INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 4 Tahun 2025 Page 342-355
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Penipuan Online Dengan Modus Social Engineering

Fuad Nur[1]✉
Fakultas Hukum, Universitas Halu Oleo
Email: fuadnur85@uho.ac.id[1]✉

Abstrak

Penelitian ini bertujuan untuk mengkaji pertanggungjawaban pidana terhadap pelaku tindak pidana penipuan online dengan modus social engineering dan juga tantangan dalam pembuktiannya. Metode penelitian yang digunakan adalah yuridis normatif dengan pendekatan perundang-undangan dan konseptual, menggunakan data sekunder berupa bahan hukum primer dan sekunder. Teknik pengumpulan data melalui studi kepustakaan yang dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa pelaku penipuan online dengan modus social engineering dapat dimintai pertanggungjawaban pidana berdasarkan Pasal 378 KUHP dan Pasal 28 ayat (1) juncto Pasal 45A ayat (1) UU ITE. Selain itu, pelaku penipuan online dapat juga dijerat pasal lainnya dalam UU ITE tergantung modus operandi, kekuatan alat bukti, tingkat kerugian dan kompleksitas teknis dari kejahatan tersebut. Pertanggungjawaban pidana didasarkan pada prinsip geen straf zonder schuld (tiada pidana tanpa kesalahan) yang mensyaratkan adanya unsur objektif (perbuatan melawan hukum) dan subjektif (kesalahan). Namun, dalam pembuktiannya menghadapi tantangan signifikan berupa ancaman pidana yang tidak proporsional dengan kerugian yang ditimbulkan, kompleksitas bukti digital yang mudah hilang dan memerlukan keahlian forensik khusus, kesulitan identifikasi pelaku yang menggunakan teknologi penyembunyian seperti VPN dan nomor telepon virtual, serta sifat transnasional kejahatan tersebut yang memperumit proses penegakan hukum.

Kata Kunci: *Pertanggungjawaban Pidana, Penipuan Online, Social Engineering*

Abstract

This study aims to examine the criminal liability of perpetrators of online fraud crimes using social engineering methods and the challenges in proving such cases. The research methodology employed is normative juridical with statutory and conceptual approaches, utilizing secondary data comprising primary and secondary legal materials. Data collection was conducted through literature review and analyzed qualitatively. The findings indicate that perpetrators of online fraud using social engineering methods can be held criminally liable under Article 378 of the Indonesian Criminal Code (KUHP) and Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) of the Electronic Information and Transactions Law (UU ITE). Additionally, online fraud perpetrators may also be subject to other provisions within the UU ITE, depending on the modus operandi, strength of evidence, degree of losses, and technical complexity of the crime. Criminal liability is based on the principle of geen straf zonder schuld (no crime without fault), which requires the presence of objective elements (unlawful acts) and subjective elements (fault). However, the evidentiary process faces significant challenges, including disproportionate criminal sanctions relative to the damages caused, complexity of digital evidence that can be easily lost and requires specialized forensic expertise, difficulties in identifying perpetrators who utilize concealment technologies such as VPNs and virtual phone numbers, and the transnational nature of such crimes that complicates law enforcement processes.

Keywords*: Criminal Liability, Online Fraud, Social Engineering*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan dalam berbagai aspek kehidupan masyarakat. Kemudahan akses informasi dan interkonektivitas global membuka peluang baru dalam berbagai bidang, namun juga menciptakan celah bagi munculnya berbagai bentuk kejahatan yang lebih kompleks. Salah satu bentuk kejahatan yang berkembang pesat di era digital adalah penipuan dengan modus social engineering.

Social engineering merupakan teknik manipulasi psikologis yang digunakan untuk mempengaruhi individu agar mengungkapkan informasi rahasia atau melakukan tindakan tertentu yang menguntungkan pelaku. Berbeda dengan serangan cyber konvensional yang memanfaatkan kelemahan teknis sistem keamanan, social engineering menargetkan faktor manusia sebagai titik lemah dalam sistem keamanan informasi. Melalui eksploitasi karakteristik dasar manusia seperti rasa percaya, keinginan untuk membantu, rasa takut, dan kecerobohan, pelaku kejahatan berhasil memperoleh akses ke informasi pribadi, keuangan, atau sistem yang seharusnya terlindungi.

