JISPENDIORA : Jurnal Ilmu Sosial, Pendidikan Dan Humaniora
Volume. 4 Nomor. 1 April 2025
e-ISSN: 2829-3886; p-ISSN: 2829-3479, Hal. 603-613
DOI: https://doi.org/10.56910/jispendiora.v4i1.2504
Available online at: https://jurnal-stiepari.ac.id/index.php/jispendiora

Implementasi Hukum terhadap Tindak Pidana Scammer

Yohanes Reston N.A Laia[1*], Rahmayanti[2], Sari Sania Tampubolon[3], Alex Sokhian Gea[4], Sudarno Hariadi Nasution[5]
[1-5]Program Studi Magister Ilmu Hukum, Universitas Pembangunan Panca Budi, Indonesia
Email : yohaneslaia263@gmail.com, rahmayanti@dosen.pancabudi.ac.id, sarisaniatampubolon23@gmail.com, geaalex8999@gmail.com, Nasutiondedek23@gmail.com

*Korespondensi penulis : yohaneslaia263@gmail.com**

Abstract : *Law enforcement is an effort to realize the ideals of law to create justice, benefit and legal certainty in reality. The crime of online fraud based on scammers is a cyber crime, the regulation is regulated in Article 378 of the Criminal Code. From year to year the number of scammer-based online fraud crimes is increasing as evidenced by community reports every year and even every week there must be victims of fraud crimes committed in cyberspace, but the number of settlements is very small, this indicates a problem, both internally and externally, so that law enforcement which is the benchmark for the effectiveness of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, The author is interested in conducting a qualitative research method, to find various reading literature related to the application of law to criminal acts of fraud committed online or can be referred to as scammers, this research aims to find legal certainty and benefits for people who feel harmed.*

Keywords: *Application, Crime, Fraud.*

Abstrak : Penegakan hukum merupakan upaya untuk mewujudkan cita-cita hukum untuk menciptakan keadilan, kemanfaatan dan kepastian hukum dalam kenyataan. Tindak pidana penipuan online berbasis Scammer merupakan kejahatan Siber, pengaturannya diatur dalam Pasal 378 KUHP pidana. Dari tahun ketahun jumlah tindak pidana penipuan online berbasis Scammer semakin meningkat dibuktikan dari laporan masayarakat setiap tahun nya bahkan setiap minggu pasti adanya korban dari kejahatan penipuan yang dilakukan di dunia maya, namun jumlah penyelesaiannya sangat kecil, Hal ini menunjukkan adanya masalah, baik secara internal maupun external, sehingga penegakan hukum yang menjadi tolak ukur dari efektivitas Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, belum tercapai secara maksimal, dan penulis tertarik untuk melakukan metode penelitian secara kualitatif, untuk mencari berbagai literatur bacaan yang berkaitan dengan penerapan hukum terhadap tindak pidana penipuan yang dilakukan secara online atau dapat disebut sebagai scammer, penelitian ini bertujuan untuk mencari kepastian hukum dan kemanfaatan bagi orang yang merasa dirugikan

Kata Kunci : Kejahatan, Penipuan, Penarapan.

1. PENDAHULUAN

Dalam kehidupan bermasyarakat selalu adanya peraturan hukum yang berlaku dan dibuat untuk perdamaian di Tengah-tengah Masyarakat agar terciptanya suatu keharmonisan dalam kehidupan sehari-hari. Penegakan hukum harus dilaksanakan sesuai dengan peraturan yang berlaku serta berlandaskan pada Pancasila dan Undang-Undang Dasar Negara Republik Indonesia. Tujuannya adalah untuk mewujudkan cita-cita bangsa Indonesia sebagaimana tercantum dalam Alinea keempat Pembukaan UUD 1945, yaitu melindungi seluruh rakyat Indonesia dan wilayahnya, meningkatkan kesejahteraan masyarakat, mencerdaskan kehidupan bangsa, serta berperan aktif dalam menciptakan ketertiban dunia yang berlandaskan kemerdekaan, perdamaian abadi, dan keadilan sosial.

