melakukan rekayasa sosial terhadap 1.700 responden di 34 provinsi. Sejalan dengan itu, Sutarli dan Kurniawan (2023) menitikberatkan kajiannya pada peran preventif pemerintah melalui implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP) sebagai instrumen untuk menekan angka kejahatan phishing. Kedua penelitian ini memberikan landasan teoritis yang kuat mengenai

karakteristik makro kejahatan *cyber* di Indonesia, namun cenderung bersifat generalis dan belum menyentuh dinamika penegakan hukum di tingkat satuan kerja kewilayahan secara spesifik.

Kajian lain oleh Kesuma et al. (2020) dan Rahmanto (2019) mengevaluasi aspek normatif yuridis dalam penegakan hukum *cyber* dengan menonjolkan kendala teknis penyidikan seperti anonimitas pelaku dan keterbatasan alat forensik digital. Rahmanto secara khusus menyoroti ketidaksiapan perangkat hukum dalam menghadapi kecepatan evolusi modus operandi penipuan berbasis transaksi elektronik yang bersifat lintas yurisdiksi. Sementara itu, penelitian Satriani (2019) memberikan dimensi tambahan dengan meninjau tindak pidana penipuan elektronik melalui perspektif hukum pidana Islam di lingkungan Pengadilan Negeri Makassar. Meskipun kajian-kajian ini telah mengeksplorasi hambatan hukum dan sanksi, terdapat kekosongan analisis terkait hambatan birokrasi komunikasi antar-lembaga pusat dan daerah yang menjadi faktor determinan dalam stagnasi kasus di lapangan.

Pembeda utama penelitian ini dengan penelitian-penelitian terdahulu terletak pada lokus penelitian dan kedalaman data empiris terkait mekanisme koordinasi antar instansi di Kota Banda Aceh. Jika penelitian sebelumnya lebih banyak berfokus pada modus operandi nasional atau tinjauan normatif UU ITE, penelitian ini secara spesifik membedah hambatan birokrasi dalam proses penyidikan di Polresta Banda Aceh, khususnya terkait efektivitas surat korespondensi kepada Kementerian Komunikasi dan Digital serta Otoritas Jasa Keuangan. Penelitian ini menggunakan data mengenai surat-surat penyidikan yang tidak terbalas pada tahun 2023 dan 2025 sebagai bukti bahwa lemahnya sistem penegakan hukum *cyber* dan bersifat ketergantungan dalam wilayah hukum Polresta Banda Aceh.

Penelitian ini membedah bagaimana penguatan mekanisme penyelesaian tindak pidana elektronik dalam wilayah Kepolisian Resor Banda Aceh yang memiliki karakteristik sosial hukum yang unik, karena selain bertumpu pada hukum konvensional, Kepolisian Resor Banda Aceh juga memiliki Qanun Jinayah sebagai landasan dalam pencegahan tindak pidana. Penelitian ini juga menunjukkan bagaimana ketergantungan pada pasal penipuan konvensional di tingkat kepolisian berkontribusi terhadap stagnasi penyelesaian perkara. Selain itu, penelitian ini juga memberikan gambaran konseptual untuk membedakan peran Otoritas Jasa Keuangan sebagai subjek penyelidikan administratif yang berjalan paralel dengan penyidikan pidana, sehingga menolak asumsi umum bahwa Otoritas Jasa Keuangan memiliki fungsi intervensi langsung dalam proses penegakan hukum pidana penipuan berbasis elektronik.

Dengan demikian, permasalahan penipuan berbasis elektronik di Banda Aceh tidak hanya berkaitan dengan aspek normatif, tetapi juga dengan efektivitas koordinasi kelembagaan dan kapasitas teknis penegakan hukum. Oleh karena itu, diperlukan model penegakan hukum yang lebih integratif melalui penguatan koordinasi antara kepolisian, Otoritas Jasa Keuangan, dan instansi terkait,

peningkatan kapasitas forensik digital, serta harmonisasi antara KUHP dan UU ITE.

Metode Penelitian

Penelitian ini menggunakan metode normatif empiris yang mengkaji hukum tidak hanya sebagai norma tertulis tetapi juga sebagai praktik yang berlangsung dalam masyarakat. Pendekatan ini dipilih karena permasalahan utama penelitian terletak pada kesenjangan antara ketentuan normatif mengenai tindak pidana penipuan elektronik dengan implementasinya dalam praktik penegakan hukum di Polresta Banda Aceh. Dengan demikian, analisis tidak hanya difokuskan pada konstruksi peraturan perundang-undangan, tetapi juga pada faktor-faktor empiris yang mempengaruhi efektivitas penegakan hukum (Muhaimin, 2020).

Penelitian ini menggabungkan dua pendekatan utama. Pertama, pendekatan perundang-undangan yang digunakan untuk menelaah ketentuan hukum positif yang relevan, khususnya Pasal 492 Kitab Undang-Undang Hukum Pidana (KUHP), ketentuan dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), serta regulasi terkait sektor jasa keuangan. Kedua, pendekatan sosiologis hukum yang bertujuan untuk mengkaji praktik penyidikan, hambatan operasional, serta dinamika koordinasi antar lembaga dalam penanganan tindak pidana penipuan berbasis elektronik.

Pemilihan metode yuridis empiris dalam penelitian ini didasarkan pada pandangan bahwa efektivitas hukum tidak hanya ditentukan oleh kualitas norma, tetapi juga oleh faktor-faktor sosial yang mempengaruhi implementasinya, seperti kapasitas aparat, sarana prasarana, dan budaya hukum masyarakat. Oleh karena itu, pendekatan ini dinilai tepat untuk mengidentifikasi secara komprehensif penyebab stagnasi penanganan perkara penipuan elektronik serta merumuskan solusi yang lebih aplikatif dalam konteks penegakan hukum di tingkat daerah.