Fenomena penipuan online dengan berbagai modus termasuk social engineering semakin marak di Indonesia. Berdasarkan data yang dihimpun dari telah Kementerian Komunikasi dan Digital dari 2017 hingga 2024 terdapat 405.000 laporan penipuan transaksi online (Nasional.sindonews.com., 2024). Adapun data dari Otoritas Jasa Keuangan (OJK) menunjukkan hingga 9 Februari 2025 ada 42.257 laporan penipuan dengan 40.936 di antaranya telah terverifikasi. Tercatat kerugian masyarakat mencapai Rp 700 miliar dalam tiga bulan terakhir akibat berbagai modus penipuan online (cnbcindonesia.com., 2025). Selain itu, data dari Patroli Siber Kepolisian Republik Indonesia, jumlah laporan kasus penipuan online di antaranya dengan modus social engineering mengalami peningkatan signifikan setiap tahunnya, bahkan di tahun 2025 tercatat 14.495 laporan penipuan online (patrolisiber.id., 2025).

Penipuan online melibatkan aktivitas tipu daya dengan media digital yang bertujuan mengelabui individu demi keuntungan finansial atau mendapatkan informasi pribadi yang sensitif. Pelaku sering menggunakan taktik seperti mengirim file APK ke ponsel android, email phishing dan situs web palsu, menyamar sebagai entitas yang dapat dipercaya untuk memperdaya pengguna memberikan detail yang rahasia atau social engineering (Patrolisiber.id., 2025). Sebagaimana yang dialami Sunarti pensiunan Aparatur Sipil Negara (ASN) di Magetan menjadi korban penipuan pada 27 Maret 2025. Uang tabungannya Sunarti di Bank Pembangunan Daerah (BPD) senilai Rp105 juta hilang setelah menerima telepon dan mengikuti instruksi penelpon yang mengaku sebagai petugas Taspen yang belakangan diketahui sebagai penipu (Batam.tribunnews.com., 2025).

Pada kasus lain, 24 Maret 2025. Direktorat Tindak Pidana Siber Bareskrim Polri berhasil mengungkap praktik penipuan online menggunakan short message service (SMS) blast dengan mencatut nama bank swata untuk kuras rekening nasabah. SMS blast merupakan metode pengiriman pesan kepada nomor seluler secara massal, biasanya dipakai untuk memasarkan produk atau informasi lainnya. Modus penipuan online ini terungkap setelah beberapa korban membuat laporan kepada Polda Metro Jaya. Berdasarkan penyelidikan awal, terdapat 12 nasabah bank yang tertipu karena mengklik link phising yang disiarkan menggunakan *SMS blast* tersebut dengan kerugian mencapai Rp 473 juta lebih (Tempo.co., 2025).

Penipuan online dengan modus social engineering ini sering kali digunakan pelakunya dalam kejahatan perbankan, di mana pelaku memanipulasi korbannya yang seolah-olah dari pihak bank. Dalam aksinya, pelaku kejahatan tersebut berpura-pura sebagai pegawai

bank untuk mendapatkan informasi pribadi korban, seperti kode OTP (One-Time Password) dan sebagainya (Nur, F., 2023). Kode OTP adalah kode keamanan akun yang digunakan untuk memverifikasi identitas pengguna saat mengakses atau melakukan transaksi pada platform online.

Penipuan online merupakan kejahatan yang dapat mengakibatkan kerugian bagi orang lain sebagaimana diatur pada Pasal 378 KUHP tentang penipuan sebagai lex generali (aturan umum), dan Pasal 28 ayat (1) UU ITE tentang penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik sebagai lex specialis (aturan khusus). Selain itu terdapat pasal lain dalam UU ITE yang dapat diterapkan pada pelaku penipuan onlie, seperti Pasal 32 jo. Pasal 48 UU ITE. Namun demikian penerapan pasal pada kasus penipuan online harus mempertimbangkan banyak hal, di antaranya modus operandi, kekuatan alat bukti, tingkat kerugian dan kompleksitas teknis dari kejahatan tersebut.