Received: Mei 14, 2025; Revised: Mei 28, 2025; Accepted: Juni 11, 2025; Published: Juni 13, 2025

Internet adalah (Inter-Network) adalah sebutan untuk sekumpulan jaringan komputer yang menghubungkan situs akademik, pemerintahan, komersial, organisasi, maupun perorangan. Layanan internet meliputi komunikasi langsung (email,chat), diskusi (Usenet News, email, milis), sumber daya informasi yang terdistribusi (World Wide Web, Gopher), remote login dan lalu lintas file (Telnet, FTP), dan aneka layanan lainnya (Asri et al., 2011). Kemajuan teknologi telah diakui membawa berbagai kemudahan dalam mendukung aktivitas manusia. Namun, seiring dengan perkembangannya, muncul pula jenis-jenis kejahatan baru yang memanfaatkan komputer dan jaringan. Kejahatan di dunia maya, yang dikenal sebagai *cybercrime*, merupakan tindakan ilegal yang dilakukan melalui sistem elektronik dengan tujuan menyerang keamanan sistem komputer serta data yang dikelola di dalamnya, salah satu bentuk tindak pidana yang sering terjadi di dunia maya yaitu penipuan, yang mana Tindakan ini sering terjadi ditengah-tengah Masyarakat, dengan di iming-iming kepada korban akan mendapatkan sesuatu hal Ketika melakukan penanaman modal dalam bentuk investasi, hal ini sering memuju Masyarakat dan tertarik dengan ajakan tersebut, Perbuatan ini merupakan tindakan yang dilarang berdasarkan Kitab Undang-Undang Hukum Pidana yang selanjutnya disebut KUHP dan UU ITE.

Tindak pidana penipuan diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) sebagai suatu perbuatan melanggar hukum yang dapat dikenai sanksi pidana. Selain itu, tindakan tersebut juga diatur dalam Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur mengenai penyebaran informasi palsu atau menyesatkan yang merugikan konsumen. Pelaku dapat dikenai hukuman berdasarkan salah satu atau kedua pasal tersebut, yaitu Pasal 378 KUHP dan Pasal 28 ayat (1) UU ITE. Meskipun ketentuan ini dimaksudkan untuk menciptakan pemanfaatan internet yang positif, aman, dan terkendali, pada kenyataannya masih ada sebagian masyarakat yang melanggar aturan tersebut, sehingga menimbulkan kerugian bagi pihak lain. Pemerintah Indonesia sebenarnya telah mengatur tindak pidana penipuan, termasuk yang dilakukan secara online, melalui berbagai perangkat hukum, seperti Kitab Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi, (Handoyo, B. et al., 2024) beserta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Kemajuan teknologi informasi dan komunikasi di era digital saat ini telah membawa perubahan besar dalam berbagai aspek kehidupan manusia, termasuk transaksi jual beli, interaksi sosial, hingga aktivitas perbankan kini dapat dilakukan secara online dengan cepat dan efisien (Rahayu, E. L. B. & Syam, N, 2021). Namun, seiring dengan

kemudahan tersebut, muncul pula berbagai bentuk kejahatan siber yang meresahkan masyarakat. Salah satu bentuk kejahatan yang paling sering terjadi adalah tindak pidaAbekas luka. Meningkatnya kasus penipuan online ini telah menimbulkan kerugian yang signifikan, baik dari segi materiil maupun psikologis bagi korban. Tidak sedikit masyarakat yang kehilangan harta benda dalam jumlah besar karena terjebak dalam tipu daya scammer. Selain itu, penipuan online juga mengganggu stabilitas ekonomi, merusak kepercayaan masyarakat terhadap platform digital, dan berpotensi meningkatkan keamanan siber

Kejahatan dunia maya adalah suatu tindak pidana yang sangat serius terjadi di tahun yang akan datang, dikarenakan dalam proses penyelesaian nya sangat kecil bahkan tidak dapat di temukan siapa pelaku nya, sehingga ini menjadi tantangan bagi pemerintah untuk dapat membasmi para pelaku yang melakukan tindak pidana melalui internet. Dengan penjelasan di atas maka kami sebegai peneliti tertarik untuk mengambil judul "**implementasi hukum terhadap tindak pidana scammer".**

Rumusan Masalah

a. Bagaimana penerapan hukum terhadap tindak pidana penipuan secara Online?
b. Apa yang menjadi rintangan dalam proses penyelidikan dan penyidikan terhadap tindak pidana Scammer?