Pembahasan/Hasil

A. Mekanisme Penanganan Penipuan Berbasis Elektronik Dalam Polresta Banda Aceh

Ketergantungan terhadap sarana elektronik telah menjadi bagian dari kebiasaan sehari-hari. Perkembangan ini di satu sisi memperluas inklusi keuangan, namun di sisi lain menciptakan kerentanan baru terhadap kejahatan, khususnya penipuan berbasis elektronik, yang memanfaatkan kecepatan dan anonimitas sistem elektronik (Masdi et al., 2022). Namun, tingginya penetrasi internet sering kali tidak dibarengi dengan literasi digital yang memadai, sehingga masyarakat rentan terhadap ancaman peretasan dan pencurian identitas (Putri et al., 2025, hlm. 38). Fenomena penipuan berbasis elektronik kini tidak hanya menyerang secara teknis, tetapi juga melalui manipulasi psikologis yang rumit (Samudra, 2017).

Penegakan hukum terkait tindak pidana penipuan berbasis elektronik di wilayah hukum Kepolisian Kota Banda Aceh saat ini berada pada titik kritis yang

menuntut perubahan paradigma dari model penyidikan linier menjadi model yang terintegrasi. Secara prosedural, penyelidikan telah dilakukan sesuai dengan hukum acara pidana, mulai dari penerimaan laporan hingga pengumpulan bukti awal berupa data rekening bank dan komunikasi digital. Namun, tahap ini sebagian besar masih bersifat administratif dan belum sepenuhnya strategis dalam menetapkan arah penyelidikan yang efektif.

Dalam Hukum Acara Pidana, kewenangan penyelidikan dan penyidikan berada pada Kepolisian berdasarkan Pasal 6 dan 7 KUHP, diperluas oleh ketentuan khusus UU ITE mengenai alat bukti elektronik dan tata cara penggeledahan/pemeriksaan sistem elektronik (Wulandari, S., 2021). Mekanisme penyidikan penipuan dengan media transaksi elektronik menempatkan Polri sebagai leading sector yang wajib mengintegrasikan alat bukti klasik (saksi, surat, petunjuk) dengan informasi dan/atau dokumen elektronik sebagai alat bukti sah.

Penelitian di Polda Sulawesi Selatan juga menunjukkan bahwa dalam praktik, Subdit *Cyber*/Ditreskrimsus mengandalkan Pasal 492 KUHP untuk pemidanaan, sementara Pasal 28 ayat (1) UU ITE lebih diposisikan untuk kasus penyebaran berita bohong yang secara eksplisit menyesatkan publik dan menyebabkan kerugian (Palembangan et al., 2023). Dalam kasus-kasus penipuan jual beli online, pertanggungjawaban pidana diatur dalam Pasal 492 KUHP dan Pasal 28 ayat (1) UU ITE dengan ancaman pidana penjara hingga 6 tahun dan denda hingga 1 miliar rupiah. Namun, di lapangan, proses penyidikan sering melunak menjadi serangkaian langkah administratif: pemblokiran rekening, pemutusan akses, tanpa selalu berujung penuntutan.

Penelitian lain mengenai penyelesaian penipuan melalui pembayaran elektronik di Barelang, Batam, juga menunjukkan bahwa kepolisian mengedepankan upaya preventif dan represif administratif, yakni sosialisasi berkala di pusat transaksi dan pengawasan penyedia metode pembayaran, sementara jalur pidana berjalan selektif dan menghadapi kendala pembuktian (Pasaribu et al., 2025). Di banyak kasus e-commerce maupun penipuan berbasis elektronik, pemerintah dan aparat mengedepankan edukasi, literasi digital, dan pemblokiran sebagai strategi utama, sementara pemidanaan pelaku hanya terjadi pada sebagian kecil kasus yang bukti dan pelakunya jelas. Platform dapat memulihkan citra reputasi, tetapi struktur kejahatan dan pelaku utama tetap dapat bermigrasi ke platform atau skema lain, sementara korban lama tidak memperoleh kompensasi.

Kewenangan penyelidikan secara formal berada penuh pada Polri, tetapi secara fungsional bergantung pada sinergi dengan lembaga lainnya seperti Otoritas Jasa Keuangan. Riset mengenai penipuan berbasis elektronik menegaskan bahwa Otoritas Jasa Keuangan dan kepolisian memiliki tiga kendala besar dalam penanganannya: locus delicti yang tidak jelas, aplikasi yang dapat kembali dioperasikan meski dibekukan, dan ketiadaan dasar hukum yang benar-benar efektif menjerat fintech ilegal sehingga mereka terus beroperasi.

Secara konseptual, hal ini menegaskan bahwa kewenangan penyelidikan penipuan online bukan hanya soal “siapa berwenang”, tetapi juga “siapa mampu”. Polres tetap menjadi pemegang kewenangan yuridis utama, tetapi tanpa dukungan teknis dan regulatif dari pusat, kewenangan itu berubah menjadi kewenangan yang “lemah secara operasional”.

Kegagalan koordinasi dan keterbatasan teknis berdampak langsung pada upaya pelacakan digital, di mana penyidik berusaha melacak alamat IP dan nomor telepon melalui ISP. Pada kenyataannya, Kepolisian Kota Banda Aceh menghadapi tantangan serius akibat keterbatasan alat forensik digital dan personel TI, sehingga analisis digital sering memakan waktu lama atau harus bergantung pada unit tingkat atas. Situasi ini mencerminkan kesenjangan antara tuntutan kejahatan digital yang kompleks dan kesiapan teknis lembaga penegak hukum lokal. Infrastruktur forensik yang lemah ini bukan sekadar masalah teknis, melainkan konsekuensi dari rendahnya prioritas kebijakan nasional dalam memperkuat kapasitas penegakan hukum *cyber* di wilayah-wilayah yang jauh dari pusat teknologi.