Meskipun kerangka hukum di atas telah memberikan landasan untuk penanganan kasus kejahatan siber, implementasinya di lapangan masih menghadapi berbagai tantangan (Widodo, 2021). Terlebih lagi pelaku kejahatan juga semakin lihai dalam memanfaatkan celah keamanan siber untuk melakukan aksi ilegal mereka (Arief, 2020). Hal tersebut diperparah dengan rendahnya literasi digital dan kesadaran masyarakat terhadap risiko kejahatan siber. Meskipun berdampak luas, penanganan kasus social engineering seringkali terkendala oleh kompleksitas pembuktian sehingga banyak laporan kasus penipuan online tidak diproses oleh penegak hukum.

Penelitian ini bertujuan untuk mengkaji secara mendalam bagaimana pertanggungjawaban pidana terhadap pelaku tindak pidana penipuan online dengan modus social engineering dan bagaimana tantangan dalam pembuktian tindak pidana penipuan online dengan modus social engineering.

METODE PENELITIAN

Jenis penelitian yang digunakan adalah penelitian yuridis normatif. Penelitian yuridis normatif yaitu penelitian yang dilakukan dengan cara mengkaji peraturan perundang-undangan yang berlaku atau diterapkan terhadap suatu permasalahan hukum tertentu. Adapun pendekatan yang digunakan adalah pendekatan perundang-undangan (statute approach) dan pendekatan konseptual (conceptual approach). Data yang digunakan adalah data sekunder yang terdiri dari bahan hukum primer dan bahan hukum sekunder. Bahan

hukum primer terdiri Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Informasi dan Transaksi Elektronik sebagaimana terakhir diubah dengan UU No. 1 Tahun 2024. Bahan hukum sekunder bersumber dari buku hukum dan jurnal hukum sebagai hasil penelitian. Teknik pengumpulan data yaitu dengan studi kepustakaan dan teknik analisis data yang digunakan adalah kualitatif yang mengkaji secara mendalam terkait pertanggungjawaban pidana terhadap pelaku penipuan online dengan modus social engineering.

HASIL DAN PEMBAHASAN

Analisis pertanggungjawaban pidana terhadap pelaku tindak pidana penipuan online dengan modus social engineering

Untuk mengatasi penyalahgunaan penggunaan media elektronik, maka pendekatan hukum digunakan untuk memperoleh kepastian hukum (Mewengkang, I. B., 2021). Pendekatan hukum digunakan dalam menangani kasus berkaitan dengan media elektronik sebagaimana halnya dengan penipuan online dengan modus social engineering di mana pelakunya dapat dimintai pertanggungjawaban pidana. Dalam hukum pidana Indonesia, konsep pertanggungjawaban pidana (criminal liability) dilandasi oleh prinsip geen straf zonder schuld atau tiada pidana tanpa kesalahan.

Pertanggungjawaban pidana (criminal liability) diartikan sebagai diteruskannya celaan yang objektif yang ada pada perbuatan pidana dan secara subjektif memenuhi syarat untuk dapat dipidana karena perbuatannya itu (Saleh, R., 1986). Celaan objektif adalah perbuatan yang dilakukan oleh seseorang tersebut merupakan perbuatan yang dilarang, baik menurut hukum formil maupun materil. Sedangkan celaan subjektif merujuk kepada orang yang melakukan perbuatan yang dilarang atau bertentangan dengan hukum. Seorang dapat dimintai pertanggungjawaban pidana tergantung pada dua hal (Martiman, P., 1997), yaitu:

a. Haruslah ada perbuatan yang bertentangan dengan hukum, atau harus ada unsur melawan hukum sebagai unsur obyektif.
b. Harus ada unsur kesalahan dalam bentuk kesengajaan atau kealpaan dari pelakunya sehingga perbuatannya dapat dipertanggungjawabkan. Unsur ini sebagai unsur subjektif.

Kaitannya dengan penipuan online, pelaku dapat dimintai pertanggungjawaban pidana berdasarkan Pasal 378 Kitab Undang-Undang Hukum Pidana (KUHP) dan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU No. 1 Tahun 2024 tentang Perubahan Kedua atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Selain untuk menindak

pelaku kejahatan penipuan online, UU ITE ini diterbitkan bertujuan pula untuk memberi perlindungan terhadap masyarakat dari kejahatan dalam dunia mayantara serta mencegah masyarakat berperan negatif dalam dunia elektronik (Sumadiyasa, I. K. A., 2021).