2. METODE PENELITIAN

Metode penelitian yang peneliti lakukan ialah kualitatif dengan menggunakan tipe studi literatur (analisis jurnal, analisis makalah, atau media lainnya) agar menjadi sebuah bacaan literatur yang tersusun secara runtut dan rapi. Metode penelitian ini adalah dengan studi literatur ini yakni mencari beragam artikel yang relavan tentang penerapan hukum terhadap tindak pidana Scammer Selain itu, data yang diperoleh berasal dari data sekunder yang berasal dari artikel ilmiah yang telah dipublikasikan diberbagai jurnal nasional terakreditasi.

3. PEMBAHASAN

Penerapan Hukum Terhadap Tindak Pidana Penipuan Secara Online

Kemajuan teknologi telah membawa perubahan dan pergeseran yang cepat dalam suatu kehidupan tanpa batas. Kemajuan juga telah melahirkan keresahan-keresahan baru dengan munculnya kejahatan yang canggih dalam bentuk *cybercrime*. Penipuan

secara *online* adalah suatu bentuk kejahatan yang sangat besar dengan menggunakan teknologi informasi dalam melakukan perbuatannya. Selalu ada korban yang dirugikan dalam setiap kasus penipuan, sehingga kasus penipuan *online* telah diatur di dalam KUHP dan UU ITE. Walaupun kasus penipuan secara online telah diatur di dalam KUHP dan UU ITE. Ada beberapa Upaya yang harus dilakukan dalam penerapan hukum terhadap tindak pidana penipuan di media sosial antara lain :

a. Upaya preventif

Upaya preventif bertujuan untuk mencegah terjadinya kejahatan siber melalui mekanisme edukasi, peningkatan literasi digital, dan penguatan sistem keamanan informasi. Salah satu ketentuan yang sangat relevan dalam konteks ini adalah yang tercantum dalam UU No. 1/2024. Secara khusus, ketentuan tersebut menyatakan bahwa setiap orang yang dengan sengaja mengirimkan atau menyebarkan informasi elektronik atau dokumen elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan, sehingga mengakibatkan kerugian materiel bagi konsumen dalam transaksi elektronik, dapat dijerat pidana.

a) Ketentuan Produk Hukum Preventif

Bunyi Pasal dan Isi Regulasi. Bunyi Regulasi: UU No. 1/2024, sebagai perubahan kedua atas UU ITE, menetapkan bahwa penyebaran informasi yang menyesatkan melalui media elektronik yang menyebabkan kerugian materiil dapat dikenai sanksi pidana. Isi Regulasi: Regulasi ini menekankan bahwa pelaku yang secara sengaja mengirim atau menyebarkan informasi bohong melalui media elektronik, yang pada akhirnya merugikan konsumen dalam transaksi daring, harus bertanggung jawab secara hukum. Penerapan: Dalam implementasinya, regulasi ini mendorong aparat penegak hukum untuk melakukan penyidikan dengan mengumpulkan bukti digital yang memadai dan melakukan evaluasi terhadap dampak penyebaran informasi palsu tersebut.

b) Unsur-unsur Sanksi Preventif.

Dalam kerangka preventif, regulasi menetapkan beberapa unsur utama yang harus dipenuhi, antara lain: Larangan Penyebaran Informasi Menyesatkan: Setiap penyebaran informasi palsu yang dapat menyesatkan masyarakat dilarang secara tegas. Penerapan Sanksi Administratif: Untuk pelanggaran yang menimbulkan kerugian kecil, dapat dikenai sanksi administratif berupa denda atau teguran. Penerapan Sanksi Pidana: Untuk kasus yang menyebabkan

kerugian besar, sanksi berupa hukuman penjara hingga 6 tahun dan/atau denda maksimal Rp1 miliar diberlakukan.

b. Sanksi Pidana (Pendekatan Represif)

Pendekatan represif dalam sistem penindakan tindak pidana penipuan di media sosial menekankan penerapan sanksi yang tegas guna memberikan efek jera kepada pelaku. Analisis produk hukum di sini mengacu pada penerapan ketentuan sanksi pidana yang termaktub dalam UU No. 1/2024 (UU ITE) serta KUHP, khususnya Pasal 378. Penerapan sanksi tersebut dijalankan melalui proses identifikasi, pengumpulan bukti digital, dan penuntutan yang sistematis.