Selain itu, dalam konteks pengelolaan bukti digital seperti ponsel dan komputer, kurangnya perangkat canggih untuk memaksimalkan ekstraksi data juga menjadi hambatan dalam mengoptimalkan penyajian bukti. Hal ini menimbulkan dilema koordinasi antar lembaga; meskipun Kepolisian Kota telah menjalin kerja sama dengan Otoritas Jasa Keuangan (OJK) dan sektor perbankan, akses terhadap data terperinci sering terhambat oleh peraturan kerahasiaan perbankan dan undang-undang perlindungan data pribadi. Sebagaimana dinyatakan oleh Aiptu Henrikus, penyidik seringkali hanya memperoleh akses ke informasi pemblokiran, bukan identitas terperinci pelaku. Situasi ini menyoroti konflik regulasi yang belum terselesaikan antara kepentingan privasi warga dan kebutuhan mendesak penegakan hukum pidana untuk mengungkap kebenaran materiil.

Keterbatasan ini semakin diperparah oleh kurangnya dukungan substantif dari lembaga pusat, seperti Kementerian Komunikasi dan Digital (Komdigi). Meskipun Polresta Banda Aceh telah mengajukan permohonan resmi sebanyak dua kali (2023 dan 2025) untuk bantuan teknis pelacakan jejak digital, respons yang diterima justru mengindikasikan bahwa lembaga pusat sendiri belum memiliki kemampuan teknis yang memadai untuk membantu secara maksimal. Fenomena ini memperkuat argumen bahwa persoalan utama penanganan penipuan berbasis elektronik bukan semata pada kinerja individu penyidik di Banda Aceh, melainkan pada desain kebijakan nasional dan koordinasi kelembagaan pusat-daerah yang tidak sinkron, yang secara langsung melumpuhkan efektivitas penyelidikan di tingkat lokal.

Redefinisi terhadap karakteristik pelaku juga menjadi tantangan besar, di mana penggunaan identitas palsu dan rekening penampung membuat model penegakan hukum konvensional yang berorientasi pada individu menjadi tidak memadai. Pelaku yang beroperasi lintas wilayah dan negara menuntut adanya

model sebagaimana diamanatkan Pasal 7 KUHP, di mana jalur pidana Polri dan jalur administratif Otoritas Jasa Keuangan berjalan simultan. Namun, karena unit *cyber* khusus di Polresta belum optimal akibat keterbatasan anggaran dan SDM, perkara penipuan berbasis elektronik sering kali kalah prioritas dibandingkan perkara pidana konvensional lainnya. Hal ini menunjukkan bahwa kejahatan *cyber* belum sepenuhnya diposisikan sebagai ancaman strategis dalam kebijakan kriminal di daerah.

Sebagai konsekuensi dari berbagai keterbatasan tersebut, penyidik di Polresta Banda Aceh secara sadar memilih Pasal 492 KUHP tentang Penipuan sebagai dasar hukum utama, alih-alih menggunakan UU ITE. Pilihan ini didasarkan pada pertimbangan praktis bahwa unsur penipuan konvensional seperti tipu muslihat dan kerugian materiil lebih mudah dibuktikan di lapangan daripada aspek teknis sistem elektronik. Penggunaan KUHP dinilai lebih realistis karena memfokuskan penyidikan pada perbuatan materiil pelaku dan kerugian korban, sehingga konstruksi hukumnya lebih cepat dipahami dan diterima oleh Jaksa Penuntut Umum maupun Hakim di persidangan, tanpa memicu perdebatan panjang mengenai keabsahan forensik digital yang rumit.

Kegagalan eskalasi perkara dari tahapan administrasi ke ranah pidana di Polresta Banda Aceh bukan sekadar hambatan teknis, melainkan manifestasi dari kebuntuan paradigma penegakan hukum konvensional yang terlalu berorientasi pada pengejaran pelaku (*follow the suspect*). Dalam konteks Teori Penegakan Hukum Integratif, fenomena di mana penyidik lebih mengedepankan pembekuan rekening tanpa kelanjutan penuntutan menunjukkan adanya ketidakseimbangan sistemik antara birokrasi penegakan hukum dan nilai kemanfaatan hukum itu sendiri. Aparat cenderung terjebak dalam pragmatisme birokrasi—mereka melakukan langkah-langkah administratif yang efisien dengan cara berkorespondensi dengan Otoritas Jasa Keuangan—namun gagal mewujudkan tujuan hukum yang substantif karena proses hukum terhenti saat anonimitas pelaku gagal ditembus. Akibatnya, hukum hanya hadir sebagai instrumen penghenti gangguan, namun absen dalam memberikan keadilan distributif bagi korban yang kehilangan materiilnya.

Hambatan utama penyidik meliputi:

- Identitas pelaku yang menggunakan nama dan akun palsu atau meminjam identitas pihak lain.
- Kesulitan membuka rekening pelaku karena aturan kerahasiaan perbankan.
- Koordinasi yang lemah dengan operator seluler/ISP dan tidak semua penyidik memiliki kompetensi dalam teknologi.
- Keterbatasan alat khusus dan laboratorium forensik digital.

Realitas di lapangan yang memaksa korban untuk mengikhlaskan kerugiannya akibat pelacakan pelaku yang menemui jalan buntu mencerminkan adanya ketidakadilan prosedural yang akut. Secara kritis, hal ini terjadi karena sistem hukum Indonesia masih sangat bergantung pada vonis pidana untuk

mengekskusi pengembalian aset. Di sinilah urgensi adopsi landasan Non-Conviction Based (NCB) Asset Forfeiture menjadi sangat krusial sebagai komplemen kebijakan kriminal masa depan. Tanpa adanya regulasi yang memungkinkan perampasan aset secara mandiri terhadap dana yang telah dibekukan, maka tindakan administratif seperti pemblokiran rekening hanya akan menghasilkan *legal limbo*. Oleh karena itu, rekonstruksi kebijakan hukum *cyber* harus bergeser dari sekadar pengejaran bayang-bayang pelaku yang anonim menuju perlindungan aset korban yang nyata, guna mengakhiri praktik impunitas fungsional yang selama ini merugikan masyarakat dalam ekosistem digital (Sitompul, 2012).