Dalam konteks teknologi dan cyber security, social engineering adalah teknik yang digunakan untuk mengelabui pengguna sehingga mereka mengungkapkan informasi pribadi atau rahasia, seperti password atau nomor kartu kredit, atau menginstal perangkat lunak berbahaya yang mengakses komputer mereka (Wicaksono, S. R., 2024). Oleh karena itu, penipuan online dengan modus social engineering dapat pula diidentifikasi dari unsur-unsur penipuan konvensional sebagaimana diatur dalam Pasal 378 KUHP sebagai lex generali (aturan umum), yaitu adanya rangkaian kebohongan, tipu muslihat, atau nama palsu yang digunakan untuk menguntungkan diri sendiri atau orang lain secara melawan hukum.

Bentuk social engineering dalam konteks perbankan seperti yang dijelaskan pada pendahuluan di mana pelaku berpura-pura sebagai pegawai bank untuk mendapatkan kode OTP menunjukkan adanya transformasi modus penipuan konvensional ke ranah digital. Hal ini memerlukan interpretasi hukum yang progresif untuk memastikan bahwa tindakan tersebut dapat dijerat dengan ketentuan hukum yang ada, mengingat KUHP disusun jauh sebelum era teknologi informasi. Oleh karena itu penggunaan UU ITE dapat berfungsi sebagai lex specialis (aturan khusus) dalam penanganan kasus penipuan online, terutama dalam hal penyebaran berita bohong dan penipuan yang terjadi dalam transaksi elektronik. Khususnya pada Pasal 28 ayat (1) dan pasal terkait lainnya dalam UU ITE, mengatur tindakan yang melanggar hukum dalam konteks digital, termasuk penipuan yang memanfaatkan teknologi informasi. Penggunaan aturan yang khsusus ini, memungkinkan penanganan kasus penipuan online tersebut dapat lebih spesifik, mengingat modus dan karakteristik kejahatan yang berbeda dibandingkan penipuan konvensional.

Untuk mengkualifikasikan *social engineering* yang digunakan pelaku untuk melakukan tindak pidana penipuan, perlu dilakukan analisis terhadap unsur-unsur yang terkandung dalam perbuatan tersebut. Bunyi Pasal 378 KUHP tentang tindak pidana penipuan adalah:

"Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun".

Berdasarkan pasal di atas R. Sugandhi (1980) mengemukakan pengertian penipuan yaitu tindakan seseorang dengan tipu muslihat, rangkaian kebohongan, nama palsu dan keadaan palsu dengan maksud menguntungkan diri sendiri dengan tiada hak. Rangkaian kebohongan ialah susunan kalimat-kalimat bohong yang tersusun sedemikian rupa yang merupakan cerita sesuatu yang seakan-akan benar. Adapun menurut R. Soesilo (1995) bahwa kejahatan pada Pasal 378 KUHP dinamakan penipuan, yang mana penipu itu pekerjaannya:

1. Membujuk orang supaya memberikan barang, membuat utang atau menghapuskan piutang,
2. Maksud pembujukan itu ialah hendak menguntungkan diri sendiri atau orang lain dengan melawan hak,
3. Membujuknya itu dengan memakai nama palsu atau keadaan palsu, akal cerdik (tipu muslihat), atau karangan perkataan bohong.

Adapun unsur-unsur penipuan kaitannya dengan modus social engineering adalah

1. Adanya maksud untuk menguntungkan diri sendiri atau orang lain.

Social engineering jelas memenuhi unsur ini karena pelaku bertujuan memperoleh keuntungan finansial atau akses ke informasi berharga yang dapat dimonetisasi atau diubah menjadi uang atau keuntungan lainnya.

2. Secara melawan hukum.

Tindakan manipulasi psikologis yang dilakukan pelaku penipuan untuk memperoleh informasi pribadi tanpa persetujuan yang sah merupakan perbuatan melawan hukum.