Analisis Pasal dalam Konteks Represif:

Bunyi dan Unsur Pasal Represif: Bunyi Pasal: Dalam UU No. 1/2024, ketentuan mengenai tindak pidana penipuan elektronik menetapkan bahwa setiap orang yang sengaja mengirimkan atau menyebarkan informasi elektronik yang berisi pemberitahuan bohong atau menyesatkan dan mengakibatkan kerugian materiel dapat dijerat pidana. Unsur Perbuatan yang Dilarang: Analisis menyebutkan bahwa unsur perbuatan yang dilarang mencakup niat untuk menipu, penyebaran informasi palsu, dan dampak kerugian yang dialami oleh korban. Klasifikasi Kejahatan: Kejahatan ini diklasifikasikan berdasarkan tingkat kerugian yang ditimbulkan, di mana kerugian yang signifikan akan dikenai sanksi pidana yang lebih berat, yaitu hukuman penjara maksimal 6 tahun dan/atau denda hingga Rp1 miliar.

Alur Penerapan Sanksi Pidana Represif:

- Identifikasi Perbuatan: Pelaku melakukan penyebaran informasi palsu atau manipulasi data melalui media sosial.
- Pengumpulan Bukti Digital: Bukti dikumpulkan melalui teknologi forensik, termasuk rekaman komunikasi, data transaksi, dan metadata aktivitas daring.
- Proses Peradilan:Kasus diajukan ke pengadilan berdasarkan ketentuan UU ITE dan KUHP.
- Pemberian Putusan: Hakim menjatuhkan hukuman penjara dan/atau denda sesuai dengan tingkat keparahan tindak pidana.
- Efek Jera: Sanksi diharapkan memberikan efek jera kepada pelaku dan mencegah terjadinya kejahatan serupa di masa depan.

Penyelesaian Terhadap Kasus Penipuan di Media Sosial Penyelesaian kasus penipuan di media sosial melibatkan dua pendekatan utama: penyelesaian melalui proses hukum dan upaya pencegahan non-hukum. Analisis menyeluruh terhadap penyelesaian kasus dilakukan dengan memeriksa data empiris, putusan pengadilan, dan laporan aparat terkait, terutama pada platform jual beli online, yang menjadi sasaran utama modus penipuan daring

- Upaya pemblokiran rekening

  Melakukan pembukaan rekening pelaku tindak pidana kepada pihak perbankan atas permintaan penyidik. Pihak kepolisian dalam hal ini telah melakukan berbagai cara seperti, mengambil solusi untuk memblokir rekening pelaku tindak pidana penipuan online yang telah dikoordinasi terlebih dahulu dengan pihak bank, dalam hal ini untuk kelancaran pada saat proses pembuktian yang dilakukan oleh pihak penyidik dalam menyelidiki kasus tindak kejahatan penipuan tersebut dan dalam pengupayaan ini pihak penyidik hanya bisa melakukan sampai pemblokiran saja kepada pihak Bank dalam menanggulangi kejahatan, yang berdasarkan ijin tertulis.

Rintangan Dalam Proses Penyelidikan dan Penyidikan Terhadap Tindak Pidana Scammer

Perkembangan teknologi informasi telah membawa perubahan besar dalam berbagai aspek kehidupan, termasuk dalam bentuk interaksi ekonomi, sosial, dan hukum. Namun, di balik kemajuan teknologi tersebut, muncul pula bentuk kejahatan baru yang memanfaatkan sarana digital, salah satunya adalah tindak pidana penipuan daring atau dikenal dengan istilah *scamming*. Modus ini memanfaatkan perangkat teknologi informasi untuk mengelabui dan mengambil keuntungan dari korban melalui penipuan yang sistematis. Scammer atau pelaku penipuan daring umumnya beroperasi dengan menyamar sebagai pihak yang dipercaya, baik sebagai instansi resmi, tokoh publik, bahkan orang terdekat korban. Metode yang digunakan sangat variatif, mulai dari phishing, social engineering, rekayasa akun palsu, hingga penipuan berkedok investasi. Tindak pidana ini memiliki kompleksitas tinggi, karena sering kali melibatkan lintas negara, penggunaan teknologi canggih, serta eksploitasi atas kelalaian atau ketidaktahuan korban.