Hal ini juga menentang perspektif victimology, yang mana korban memiliki hak atas restitusi dan ini seringkali menjadi aspek yang terabaikan akibat UU ITE yang hanya menitikberatkan pada pidana pokok tanpa mengatur mekanisme ganti rugi yang eksplisit. Secara teoritis, korban memang memiliki instrumen legal seperti penggabungan ganti kerugian, gugatan perdata perbuatan melawan hukum, atau mekanisme melalui LPSK. Namun, dalam praktiknya, ketiadaan putusan pidana yang menetapkan ganti rugi memaksa korban menempuh jalur perdata yang melelahkan secara biaya dan waktu. Ketika perkara berakhir pada SP3 atau sekadar pemblokiran administratif, hak pemulihan ekonomi korban secara praktis gugur, menciptakan ketidakadilan substantif bagi pihak yang dirugikan (Kakoe, Ruba'i, & Madjid, 2020).

Oleh karena itu, diperlukan rekonseptualisasi terhadap status perkara melalui inovasi seperti penangguhan penyidikan formal saat menunggu koordinasi mandatori dengan lembaga pusat atau otoritas keuangan. Sebelum penghentian penyidikan (SP3) dilakukan, harus ada kewajiban bagi penyidik untuk mendapatkan konfirmasi formal dari Otoritas Jasa Keuangan atau perbankan terkait ketersediaan data transaksi. Hal ini memastikan bahwa hak konstitusional korban atas perlindungan harta benda tidak hilang begitu saja hanya karena fragmentasi birokrasi. Sinergi ini akan memastikan bahwa meskipun jalur pidana mengalami hambatan teknis, mekanisme pemulihan aset melalui jalur administratif tetap dapat diupayakan secara maksimal.

Dalam teori faktor-faktor penegakan hukum dari Soerjono Soekanto, disebutkan bahwa efektivitas penegakan hukum ditentukan oleh interaksi lima faktor, yaitu faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas, faktor masyarakat, dan faktor kebudayaan (Soekanto, 2016). Keempat faktor pertama teridentifikasi secara simultan dalam praktik penyidikan di Polresta Banda Aceh. Pada level faktor hukum, keberadaan *lex specialis* berupa UU ITE tidak serta-merta dikenakan oleh penyidik, karena kompleksitas pembuktian unsur elektronik dinilai lebih tinggi dibandingkan Pasal 492 KUHP. Pada level faktor penegak hukum dan faktor sarana, keterbatasan kapasitas teknis penyidik dalam menangani forensik digital, sebagaimana keterangan wawancara bersama Aiptu Henrikus Sricardo, serta ketiadaan laboratorium *cyber* yang memadai, memperkuat bukti bahwa persoalan yang dihadapi bukan sekadar kemauan aparat, melainkan keterbatasan struktural yang bersifat sistemik. Pada level faktor

kebudayaan, kecenderungan aparat untuk tetap berorientasi pada paradigma penegakan hukum konvensional turut menjelaskan mengapa pendekatan follow the suspect masih dipertahankan sebagai pendekatan dominan. Dengan demikian, dominasi penggunaan Pasal 492 KUHP di tingkat Polresta Banda Aceh tidak dimaknai semata sebagai preferensi teknis, melainkan sebagai konsekuensi dari akumulasi keterbatasan yang bersifat multidimensi.

Ditinjau lebih lanjut melalui teori sistem hukum yang dikemukakan Friedman (1975), yang membedakan hukum ke dalam tiga unsur, yaitu struktur, substansi, dan kultur hukum, persoalan utama yang dihadapi Polresta Banda Aceh ditemukan tidak semata terletak pada substansi hukum, tetapi juga pada aspek struktur, yaitu relasi kelembagaan dengan Otoritas Jasa Keuangan (OJK) dan Kementerian Komunikasi dan Digital yang belum terintegrasi secara fungsional. Data mengenai surat korespondensi penyidikan yang tidak memperoleh balasan pada tahun 2023 dan 2025 dipandang sebagai bukti atas kegagalan proses birokrasi, di mana dua atau lebih institusi penegak hukum berjalan sebagai entitas yang terpisah meskipun secara substansi hukum, melalui Pasal 7 KUHP dan Pasal 49 ayat (5) UU P2SK, kewajiban koordinasi telah diatur secara eksplisit.

B. Kedudukan Otoritas Jasa Keuangan dalam Penanganan Penipuan Berbasis Elektronik

Kedudukan Otoritas Jasa Keuangan dalam penanganan penipuan berbasis elektronik tidak dapat dilepaskan dari perdebatan konstitusional yang mengiringi kelahiran kewenangannya. Pasal 49 ayat (5) UU P2SK pada mulanya merumuskan bahwa penyidikan atas tindak pidana di sektor jasa keuangan “hanya dapat dilakukan oleh penyidik Otoritas Jasa Keuangan”, suatu formulasi yang dimaknai sebagian pihak sebagai peniadaan kewenangan Polri di sektor tersebut. Ketentuan ini kemudian dimohonkan pengujian ke Mahkamah Konstitusi oleh Serikat Pekerja Niaga Bank Jasa Asuransi bersama sejumlah nasabah korban lembaga keuangan, dan melalui Putusan Mahkamah Konstitusi Nomor 59/PUU-XXI/2023, frasa “hanya” dinyatakan bertentangan dengan UUD 1945 dan dihapuskan, sehingga norma tersebut kembali membuka ruang bagi Polri untuk turut serta melakukan penyidikan di sektor jasa keuangan. Mahkamah menilai bahwa kewenangan penyidikan tunggal Otoritas Jasa Keuangan berpotensi menegasikan kedudukan Polri sebagai penyidik utama dalam Sistem Peradilan Pidana Terpadu, serta bertentangan dengan prinsip negara hukum dan jaminan kepastian hukum sebagaimana diatur dalam Pasal 1 ayat (3), Pasal 28D ayat (1), dan Pasal 30 ayat (4) UUD 1945 (Mahkamah Konstitusi, 2023). Putusan ini penting dikemukakan karena menunjukkan bahwa kedudukan Otoritas Jasa Keuangan dalam penanganan penipuan berbasis elektronik, sebagaimana ditemukan dalam penelitian ini, beroperasi di atas fondasi kewenangan yang pernah dipersoalkan secara konstitusional, bukan otoritas yang sejak semula final dan tidak terbantahkan.