3. Menggunakan nama palsu atau martabat palsu, tipu muslihat, atau rangkaian kata kebohongan.

Dalam kasus penipuan dengan modus social engineering, pelaku sering menyamar sebagai pihak resmi (misalnya pegawai bank) atau menggunakan berbagai narasi bohong untuk membangun kepercayaan korban.

4. Menggerakkan orang lain untuk menyerahkan barang atau memberikan hutang atau menghapuskan piutang

Dalam konteks digital, barang dapat diinterpretasikan secara luas mencakup informasi pribadi, kode OTP (One-Time Password), atau akses ke rekening digital milik korban.

Seseorang baru dapat dikatakan telah melakukan tindak penipuan sebagaimana dimaksud di dalam Pasal 378 KUHP, apabila unsur-unsur yang disebut di dalam Pasal 378 KUHP terpenuhi, maka pelaku tindak pidana penipuan tersebut dapat dijatuhi pidana sesuai

perbuatannya (Mulyadi, D., 2017). Selain diatur dalam Pasal 378 KUHP, UU ITE telah memberikan perluasan lingkup dari tindak pidana penipuan ke ranah digital. Pasal 28 ayat (1) UU ITE mengatur tentang larangan penyebaran berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

Adapun unsur-unsur tindak pidana sebagaimana diatur dalam Pasal 28 ayat (1) UU ITE yang berbunyi "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik." Dari rumusan pasal tersebut, terdapat beberapa unsur penting, yaitu:

a. Unsur subjektif, yaitu dengan sengaja (dolus/kesengajaan).
b. Unsur melawan hukum, yaitu tanpa hak.
c. Adanya perbuatan yang dilarang, berupa menyebarkan berita bohong dan menyesatkan.
d. Adanya akibat yang ditimbulkan dari perbuatannya, yaitu mengakibatkan kerugian konsumen dalam Transaksi Elektronik.

Adapun sanksi pidana sebagaimana dimaksud dalam Pasal 28 ayat (1) UU ITE dapat dilihat dalam Pasal 45A ayat (1) UU ITE, yaitu:

"Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)."

Sebagai analisis pertanggungjawaban pidana pada penipuan online dengan modus social engineering adalah sebagai berikut:

1. Kesengajaan

Adanya kesengajaan yang menghendaki pelaku untuk mewujudkan suatu perbuatan pidana. Kesengajaan merupakan salah satu bentuk mens rea (sikap batin pelaku) yang paling umum dijadikan dasar pembuktian dalam kasus pidana. Pelaku penipuan online dengan modus social engineering dapat dipertanggungjawabkan secara pidana jika terbukti memiliki niat atau adanya kesengajaan untuk melakukan tindak pidana. Adapun kesengajaan dalam kasus ini dapat mencakup:

a. Kesengajaan sebagai maksud: Pelaku memiliki tujuan khusus untuk menipu korban melalui media atau transaksi elektronik.
b. Kesengajaan sebagai kepastian: Pelaku mengetahui bahwa perbuatannya pasti akan menimbulkan kerugian terhadap korbannya.

c. Kesengajaan sebagai kemungkinan: Pelaku menyadari betul adanya risiko dari perbuatannya yang dapat menyebabkan kerugian terhadap korbannya.

2. Tanpa Hak

Adapun unsur tanpa hak menunjukkan bahwa pelaku tidak memiliki kewenangan hukum untuk menyebarkan informasi palsu, terlebih lagi dalam memanipulasi korbannya untuk memberikan informasi pribadi. Dalam konteks penipuan online, unsur ini terpenuhi ketika pelaku:

a. Menggunakan identitas palsu,
b. Menyebarkan informasi palsu seolah-olah dari otoritas tertentu untuk memanipulasi psikologis korbannya,
c. Memberikan keterangan palsu tentang produk atau jasa yang tidak dimilikinya.

3. Menyebarkan Berita Bohong dan Menyesatkan

Perbuatan menyebarkan berita bohong tidak diartikan secara umum, melainkan penyebaran berita bohong dalam konteks transaksi elektronik yang berakibat korbannya keliru atau salah dalam mengambil keputusan sehingga mengalami kerugian.