Dalam konteks penegakan hukum, penyelidikan dan penyidikan terhadap kejahatan scammer menghadapi berbagai kendala. Tulisan ini bertujuan untuk menjelaskan secara mendalam rintangan-rintangan yang muncul dalam proses

penyelidikan dan penyidikan, baik dari sisi teknis, yuridis, maupun institusional, serta memberikan refleksi atas tantangan tersebut sebagai bahan masukan bagi pembuat kebijakan dan aparat penegak hukum. Proses penyelidikan dan penyidikan terhadap tindak pidana scammer dimulai dengan diterimanya laporan dari korban kepada aparat penegak hukum, biasanya kepolisian. Pada tahap penyelidikan, petugas melakukan serangkaian tindakan awal untuk mencari dan menemukan peristiwa pidana, seperti mengidentifikasi modus penipuan, mengumpulkan bukti awal, serta menelusuri profil korban dan dugaan pelaku. Bila dari hasil penyelidikan diperoleh bukti permulaan yang cukup, maka kasus ditingkatkan ke tahap penyidikan, yaitu proses hukum yang lebih mendalam untuk mencari serta mengumpulkan bukti guna menemukan tersangka dan membuktikan bahwa suatu tindak pidana benar terjadi. Dalam tahap ini, penyidik akan melakukan pemanggilan dan pemeriksaan saksi, meminta keterangan dari korban, melakukan pelacakan jejak digital termasuk IP address, aktivitas media sosial, transaksi keuangan, hingga identitas yang digunakan oleh pelaku dalam melakukan aksinya. Penyidik juga sering bekerja sama dengan lembaga lain seperti bank, OJK, PPATK, maupun penyedia layanan internet (ISP) untuk memperoleh data yang relevan. Bila penyidik berhasil menemukan alat bukti yang cukup, mereka dapat menetapkan seseorang sebagai tersangka, melakukan upaya paksa seperti penangkapan dan/atau penahanan, serta menyita barang bukti. Setelah itu, berkas perkara akan disusun dan dilimpahkan ke jaksa penuntut umum untuk diteliti, sebelum akhirnya dibawa ke persidangan guna diproses secara hukum di pengadilan. Proses ini bertujuan untuk memberikan kepastian hukum, rasa keadilan bagi korban, serta efek jera terhadap pelaku tindak pidana penipuan atau scam.

Beberapa kendala yang akan dihadapi dalam proses penyidikan terhadap tindak pidana scammer berupa kesulitan dalam mengidentifikasi dan melacak pelaku yang sering kali menggunakan identitas palsu atau berdomisili di luar negeri, kurangnya sinergitas antar instansi penegak hukum, serta lemahnya pemahaman masyarakat terhadap proses hukum dan cara melindungi diri dari kejahatan digital. Aparat penegak hukum juga sering kali menghadapi keterbatasan dalam hal sumber daya manusia, pendukung teknologi, serta prosedur hukum yang belum sepenuhnya adaptif terhadap perkembangan kejahatan berbasis teknologi. Ciri khas utama dari tindak pidana scammer adalah anonimitas. Pelaku umumnya menyembunyikan identitas asli dengan memanfaatkan teknologi seperti VPN, server relay, TOR (The Onion Router), dan akun palsu. Mereka juga menggunakan identitas orang lain yang diperoleh melalui pencurian data (*identity theft*). Kesulitan dalam mengungkap identitas pelaku menjadi hambatan utama dalam proses penyelidikan, karena

