

Analisis Penipuan Online Melalui Media Sosial Dalam Kasus Kejahatan Belanja Online di Wilayah Jawa Timur

Marselinus Goa¹, Hudi Yusuf²

^{1,2} Universitas Bung Karno, Jakarta
e-mail: marselinusgoa@gmail.com

Abstrak: Tindakan penipuan yang bersifat konvensional diatur secara rinci di dalam KUHP berikut dengan ancaman hukumannya. Namun, pada zaman modern saat ini, tindakan penipuan berkembang yang sebelumnya bersifat konvensional, menjadi dapat dilakukan dengan menggunakan teknologi atau biasa disebut secara daring atau online. Pendekatan penelitian menggunakan penelitian kualitatif dengan jenis penelitian empiris. Analisis ini bertujuan untuk menganalisis modus serta faktor penyebab terjadinya penipuan jual beli melalui sarana e-commerce serta untuk menganalisis penanganan tindak pidana penipuan jual beli online serta kendala yang terjadi dalam proses penegakan hukumnya. Kepustakaan penelitian ini menggunakan konsep tindak pidana, konsep penipuan, ketentuan pidana dalam UU ITE, teori kejahatan, pembuktian dalam perkara pidana serta kebijakan penanggulangan tindak pidana. Modus yang digunakan pelaku penipuan jual beli online adalah dengan mengajak pembeli bertransaksi di luar marketplace resmi, berpura-pura mengatasnamakan merchant online, meminta OTP korban, penipu berpura-pura dari bea cukai dan meminta tambahan pembayaran pada korbannya, penipu mengirimkan barang secara COD dan kurir meminta pembayaran pada korbannya dan tentunya barang tersebut tidak sesuai dengan deskripsinya. Adapun penyebab terjadinya penipuan jual beli online lebih dikarenakan oleh kultur budaya masyarakat, belum tersertifikasinya secara menyeluruh setiap proses jual beli melalui media sosial ataupun online, faktor ekonomi, pencarian jati diri serta minimnya resiko tertangkap yang menyebabkan penipuan online marak terjadi. Upaya pencegahan terjadinya penipuan online, yaitu perlu adanya peningkatan serta perbaikan profesionalitas dan integritas dari aparat penegak hukum dalam menangani kasus kejahatan penipuan online yang marak terjadi di masyarakat. Hal tersebut dilakukan supaya adanya kepastian hukum dan jaminan perlindungan bagi masyarakat.

Article History

Received: July 05, 2025

Revised: July 21, 2025

Published: July 23, 2025

Kata Kunci:

Penipuan online, media sosial, belanja online, Jawa Timur



<https://doi.org/10.5281/zenodo.16351523>

This is an open-access article under the [CC-BY-SA License](#).



PENDAHUUAN

Kejahatan penipuan merupakan kejahatan yang sering terjadi di tengah masyarakat Indonesia yang bahkan hampir setiap harinya terjadi. Terjadinya kejahatan penipuan tidak mengenal status sosial, agama, ras, jenis kelamin, artinya kejahatan ini terjadi dan dilakukan oleh siapa saja dan pada siapa saja dan kapan saja. Pelaku penipuan ini selalu menggunakan cara/modus baru untuk menipu korbannya, sehingga perbuatan penipuan yang dilakukan tidak disadari oleh korbannya. Korban kejahatan akan tersadar apabila perbuatan kejahatan telah dilakukan.

Dalam perspektif kriminologi, kejahatan penipuan ini termasuk dalam kejahatan yang selalu berulang terjadi. Hal ini memperlihatkan bahwa penanganan dan penegakan hukum terhadap para pelaku kejahatan penipuan masih belum mencapai sasaran. Artinya, tujuan pemidanaan hukum pidana nasional belum tercapai.

Pada era teknologi modern seperti saat ini, kemudahan dalam melakukan transaksi jual-beli semakin terwujud, terutama berkat kehadiran internet yang membuat proses tersebut menjadi lebih praktis dan efisien. Proses jual-beli melalui internet dikenal sebagai Electronic Commerce (ECommerce), yang mencakup berbagai fasilitas seperti media transaksi, pemesanan, pengiriman, dan pembayaran barang.