4. Kerugian Konsumen dalam Transaksi Elektronik

Kerugian di sini tidak sebatas pada kerugiaan materiil, namun dapat juga mencakup kerugian immateriil. Sehingga pertanggungjawaban pidana terhadap pelaku penipuan online dengan modus social engineering dapat diterapkan jika dapat dibuktikan adanya kerugian yang dialami korban (konsumen) sebagai akibat langsung dari berita bohong dan menyesatkan yang disebarkan pelaku melalui media elektronik seperti telepon, media sosial, aplikasi digital, email, situs dan lainnya.

Selain pelaku penipuan online dapat dijerat dengan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE, pelaku juga dapat dijerat dengan pasal lainnya dalam UU ITE seperti Pasal 32 jo. Pasal 48 UU ITE. Namun demikian, penerapan pasal pemidanaan dalam UU ITE terkait kasus penipuan online tentunya harus mempertimbangkan banyak hal, seperti modus operandi, kekuatan alat bukti, tingkat kerugian dan kompleksitas teknis dari kejahatan tersebut. Hal ini dapat mempengaruhi pembuktian di pengadilan.

Dalam sistem peradilan pidana (criminal justice system), pertanggungjawaban pidana merupakan konsep fundamental yang memiliki hubungan yang signifikan terhadap penegakan hukum, khususnya dalam konteks kasus penipuan online. Penegak hukum mencari kebenaran materiil guna menghindari adanya kekeliruan dalam menjatuhkan putusan pidana terhadap seseorang. Hal tersebut sebagaimana diatur dalam Pasal 6 angka

2 UU No. 48 Tahun 2009 tentang Kekuasaan Kehakiman yang menegaskan bahwa "tidak seorang pun dapat dijatuhi pidana, kecuali apabila pengadilan karena alat pembuktian yang sah menurut undang-undang, mendapat keyakinan bahwa seseorang yang dianggap dapat bertanggung jawab, telah bersalah atas perbuatan yang didakwakan atas dirinya" (Nur, F., 2023). Olehnya itu, pertanggungjawaban pidana memastikan bahwa hukuman pidana dijatuhkan hanya kepada mereka yang benar-benar layak dipersalahkan (culpabilitas) baik itu karena kesengajaan (dolus) maupun karena kealpaan (culpa).

Tantangan dalam Pembuktian Tindak Pidana Penipuan Online dengan Modus Social Engineering

Kerangka hukum pidana Indonesia, khususnya KUHP dan UU ITE, merupakan instrumen untuk menindak pelaku penipuan online dengan modus social engineering. Namun, terdapat beberapa keterbatasan yang signifikan:

1. Ancaman pidana yang tidak proporsional

Pasal 378 KUHP menetapkan ancaman pidana maksimal 4 tahun penjara untuk tindak pidana penipuan, sementara Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE menetapkan ancaman pidana maksimal 6 tahun penjara dan/atau denda maksimal Rp1 miliar. Adapun pidana penjara maksimal dalam KUHP dan UU ITE dinilai tidak proporsional dengan kerugian yang ditimbulkan dari penipuan dengan modus social engineering. Dampak yang ditimbulkan bisa saja bernilai miliaran rupiah, belum lagi dampak buruk lainnya terhadap korban.

2. Kompleksitas Bukti Digital

Bukti pada penipuan dalam dunia digital khususnya dengan modus social engineering dapat dengan mudah hilang. Sehingga bukti berupa rekaman panggilan telepon atau pesan teks transaksi online memerlukan penanganan khusus. Dalam proses pengumpulan dan analisis bukti digital memerlukan keahlian khusus yaitu keahlian digital forensik yang tidak selalu tersedia di kantor Kepolisian di berbagai daerah di Indonesia.

3. Identifikasi Pelaku

Pelaku social engineering sering menggunakan identitas palsu dan memanfaatkan berbagai teknologi, seperti penggunaan VPN atau Jaringan Pribadi Virtual (Virtual Private Network) membuat koneksi jaringan privat di antara beberapa perangkat melalui internet. Selain itu, pelaku menggunakan nomor telepon virtual (virtual phone number) yang merupakan nomor telepon yang tidak terikat pada kartu atau perangkat pada umumnya.