tanpa identitas yang jelas, sulit untuk menentukan subjek hukum yang akan dimintai pertanggungjawaban pidana. Menurut INTERPOL, hampir 70% kasus scammer lintas negara tidak dapat ditindaklanjuti secara optimal karena pelaku tidak dapat diidentifikasi secara pasti. Bahkan dalam beberapa kasus, pelaku menggunakan perangkat lunak untuk memalsukan alamat IP dan lokasi fisik mereka. Penanganan tindak pidana scammer membutuhkan aparat yang memiliki pemahaman mendalam mengenai teknologi informasi dan digital forensik. Sayangnya, tidak semua aparat penegak hukum, khususnya di daerah, memiliki pelatihan dan keahlian yang mumpuni. Selain itu, lembaga penegak hukum juga menghadapi keterbatasan infrastruktur seperti perangkat lunak pemulihan data, laboratorium digital, dan akses terhadap data internasional. Sebagaimana dikemukakan Wahyuni, kurangnya personel yang menguasai TI menyebabkan penanganan kasus cybercrime menjadi tidak efektif. Keterbatasan ini diperparah oleh tingginya beban kerja dan kurangnya anggaran untuk pelatihan berkelanjutan bagi aparat penegak hukum.

Bukti dalam kasus scammer umumnya berupa bukti elektronik seperti log komunikasi, email, transaksi digital, dan metadata. Bukti ini sangat rentan terhadap penghapusan, modifikasi, atau hilangnya integritas data. Bahkan, waktu menjadi faktor krusial karena semakin lambat penyitaan bukti, semakin besar kemungkinan bukti tersebut tidak dapat digunakan di pengadilan. Forensik digital membutuhkan keahlian khusus untuk menjaga *chain of custody* dan memastikan bukti tidak terkontaminasi. Namun, dalam praktiknya, masih banyak aparat yang belum memiliki SOP digital forensik yang ketat, sehingga bukti menjadi tidak sah di hadapan hukum.

Tindak pidana scammer sangat sering melibatkan pelaku, korban, dan server dalam wilayah hukum yang berbeda. Dalam konteks ini, yurisdiksi menjadi tantangan besar. Penegakan hukum terhadap pelaku yang berada di luar negeri membutuhkan mekanisme bantuan hukum timbal balik (Mutual Legal Assistance/MLA), perjanjian ekstradisi, serta kerja sama dengan lembaga internasional. Sayangnya, proses MLA sering kali memakan waktu berbulan-bulan, bahkan bertahun-tahun, dan tidak semua negara bersedia memberikan data atau menangkap pelaku yang bukan warga negaranya. Hal ini menjadikan penegakan hukum terhadap scammer berskala internasional menjadi sangat terbatas.

Korban scammer sering kali enggan melaporkan kasusnya karena merasa malu, takut dipermalukan, atau merasa tidak ada gunanya melapor. Kurangnya literasi digital juga menyebabkan masyarakat tidak memahami cara melindungi diri mereka sendiri dari kejahatan digital. Data dari APJII menyebutkan bahwa hanya 1 dari 5 korban penipuan

daring yang benar-benar melaporkan kasusnya ke aparat penegak hukum. Hal ini menyebabkan banyak kasus tidak tercatat secara resmi, dan menurunkan efektivitas penegakan hukum berbasis data. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) memang telah menyediakan dasar hukum untuk menindak kejahatan siber, termasuk penipuan daring. Namun, regulasi ini belum cukup komprehensif dalam menjawab perkembangan modus-modus baru yang sangat dinamis. Sebagai contoh, penipuan berbasis kripto, *deepfake*, dan *social engineering* berbasis AI belum secara eksplisit diatur. Selain itu, ketentuan mengenai pembuktian digital dalam hukum acara pidana Indonesia masih belum detail, sehingga menyulitkan pembuktian di pengadilan.