E – commerce hadir sebagai opsi yang menarik untuk perkembangan bisnis saat ini karena memberikan sejumlah keuntungan bagi penjual maupun pembeli. Salah satu keuntungan tersebut adalah bahwa transaksi antara kedua belah pihak tidak memerlukan pertemuan langsung, sehingga memberikan fleksibilitas dalam proses produksi dan mempercepat proses tawar-menawar harga serta pengiriman barang. Namun dibalik kemudahan yang ditawarkan oleh kemajuan teknologi tersebut, memiliki segudang resiko yang cukup besar di dalamnya. Seperti halnya kejahatan – kejahatan yang terjadi di dunia maya, baik di lakukan secara langsung di dalamnya atau hanya sekedar menjadikan internet sebagai media perantaranya, yang kerap kali disebut sebagai cyber crime. Di ranah digital, kejahatan yang sering terjadi umumnya terkait penipuan yang mengaku sebagai bisnis jual-beli oleh toko atau penjual yang menawarkan harga barang mereka jauh di bawah harga pasar.

Penipuan online seperti Jual beli online yang dapat diterima dengan baik oleh masyarakat, karena jika menggunakan fasilitas di market place maka pembeli dapat dengan mudah memilih-milih barang, melihat review dari pembeli sebelumnya serta tidak perlu ke lokasi penjual untuk membeli barang. Hanya tinggal memilih barang yang diinginkan kemudian uang di transfer kepada penyedia market place-nya menggunakan rekening bersama yang kemudian oleh market place tersebut si penjual diberikan notifikasi untuk segera mengirimkan barangnya yang mana setelah pembeli menerima barangnya dan sesuai dengan deskripsi yang dijual maka pembeli segera melakukan konfirmasi penerimaan barang yang kemudian oleh market place uang dari pembeli tersebut ditransferkan pada penjual.

Market place merupakan salah satu model-model bentuk e-commerce atau transaksi jual beli online. Untuk di Indonesia sendiri bentuk e-commerce terdiri dari beberapa model, yaitu:

- E-Retail - Toko online dengan alamat website (domain) sendiri dimana penjual memiliki stok produk/ jasa dan menjualnya secara online. Contoh: Blibli.com, Lazada.co.id, Tiket.com,dll.
- Iklan Baris Online - Merupakan situs iklan baris, di mana situs yang bersangkutan tidak memfasilitasi kegiatan transaksi online. Contoh: Kaskus, OLX.co.id.
- Market Place - Model bisnis seperti ini merupakan website yang tidak hanya membantu mengiklankan barang dagangan saja, tetapi juga memfasilitasi transaksi uang secara online untuk para pedagang online. Contoh: Shopee.com, Tokopedia, Bukalapak.com.

Situs-situs jual beli online yang ada membuat arus jual beli online menjadi tujuan utama dari beberapa pembeli. Banyaknya manfaat dari jual beli online ternyata memiliki risiko yang menimbulkan kekhawatiran bagi para pelaku jual beli online. Risiko ini muncul karena transaksi antara penjual dan pembeli dilakukan tanpa melalui face to face, tetapi melalui media internet (dunia maya) yang seringkali sulit dilacak keberadaannya. Oleh karena itu, risiko yang paling umum terjadi adalah terkait dengan masalah keamanan, penipuan dan ketidakpuasan karena barang yang ditampilkan secara online tidak sama dengan yang diterima saat dikirimkan.

Kasus-kasus penipuan jual beli online yang terjadi saat ini paling banyak mendapat sorotan adalah kasus penipuan pembelian barang secara online. Salah satu kasus penipuan pembelian jual beli online adalah yang dialami oleh salah satu putra dari Presiden Joko Widodo yakni Kaesang Pangarep yang membagikan pengalamannya hendak ditipu akun Instagram dengan user name @luckycatsauction. Oleh Bareskrim Polri pelaku telah dibekuk yang mana penipuan online tersebut dilakukan dengan modus pelelangan barang di Instagram yang mencapai nilai jutaan rupiah.

Pada kasus-kasus yang sering terjadi, modus operandi yang sering dilakukan pelaku penipuan jula beli online antara lain :

- Sosial engineering, pelaku melakukan profile calon korban, mulai dari nomor hp korban, rekening bank, media sosial, akun e-commerce, dan kebiasaan-kebiasaan yang dilakukan

korban setiap hari. Sosial engineering sendiri adalah cara mendapatkan identitas korban tanpa diketahui karena pelaku juga ikut bersama dalam aktifitas yang sering dilakukan oleh calon korban.