Terlepas dari kontroversi konstitusional tersebut, kewenangan Otoritas Jasa Keuangan di sektor jasa keuangan tetap dibangun atas argumen fungsionalis, yaitu kebutuhan akan penegakan hukum berbasis keahlian teknis, mengingat kejahatan

keuangan modern sangat tergantung pada kompleksitas produk dan rekayasa transaksi digital (Republik Indonesia, 2023). Otoritas Jasa Keuangan menekankan bahwa kehati-hatian dalam mengakses data nasabah merupakan konsekuensi logis dari rezim perlindungan data pribadi dan prinsip kerahasiaan bank yang harus dihormati secara proporsional. Akan tetapi, prinsip kehati-hatian tersebut, dalam praktiknya, turut menjadi salah satu sumber hambatan bagi penyidik kepolisian dalam memperoleh akses data yang lebih terperinci. Dengan demikian, prinsip kehati-hatian Otoritas Jasa Keuangan, alih-alih murni menjadi strategi penanganan yang terstruktur, pada saat yang sama berkontribusi terhadap ketegangan fungsional dengan kebutuhan penyidikan pidana yang bersifat mendesak (Otoritas Jasa Keuangan, 2026).

Integrasi operasional Indonesia Anti-Scam Centre (IASC) dalam ekosistem keuangan digital merupakan manifestasi krusial dari mandat Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (Republik Indonesia, 2023). Eskalasi kasus penipuan elektronik di Banda Aceh yang mencatatkan kerugian hingga Rp 14,2 miliar sepanjang tahun 2025 hingga awal 2026 menegaskan bahwa mekanisme penegakan hukum konvensional tidak lagi memadai untuk membendung laju kejahatan *cyber* yang bersifat sistemik (Otoritas Jasa Keuangan Provinsi Aceh, 2026). Karakteristik teknis dari modus operandi seperti rekayasa sosial (*social engineering*) dan penyalahgunaan file APK palsu menuntut adanya pendekatan *lex specialis* yang berbasis pada keahlian teknologi finansial. Dalam konteks ini, Otoritas Jasa Keuangan memegang peran sentral sebagai aktor utama dalam fase identifikasi risiko dan pemetaan pola kejahatan untuk menghindari fragmentasi penegakan hukum yang selama ini melemahkan efektivitas penanganan kejahatan lintas platform (Indonesia Anti-Scam Centre, 2026).

Efektivitas IASC sebagai instrumen perlindungan konsumen sangat bergantung pada standarisasi prosedur pelaporan yang wajib dipenuhi oleh korban guna menjamin validitas bukti hukum. Prosedur ini dimulai dengan pengumpulan data identitas diri berupa KTP atau SIM dan bukti kepemilikan rekening sebagai dasar legalitas pelapor, yang kemudian wajib diikuti dengan penyusunan kronologi kejadian secara sistematis serta lampiran bukti transaksi atau mutasi rekening yang akurat (Indonesia Anti-Scam Centre, 2026). Penggunaan kanal pelaporan yang terintegrasi, seperti situs resmi iasc.ojk.go.id, Kontak 157, maupun layanan WhatsApp resmi, memungkinkan terjadinya percepatan koordinasi antar-Penyedia Jasa Keuangan (PJK) secara real-time. Formalisasi prosedur ini berfungsi sebagai filter integritas yang memungkinkan otoritas melakukan tindakan darurat berupa penundaan transaksi atau pemblokiran rekening pelaku secara instan, sehingga meminimalisir risiko hilangnya aset korban akibat lambatnya proses birokrasi perbankan manual (Otoritas Jasa Keuangan, 2026).

Dalam praktik operasionalnya, prosedur internal Otoritas Jasa Keuangan menitikberatkan pada paradigma *follow the money* yang bersifat investigatif administratif, bukan pada penindakan pidana terhadap pelaku secara langsung. Data menunjukkan bahwa tingkat penyelamatan dana korban di wilayah Banda

Aceh baru menyentuh angka 12% (Satgas PASTI, 2026). Capaian ini sepatutnya dibaca secara kritis: rendahnya rasio pengembalian dana justru mengindikasikan bahwa pendekatan administratif yang mengandalkan pemblokiran rekening semata, tanpa disertai eskalasi yang konsisten ke ranah pidana terhadap pelaku, belum cukup memberikan pemulihan ekonomi yang memadai bagi korban. Penyelidikan melalui tahapan internal ini menitikberatkan pada analisis data keuangan dan klarifikasi kepada pelaku usaha jasa keuangan, bukan pada tindakan koersif secara langsung, sehingga legitimasinya sebagai instrumen pengawasan sektor jasa keuangan tidak dapat disamakan dengan penegakan hukum pidana yang berorientasi pada pemidanaan pelaku dan pemulihan hak korban secara utuh di era *cyber*.