Dengan nomor telepon virtual tersebut, seseorang dapat memiliki nomor telepon dengan kode area atau negara yang berbeda dari lokasi orang tersebut berada (Miitel.com., 2024). Hal ini akan menyulitkan pelacakan identitas asli pelaku kejahatan tersebut. Diperparah lagi dengan sifat lintas batas (transnasional) dari kejahatan siber yang membuat proses penegakan hukum menjadi lebih rumit karena melibatkan yurisdiksi berbeda. Karena pada banyak kasus antara pelaku dan korban berada di wilayah yang berbeda.

Seiring dengan peningkatan ancaman dari social engineering, maka kebutuhan terhadap regulasi dan kebijakan yang memberi perlindungan terhadap data seseorang dan korporasi. Begitu pula sanksi pidana yang lebih keras untuk kejahatan ini, atau regulasi yang lebih ketat tentang bagaimana data dapat dikumpulkan dan digunakan (Wicaksono, S. R., 2024). Terdapat pula tantangan dalam penegakan hukum terutama berkaitan dengan pemenuhan unsur-unsur tindak pidana dan pertanggungjawaban pidana pelaku. Penegak hukum harus mampu mengumpulkan, menganalisis, dan menghadirkan bukti digital yang dapat diterima di pengadilan (Aini, N., 2024). Olehnya itu, tantangan pembuktian tindak pidana tersebut memerlukan transformasi mendasar dalam pendekatan investigasi dan pembuktian terutama di era digital terlebih lagi pelaku kejahatan tersebut memiliki keahlian dalam memanipulasi psikologis korbannya melalui media digital. Hal ini menjadi tantangan bagi penegakan hukum yang harus mampu mengumpulkan, menganalisis, dan menghadirkan bukti digital yang dapat diterima di pengadilan (Aini, N., 2024). Sehingga menjadi hal penting pula penguatan keahlian secara teknis di bidang digital forensik bagi penegak hukum.

Keharusan penegak hukum membuktikan tindak pidana penipuan online tersebut karena memiliki karakteristik yang berbeda dengan penipuan konvensional sebagaimana diatur dalam KUHP, seperti kemampuan membuktikan adanya tipu muslihat dan rangkaian kebohongan yang disengaja harus harus dapat diterjemahkan ke dalam konteks digital yang sering kali tidak meninggalkan jejak fisik. Ketika pelaku social engineering menggunakan teknik manipulasi psikologis korbannya dengan cara berpura-pura menjadi orang lain atau pada teknik phishing yang memancing korbannya memberikan informasi pribadi dan rahasia. Begitu pula kemampuan membuktikan adanya unsur mens rea (niat jahat) pelaku penipuan online. Olehnya itu, keberhasilan pembuktian pada tindak pidana penipuan online dengan modus social engineering bergantung pada kemampuan penegak hukum.

SIMPULAN

Penelitian ini menunjukkan bahwa pelaku penipuan online dengan modus social engineering dapat dimintai pertanggungjawaban pidana berdasarkan Pasal 378 KUHP dan Pasal 28 ayat (1) jo. Pasal 45A ayat (1) UU ITE. Selain itu, pelaku penipuan online dapat juga dijerat pasal lainnya dalam UU ITE tergantung modus operandi, kekuatan alat bukti, tingkat kerugian dan kompleksitas teknis dari kejahatan tersebut. Penipuan online dengan social engineering dapat memenuhi unsur-unsur penipuan, yaitu adanya maksud menguntungkan diri sendiri secara melawan hukum melalui tipu muslihat dan rangkaian kebohongan untuk menggerakkan korban menyerahkan informasi pribadi yang mengakibatkan kerugian terhadap korbannya. Adapun pertanggungjawaban pidana didasarkan pada prinsip geen straf zonder schuld (tiada pidana tanpa kesalahan) yang mensyaratkan adanya unsur objektif (perbuatan melawan hukum) dan subjektif (kesalahan). Namun, pembuktian tindak pidana ini menghadapi tantangan seperti keterbatasan regulasi berupa ancaman pidana yang tidak proporsional dengan kerugian miliaran rupiah yang dapat ditimbulkan, kompleksitas bukti digital yang mudah hilang dan memerlukan keahlian forensik khusus, serta kesulitan identifikasi pelaku yang menggunakan identitas palsu dan teknologi penyembunyian seperti VPN dan sejenisnya. Begitu pula kejahatan ini sifat transnasional yang dapat memperumit proses penegakan hukum karena melibatkan yurisdiksi berbeda.