- Membajak akun media sosial, akun bank atau whatsapp yang dimiliki oleh korban, kemudian pelaku mengambil alih dan mengubah password, mengambil manfaat dari seluruh akun yg sdh di ambil alih.
- Pelaku membuat akun facebook / Instagram baru atau membobol akun media sosial milik orang lain kemudian menambah pertemanan hingga ribuan orang. Kemudian pelaku menawarkan barang-barang elektronik dengan harga murah. Untuk meyakinkan korbannya, pelaku mengaku sebagai bagian marketing dan berusaha meyakinkan bahwa barang akan dikirim melalui kurir semisal TIKI JNE, JNT, dll. Apabila uang muka / down payment (DP) sudah dikirim ke rekening pelaku, maka seolah-olah ada yang menelepon korban mengaku sebagai bagian pengiriman barang dan mengatakan bahwa barang sudah dikirim. Untuk meyakinkan korbannya, pelaku mengiririnkan resi pengiriman. Keesokan harinya korban mendapat telepon mengaku bagian pengiriman dan menginformasikan bahwa telah terjadi kelebihan jumlah item yang dikirimkan dan mengharuskan korban untuk membayar saja kelebihan barang yang dikirimkan tersebut dengan iming-iring diberikan diskon karena hal tersebut adalah kesalahan bagian pengiriman. Korban pun banyak yang tergiur dengan penawaran pelaku kemudian dengan mudahnya mentransfer uang ke rekening pelaku.

Dari beberapa contoh kasus di atas menunjukkan bahwa sangatlah mudah untuk para pelaku tindak pidana untuk melakukan penipuan jual beli online dalam jejaring sosial. Secara aturan perundangan pada dasarnya untuk menanggulangi kasus-kasus tersebut pada tanggal 21 April 2008, telah diundangkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. UU 11 Tahun 2008 ini kemudian diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disebut dengan UU ITE). Diundangkannya UU ITE menunjukkan bahwa bangsa Indonesia, tidak ingin ketinggalan dalam kancah perkembangan teknologi informasi, khususnya dalam rangka mencegah penyalahgunaan pemanfaatan teknologi informasi. Terkait dengan pencegahan ini, dalam UU ITE, telah diatur tentang perbuatan-perbuatan apa saja yang dilarang dan juga ancaman sanksi pidana bagi siapa saja yang melanggar larangan tersebut.

Dengan demikian, berdasarkan latar belakang masalah di atas, peneliti tertarik untuk mengkaji serta melakukan penelitian terhadap macam-macam bentuk konkret penipuan online di media sosial serta regulasi hukum yang berlaku di Indonesia mengenai penipuan online melalui media sosial dan tindakan represif serta preventif dalam meminimalisir terjadinya penipuan online melalui media sosial dengan judul penelitian Analisis Penipuan Online Melalui Media Sosial dalam Perspektif Kriminologi.

METODE

Metode penelitian dalam kasus ini menggunakan metode penelitian kualitatif yang bersifat empiris, dimana Metode penelitian empiris adalah pendekatan penelitian yang mengandalkan data dari pengalaman pengamatan, atau eksperimen untuk menghasilkan pengetahuan dan pemahaman. Penelitian ini berfokus pada fakta-fakta yang dapat diamati dan diukur, bukan pada teori atau spekulasi semata.

- **Dasar Penelitian:**
Penelitian empiris didasarkan pada prinsip empirisme, yaitu filsafat yang menekankan pengalaman sebagai sumber utama pengetahuan.
- **Pengumpulan Data:**
Data dalam penelitian empiris diperoleh melalui berbagai metode, seperti observasi langsung, wawancara, eksperimen, dan survei.

- **Tujuan:**

Tujuan utama penelitian empiris adalah untuk menguji hipotesis, mengembangkan teori baru, atau memberikan pemahaman lebih mendalam tentang fenomena yang diteliti.

HASIL DAN PEMBAHASAN

Modus Penipuan Jual Beli Melalui Sarana Ecommerce

Tindak pidana siber merupakan tindakan tindak pidana yang berhubungan dan berkaitan dengan dunia maya dan tindakan tindak pidana yang menggunakan komputer. Bila seseorang menggunakan komputer atau bagian dari jaringan komputer secara menyalahi Undang-Undang maka tindakan tersebut sudah tergolong pada tindak pidana siber. Indonesia tidak memiliki definisi hukum untuk kejahatan siber. Sebenarnya, Undang-Undang Nomor 11 Tahun 2008 sebagai amandemen dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang administratif. Namun, legislator memasukkan beberapa ketentuan tentang tindak pidana.