4. KESMIPULAN

Berdasarkan uraian yang dijelaskan oleh penulis diatas, maka kesimpulan yang penulis dapat dari penelitian ini adalah sebagai berikut :

1) Tindak pidana penipuan diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) sebagai suatu perbuatan melanggar hukum yang dapat dikenai sanksi pidana. Selain itu, tindakan tersebut juga diatur dalam Pasal 28 ayat (1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang mengatur mengenai penyebaran informasi palsu atau menyesatkan yang merugikan konsumen. Pelaku dapat dikenai hukuman berdasarkan salah satu atau kedua pasal tersebut, yaitu Pasal 378 KUHP dan Pasal 28 ayat (1) UU ITE.
2) Tindak pidana Scammer adalah salah satu kejahatan penipuan secara online untuk memperoleh keuntungan dari korban, yang mana selalu memberikan berbagai modus untuk mempengaruhi orang lain dengan menjanjikan akan mendapatkan sesuatu yang lebih besar dari modal yang di tanamkan.
3) Bahwa tindak pidana Scammer adalah suatu kejahatan yang sangat serius kedepan nya, jika pemerintah mengabaikan permasalahan ini, apalagi setiap harinya selalu ada laporan dari Masyarakat tentang kejahatan ini. Namun dalam proses penyelidikan belum bisa menjamin dapat di tangkap para pelaku kejahatan Scammer. Sehingga dengan alasan ini Masyarakat lebih memilih untuk mendiamkan permasalahan yang sedang di alami dari pada melaporkan kepihak berwajib.
4) Bahwa Bukti dalam kasus scammer umumnya berupa bukti elektronik seperti log komunikasi, email, transaksi digital, dan metadata. Bukti ini sangat rentan terhadap penghapusan, modifikasi, atau hilangnya integritas data. Bahkan, waktu menjadi

faktor krusial karena semakin lambat penyitaan bukti, semakin besar kemungkinan bukti tersebut tidak dapat digunakan di pengadilan. Forensik digital membutuhkan keahlian khusus untuk menjaga *chain of custody* dan memastikan bukti tidak terkontaminasi.

DAFTAR PUSTAKA

Alamsyah, M. (2021). Kerjasama internasional dalam penanganan cybercrime. *Jurnal Hukum Internasional*, 18(1), 105–106.

APJII. (2022). *Survei penetrasi internet Indonesia 2022* (Bab IV, hlm. 77–78).

Ardiansyah, N. D., Gunawan, B. P., & Siswono, D. (2024). Penerapan UU ITE dalam penegakan hukum siber di Indonesia: Studi kasus pada Pasal 27 hingga Pasal 37. *Jurnal Reformasi Hukum: Cogito Ergo Sum*, 7(2), 17–22.

Asri, Sukirman, & Munawir. (2011). *Pengetahuan dasar komputer*. Makassar: YAPMA Makassar.

Fitriani, & Kunarto. (2017). Upaya kepolisian dalam penanggulangan tindak pidana penipuan terhadap calon pegawai negeri sipil (Studi Polres Lampung Utara). *Jurnal Hukum*. Retrieved from https://digilib.unila.ac.id

Handoyo, B., Husamuddin, M. Z., & Rahma, I. (2024). Tinjauan yuridis penegakan hukum kejahatan cyber crime studi implementasi Undang-Undang Nomor 11 Tahun 2008. *MAQASIDI: Jurnal Syariah dan Hukum*, 40–55.

INTERPOL. (2022). *Cybercrime: Typologies and response*. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

Kamran, M., & Maskun. (2021). Penipuan dalam jual beli online: Perspektif hukum telematika. *Balobe Law Journal*, 1(1), 41–56.

Kitab Undang-Undang Hukum Acara Pidana (KUHAP).

Kitab Undang-Undang Hukum Pidana (KUHP).

Nurhayati, E. (2022). Kekosongan hukum dalam penindakan penipuan digital berbasis investasi. *Jurnal Legislasi Indonesia*, 19(2), 201–202.

Rahayu, E. L. B., & Syam, N. (2021). Digitalisasi aktivitas jual beli di masyarakat: Perspektif teori perubahan sosial. *Ganaya: Jurnal Ilmu Sosial dan Humaniora*, 4(2), 672–685.

Southeast Asian Cybercrime Unit. (2023). *Cybercrime in ASEAN: 2023 threat report*. ASEANPOL.

Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Wahyuni, N. (2020). Tantangan penegakan hukum terhadap kejahatan siber di Indonesia. *Jurnal Hukum & Pembangunan*, 50(3), 354–367.

Wibowo, M. S. I., & Munawar, A. (2024). Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia. *Jurnal Hukum Lex Generalis*, 5(7).