Dari perspektif kebijakan hukum, posisi Otoritas Jasa Keuangan dalam mengelola IASC mencerminkan upaya sistematis untuk menyeimbangkan kepentingan perlindungan konsumen, stabilitas sistem keuangan, dan kepastian hukum bagi masyarakat di wilayah otonomi khusus seperti Aceh. Penanganan yang dilakukan secara mandiri dalam tahap awal, mulai dari penerimaan laporan hingga pemetaan pola kejahatan, merupakan manifestasi dari desain hukum yang menempatkan sektor jasa keuangan sebagai rezim khusus (Republik Indonesia, 2023). Hal ini membuktikan bahwa efektivitas pemberantasan penipuan online sangat bergantung pada kemampuan otoritas dalam melakukan intervensi teknis secara seketika (*immediate intervention*). Sinergi antara 21 instansi dalam Satgas PASTI dan asosiasi industri menjadi pilar utama dalam menciptakan ekosistem keuangan yang tangguh dan responsif terhadap dinamika kejahatan ekonomi digital (Asosiasi Sistem Pembayaran Indonesia & iDEA, 2026).

Integrasi data kasus di Kota Banda Aceh menunjukkan bahwa kerentanan digital tidak mengenal batas wilayah ataupun sistem perbankan tertentu, termasuk perbankan syariah yang dominan di Aceh. Meskipun Aceh memiliki karakteristik regulasi daerah yang khusus, ketergantungan masyarakat terhadap sistem pembayaran nasional tetap menempatkan warga pada risiko scam yang serupa dengan wilayah lainnya (Otoritas Jasa Keuangan Provinsi Aceh, 2026). Oleh karena itu, prosedur IASC yang bersifat nasional namun dapat diakses secara lokal menjadi jembatan penting dalam memberikan perlindungan hukum yang inklusif. Keberadaan IASC di Aceh berfungsi untuk memotong rantai birokrasi yang panjang, memastikan bahwa setiap pengaduan masyarakat Aceh dapat segera dikoordinasikan dengan bank tujuan di seluruh Indonesia guna membekukan aliran dana ilegal secepat mungkin.

Transformasi prosedural melalui IASC yang didorong oleh mandat UU P2SK merupakan langkah signifikan dalam memperluas kanal perlindungan konsumen sektor jasa keuangan. Namun demikian, peran Otoritas Jasa Keuangan dalam sistem ini perlu dipahami secara proporsional, tidak sebagai bentuk penyelesaian pidana atas penipuan berbasis elektronik, melainkan sebagai fungsi administratif-preventif yang berjalan pada rezim kewenangan yang berbeda dan, sebagaimana ditunjukkan oleh Putusan Mahkamah Konstitusi Nomor 59/PUU-XXI/2023, sempat dipersoalkan legitimasinya. Ditinjau melalui teori Sistem Peradilan Pidana

Terpadu yang dikembangkan Muladi dan Barda Nawawi Arief (1992), penegakan hukum pidana semestinya berjalan sebagai rangkaian subsistem yang koheren antara kepolisian, kejaksaan, dan pengadilan. Berbeda halnya, Otoritas Jasa Keuangan saat ini justru menunjukkan keterputusan antar-subsistem tersebut: proses administratif Otoritas Jasa Keuangan melalui IASC berhenti pada tahap pemblokiran rekening tanpa disertai pelimpahan data secara otomatis kepada subsistem penyidikan pidana Polri, sehingga tujuan akhir sistem peradilan pidana terpadu, yaitu kepastian hukum dan pemulihan hak korban, tidak sepenuhnya tercapai.

Persoalan ini diperberat oleh keterbatasan kapasitas kelembagaan Otoritas Jasa Keuangan sendiri sebagai penyidik. Data resmi menunjukkan bahwa Otoritas Jasa Keuangan secara nasional baru memiliki sekitar 10 penyidik dari unsur Polri, 5 PPNS, dan 5 jaksa penugasan sebagai analis perkara, suatu jumlah yang jauh dari memadai untuk menjangkau volume laporan penipuan elektronik yang terus meningkat di seluruh Indonesia, termasuk di Aceh. Dengan demikian, keterbatasan sumber daya manusia bukan hanya persoalan yang melekat pada kepolisian di tingkat kewilayahan sebagaimana diuraikan pada bagian sebelumnya, melainkan juga persoalan yang melekat pada Otoritas Jasa Keuangan sebagai otoritas yang diberi kewenangan penyidikan mandiri. Ditinjau melalui teori efektivitas hukum, UU P2SK dan mekanisme IASC dinyatakan telah memenuhi syarat keberlakuan yuridis, karena kedua instrumen tersebut sah secara hierarki peraturan perundang-undangan. Namun demikian, secara sosiologis, rendahnya rasio pengembalian dana serta ketiadaan pelimpahan otomatis ke ranah pidana menunjukkan penyimpangan implementasi dari desain normatifnya, sehingga secara filosofis, tujuan hukum berupa kepastian hukum dan keadilan distributif bagi korban belum sepenuhnya tercapai. Oleh karena itu, keberadaan IASC sepatutnya dipandang sebagai pelengkap, bukan pengganti, bagi proses penegakan hukum pidana yang harus tetap dijalankan secara paralel oleh kepolisian, dengan mekanisme koordinasi fungsional yang jelas dan mengikat antara kedua lembaga.

Kesimpulan

Penelitian ini menyimpulkan bahwa penanganan tindak pidana penipuan berbasis elektronik di wilayah hukum Polresta Banda Aceh belum mencapai tingkat efektivitas yang diharapkan, sebagaimana ditunjukkan oleh tidak adanya kasus yang diselesaikan hingga tahap penangkapan pelaku. Kondisi tersebut tidak semata-mata disebabkan oleh faktor teknis penyidikan, melainkan merupakan konsekuensi dari pendekatan penegakan hukum yang masih bertumpu pada paradigma hukum pidana konvensional melalui penerapan Pasal 492 Kitab Undang-Undang Hukum Pidana (KUHP). Meskipun pasal tersebut memberikan kemudahan dari aspek pembuktian, penerapannya tidak sepenuhnya mampu merespons karakteristik khas kejahatan penipuan berbasis elektronik yang bersifat anonim, berbasis teknologi informasi, serta melibatkan alur transaksi keuangan yang kompleks dan lintas yurisdiksi.