DAFTAR PUSTAKA

Aini, N., & Lubis, F. (2024). Tantangan Pembuktian Dalam Kasus Kejahatan Siber. Judge: Jurnal Hukum, 5(02), 55-63.

Arief, B. N. (2020). Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan Siber. Jurnal Hukum Ius Quia Iustum, 27(1), 1-22.

Batam.tribunnews.com. (2025). https://batam.tribunnews.com/2025/04/03/pensiunan-asn-di-magetan-kehilangan-uang-rp-105-juta-di-tabungan-usai-terima-telepon

Cnbcindonesia.com. (2025) https://www.cnbcindonesia.com/tech/20250312130545-37-617912/marak-penipuan-online-bri-minta-waspadai-5-modus-ini

Marbun, R., & Ariani, M. (2022). Melacak Mens Rea Dalam Penyebaran Berita Bohong Melalui WhatsApp Group: Mengenal Sekilas Psikolinguistik Dalam Hukum Pidana. Jurnal Hukum Pidana Dan Kriminologi, 3(2), 72-85.a

Martiman, P. (1997). Memahami dasar-dasar hukum pidana Indonesia, PT Pradnya Paramita, Jakarta.

Mewengkang, I. B. (2021). Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya. Lex Crimen, 10(5). Mewengkang, I. B. (2021). Kajian Yuridis Cyber Crime Penanggulangan Dan Penegakan Hukumnya. Lex Crimen, 10(5).

Miitel.com. (2024) https://miitel.com/id/apa-itu-virtual-phone-number-dan-4-fungsi-bisnisnya

Mulyadi, D. (2017). Unsur-Unsur Penipuan Dalam Pasal 378 KUHP Dikaitkan Dengan Jual Beli Tanah. Jurnal Ilmiah Galuh Justisi, 5(2), 206-223.

Nasional.sindonews.com. (2024) https://nasional.sindonews.com/read/1419745/13/kemenkominfo-catat-405000-laporan-penipuan-transaksi-online-sepanjang-2017-2024-1721524077?showpage=all

Nur, F. (2023). Penegakan Hukum terhadap Kejahatan Digital Perbankan. Innovative: Journal Of Social Science Research, 3(6), 3234-3249.

Nur, F., & Sirjon, L. (2023). Akses Keadilan Bagi Korban Tindak Pidana Dalam Perspektif Hak Asasi Manusia. Innovative: Journal Of Social Science Research, 3(5), 7588-7603.

Patrolisiber.id. (2025). https://patrolisiber.id/about-us/

R. Soesilo. (1995). Kitab Undang-Undang Hukum Pidana (KUHP) Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal, Politeia, Bogor.

R. Sugandhi. (1980). Kitab Undang-Undang Hukum Pidana dengan Penjelasannya, Usaha Nasional, Surabaya.

Saleh, R. (1986). Pikiran-Pikiran Tentang Pertanggungjawaban Pidana, Ghalia Indonesia, Jakarta.

Sumadiyasa, I. K. A., Sugiartha, I. N. G., & Widyantara, I. M. M. (2021). Pertanggungjawaban Pidana Pelaku Cyber Crime Dengan Konten Pornogafi. Jurnal Interpretasi Hukum, 2(2), 372-377.

Tempo.co. (2025) https://www.tempo.co/hukum/modus-penipuan-online-lewat-sms-blast-catut-nama-bank-untuk-kuras-rekening-nasabah-1223705

Wicaksono, S. R. 2024, Social Engineering: Konsep Dasar dan Perkembangan, Seribu Bintang, Malang, Jawa Timur.

Zulfadli, M., Abdullah, K., & Nur, F. (2017). Penegakan hukum yang responsif dan Berkeadilan Sebagai Instrumen Perubahan Sosial Untuk Membentuk Karakter Bangsa. In Prosiding Seminar Nasional Himpunan Sarjana Ilmu-ilmu Sosial (Vol. 2, pp. 265-284).