Di sisi lain, stagnasi penanganan perkara penipuan berbasis elektronik dipengaruhi oleh keterbatasan kewenangan penyidikan di tingkat kepolisian,

rigiditas prosedur birokrasi internal, serta ketergantungan struktural terhadap akses data keuangan dan data elektronik yang berada di luar otoritas langsung kepolisian. Kondisi tersebut secara signifikan membatasi kemampuan penyidik untuk melakukan penelusuran aliran dana, identifikasi pelaku, dan pengumpulan alat bukti digital secara komprehensif, sehingga perkara cenderung terhenti pada tahap proses penyelidikan.

Dalam konteks kelembagaan, peran Otoritas Jasa Keuangan (OJK) dalam penanganan fenomena penipuan berbasis elektronik berjalan dalam kerangka kewenangan yang berbeda dan tidak bersifat intervensi terhadap proses penyidikan pidana. Otoritas Jasa Keuangan menjalankan fungsi penyelidikan mandiri terhadap dugaan pelanggaran di sektor jasa keuangan sebagaimana diatur dalam Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan, khususnya Pasal 49 ayat (5). Namun demikian, ketiadaan mekanisme koordinasi fungsional yang terstruktur antara Otoritas Jasa Keuangan dan kepolisian menyebabkan hasil penyelidikan tersebut belum terintegrasi secara optimal.

Dengan demikian, dapat disimpulkan bahwa belum terselesaikannya perkara penipuan berbasis elektronik di Polresta Banda Aceh merefleksikan adanya ketidaksinkronan antara karakter kejahatan digital dan desain kelembagaan penegakan hukum yang masih sektoral. Penelitian ini menegaskan urgensi pembaruan kerangka penegakan hukum pidana *cyber* melalui penguatan kapasitas institusional, penegasan batas kewenangan antar lembaga, serta pembangunan mekanisme koordinasi yang efektif dan berkelanjutan, guna menjamin kepastian hukum dan perlindungan yang optimal bagi masyarakat di era ekonomi digital.

Daftar Pustaka

Buku

- Ahmad M. Ramli. (2004). *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*. Bandung: Refika Aditama.
- Sitompul, J. (2012). *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.
- Utama, P. (2013). *Memahami Asset Recovery & Non-Conviction Based Asset Forfeiture di Indonesia*. Jakarta: Kencana.
- Atmasasmita, R. (2012). *Teori Hukum Integratif: Rekonstruksi Transformatif Hukum Indonesia*. Jakarta: Ghalia Indonesia.
- Hum, M., & Sh, D. M. (2020). *Metode Penelitian Hukum*.
- Friedman, L. M. (1975). *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation.
- Muladi, & Arief, B. N. (1992). *Teori-Teori dan Kebijakan Pidana*. Bandung: Alumni.

Soekanto, S. (2016). Faktor-Faktor yang Mempengaruhi Penegakan Hukum. Jakarta: Rajawali Pers.

Jurnal

Affianto, A., & Ishlahuddin, M. (2025). Penegakan Hukum bagi Pelaku Tindak Pidana Transaksi Jual Beli Online E-Commerce. AHKAM. <https://doi.org/10.58578/ahkam.v4i3.6662>

Apsimet, N. M., & Muratova, A. Zh. (2025). On the possibility of using the provisions of the Budapest Convention on cybercrime in the investigation of crimes in the field of online fraud. Bulletin of the Karaganda University. Law Series, 117(1), 87–97. <https://doi.org/10.31489/2025L1/87-97>

Duarif, & Saleh, M. (2023). Pencegahan dan penindakan tindak pidana cyber. Unes Law Review, 6(4).

Faiz, E. M., & Harefa, B. (2023). Pengaturan tindak pidana bagi pelaku penipuan phising berbasis web. Jurnal Hukum, 1–15.

Găbudeanu, M., et al. (2021). Cyber fraud, digital banking and risk management. Risks, 9(6), 104.

Hanif, A. (2024). Peran hukum pidana dalam menangani kejahatan cyber pada masa sekarang: Tinjauan terhadap UU ITE. Jurnal Education and Law Review, 2(6).

Harunulah, A., & Gunawan, Y. (2023). Law Enforcement in Revealing Fraud Crime Cases via Internet Media (Study at POLRES Metro Depok City). FOCUS: Journal of Social Studies, 4(2), 1–10. <https://doi.org/10.37010/fcs.v4i2.1331>

Kakoe, S., Ruba'i, M., & Madjid, A. (2020). Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi Sebagai Pidana Tambahan. Legalitas Jurnal. <https://doi.org/10.33756/jelta.v13i02.7612>

Kesuma, I. G. M. J., Widiati, I. A. P., & Sugiarta, I. N. G. (2020). Penegakkan hukum terhadap penipuan melalui media elektronik. Jurnal Preferensi Hukum, 1(2), 72–77. <http://doi.org/10.22225/jph.v1i2.2381.72-77>

Khusnaeni, I. (2023). Urgensi Otoritas Jasa Keuangan sebagai penyidik tunggal tindak pidana fintech dalam UU P2SK [Skripsi, UIN Maulana Malik Ibrahim Malang]. Repository UIN Malang.

Kurnia, N., Rahayu, Wendratama, E., Monggilo, Z. M. Z., Damayanti, A., Angendari, D. A. D., Abisono, F. Q., Shafira, I., & Desmalinda. (2022). Penipuan digital di Indonesia: Modus, medium, dan rekomendasi. Center for Digital Society (CfDS) UGM.

Masdi, A. S., Alam, S., & Rustan, R. (2022). Upaya hukum dalam penanggulangan tindak pidana penipuan berbasis elektronik oleh kepolisian. Legal Dialogica, 4(2), 112–125. <https://jurnal.fh.umi.ac.id/index.php/legal/article/view/1468>

- Palembangan, P., Mading, B., & Almusawir, A. (2023). Analisis Yuridis Penerapan Sanksi Pidana Terhadap Penipuan Bisnis Melalui Elektronik di Kepolisian Daerah Sulawesi Selatan. *Jurnal Legalitas Hukum Indonesia*. <https://doi.org/10.35965/ijlf.v5i2.2677>
- Pangemanan, P. P. R. G., Suoth, J. D., & Ante, R. (2026). Penerapan hukum tindak pidana penipuan menurut Pasal 378 KUHP di Indonesia. *Politico: Jurnal Ilmu Politik*, 7(1).
- Pasaribu, R., Prasetyasari, C., Lubis, I., & Damayanti, I. (2025). Proses Penyelesaian Tindak Pidana Terhadap Pelaku Penipuan Melalui Pembayaran Elektronik. *Zona Keadilan: Program Studi Ilmu Hukum (S1) Universitas Batam*. <https://doi.org/10.37776/zkih.v15i1.1813>
- Purwanti, Y., Rachman, F., Gunawan, T., & Kartadinata, A. (2023). Upaya Penanggulangan Tindak Pidana Penipuan dengan Metode Phising oleh Kepolisian Daerah Lampung. *Audi Et AP: Jurnal Penelitian Hukum*, 2(1), 64–71. <http://doi.org/10.24967/jaeap.v2i01.2088>
- Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, 6(1), 38–45. <https://doi.org/10.35870/jpni.v6i1.1097>
- Rahmanto, T. Y. (2019). Penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik. *Jurnal Penelitian Hukum De Jure*, 19(1), 31–52. <http://dx.doi.org/10.30641/dejure.2019.V19.31-52>
- Samudra, A. H. (2017). Modus Operandi dan Problematika Penanggulangan Tindak Pidana Penipuan Daring. *Jurnal Hukum*, 1–15.
- Sariani, A. L. (2023). Efektivitas penegakan hukum terhadap kejahatan cyber di Indonesia. *AlDalil: Jurnal Hukum dan Politik Islam*, 4(1), 45–60. <https://ejournal.indrainstitute.id/index.php/aldalil/article/view/824>
- Satriani. (2019). Perspektif hukum pidana Islam terhadap tindak pidana penipuan di media elektronik (Studi Kasus PN Makassar) [Skripsi, UIN Alauddin Makassar]. Repository UIN Alauddin.
- Sutarli, A. F., & Kurniawan, S. (2023). Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia. *INNOVATIVE: Journal Of Social Science Research*, 3(2), 4208–4221.
- Syahril, M. A. F., & Aris, A. (2021). Strategies and dynamics of online fraud in Indonesia: Tracing the effectiveness of the implementation of the electronic information and transactions act. *Journal of Law Justice*, 6(2), 89–104. <https://ejournal.umsorong.ac.id/index.php/jlj/article/view/3711>
- Wahyudin, J., Renggong, R., & Hamid, A. H. (2024). Analisis tindak pidana penipuan secara online di wilayah kepolisian daerah Sulawesi Selatan.

Indonesian Journal of Legality of Law, 6(2), 273–280.
<https://doi.org/10.35965/ijlf.v6i2.4474>

Wulandari, S. (2021). Mekanisme Penyidikan Tindak Pidana Penipuan Yang Menggunakan Media Transaksi Elektronik. *Spektrum Hukum*.
<https://doi.org/10.35973/sh.v18i1.2388>

Web

ALO. (2024). Peranan Otoritas Jasa Keuangan (OJK) sebagai Penyidik Tindak Pidana Pencucian Uang (TPPU) Pasca Undang-Undang P2SK.
<https://alchemistgroup.co/peranan-otoritas-jasa-keuangan-ojk-sebagai-penyidik-tindak-pidana-pencucian-uang-tppu-pasca-undang-undang-p2sk/>

Asosiasi Sistem Pembayaran Indonesia & iDEA. (2026). Sinergi Industri dalam Mendukung Infrastruktur IASC. Jakarta: Sekretariat Asosiasi Industri Keuangan.

Mahkamah Konstitusi. (2023). Putusan Nomor 59/PUU-XXI/2023 tentang Pengujian Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. Jakarta: Mahkamah Konstitusi Republik Indonesia.

Hukumonline. (2024). Urgensi koordinasi OJK dan Polri dalam penyidikan tindak pidana sektor jasa keuangan. <https://www.hukumonline.com>

Indonesia Anti-Scam Centre. (2026). Pedoman Operasional dan Prosedur Pelaporan Penipuan Transaksi Keuangan. Jakarta: Pusat Penanganan Penipuan Transaksi Keuangan - Otoritas Jasa Keuangan.

Otoritas Jasa Keuangan Provinsi Aceh. (2026). Laporan Tren Kejahatan Keuangan Digital dan Perlindungan Konsumen Wilayah Kerja Provinsi Aceh Tahun 2025. Banda Aceh: Kantor OJK Aceh.

Otoritas Jasa Keuangan. (2026). Strategi Mitigasi Penipuan Elektronik melalui Penguatan Kewenangan Penyelidikan Mandiri OJK. Jakarta: OJK.

Republik Indonesia. (2023). Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK). Jakarta: Sekretariat Negara.

Satgas Pemberantasan Aktivitas Keuangan Ilegal (PASTI). (2026). Data Statistik Pemblokiran Entitas Keuangan Ilegal dan Aliran Dana Penipuan Digital Nasional. Jakarta: Satgas PASTI.

Wawancara

Wawancara dengan Aiptu Henrikus Sricardo, S.H., Penyidik Polresta Banda Aceh, Banda Aceh, 25 November 2025.

Wawancara dengan pembantu penyidik Polresta Banda Aceh.