Definisi kejahatan siber dapat disimpulkan dari artikel tentang kejahatan tersebut. Anatomi kejahatan siber berdasarkan UU ITE dapat dibagi menjadi dua kelompok. Pertama, kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Di bawah Undang-Undang Informasi dan Transaksi Elektronik, ada tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Kejahatan-kejahatan tersebut dianggap sebagai kejahatan kontemporer yang menghasilkan bentuk kejahatan baru.

Kelompok kedua adalah konten ilegal dengan menggunakan internet, komputer dan teknologi terkait untuk melakukan kejahatan. Di bawah UU ITE, ada tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Kejahatan ini terkait dengan publikasi dan distribusi konten ilegal. Tidak seperti kelompok pertama yang menganggap bentuk kejahatan baru, kelompok kedua dianggap sebagai kejahatan lama, tetapi perkembangan teknologi telah menciptakan media baru untuk memberikan kebebasan berekspresi. Oleh karena itu, legislator mengatur ulang kejahatan dalam Undang-Undang Informasi dan Transaksi Elektronik. Sebenarnya, semua jenis kejahatan ini sudah diatur dalam tindakan kriminal lainnya dan ini menciptakan apa yang disebut Douglas Huzak sebagai kriminalisasi berlebihan.

Terkait kejahatan Siber, institusi Polri telah melakukan antisipasi sejak dua puluh tahun yang lalu, yang mana pada Tahun 2002 Polri membentuk Subdit IT dan Cyber Crime berdasarkan Surat Keputusan Kapolri Nomor 53 dan 54 tahun 2002, yang saat itu bernama Unit Cyber Crime, dipimpin seorang Pamen berpangkat Komisaris Polisi, dan berada dibawah Direktorat Tindak Pidana Ekonomi dan Khusus Bareskrim Polri. Nomenklatur ini kemudian diubah berdasarkan Perkap Nomor 21 Tahun 2010 tentang Susunan Organisasi Dan Tata Kerja pada tingkat Markas Besar Kepolisian Negara Republik Indonesia dan Perkap Nomor 22 Tahun 2010 tentang Susunan Organisasi Dan Tata Kerja Pada Tingkat Kepolisian Daerah, menjadi Subdirektorat IT dan Cyber Crime Dit Tipideksus Bareskrim Polri.

Untuk di tingkat Kepolisian Daerah khususnya Kepolisian Daerah Jawa Timur, struktur organisasi cyber crime di Polda Jawa Timur statusnya pada leveling Subdirektorat, artinya kedudukan struktur organisasi cyber crime dibawah kendali Direktorat Kriminal Khusus (Krimsus) sebagai Subdit V. Kepala Subdit V cyber crime membawahi 4 Unit dan Kepala Team IT. Team IT dalam melaksanakan tugas siber dibantu oleh Team Analisis, Team Direction Finder, dan Team Digital Forensik.

Kedudukan struktur organisasi cyber di tingkat Polda Jawa Timur semacam itu sudah sesuai dengan amanat Perkap Nomor 23 Tahun 2010 tentang Struktur Organisasi Tata Kerja Polri. Jadi di Polda Jatim SOTK-nya sudah sesuai dengan Peraturan Kapolri Nomor 23 Tahun 2010. Artinya, kedudukan organisasi satuan cyber crime di Polda Jawa Timur dibawah kendali Direktorat Kriminal Khusus, yakni berbentuk Sub Direktorat di Direktorat Kriminal Khusus (Subdit Cyber Crime). Mengenai tugas-tugas yang diemban oleh subdit cyber crime, yaitu

- Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik, money laundering, pasar modal, pajak, perbankan, dll)
- Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi (penyadapan telepon, penyalahgunaan Voip, penipuan melalui telepon genggam)
- Penyelidikan kejahatan yang menggunakan fasilitas Internet (cyber gambling, cyber terrorism, cyber fraud, cyber sex, cyber narcotism, cyber smuggling, cyber attacks on critical infrastructure, cyber black mail, cyber threatening, pencurian data, pencemaran nama baik, dll)
- Penyidikan kejahatan computer (masuk ke system secara illegal, ddos attack, hacking, tracking, phreacing, membuat dan menyebarkan yang bersifat merusak seperti malicious code al viruses, worm, rabbits trojan, dll).
- Penyidikan kejahatan yang berhubungan dengan Hak atas Intelektual (Pirated Software, rekaman suara, merubah tampilan website)

Bentuk dan jenis penipuan adalah berupa pencurian uang atau harta benda dengan sarana komputer/cyber dengan melawan hukum, yaitu dalam bentuk penipuan data dan penipuan program, yang secara terinci adalah seagai berikut:

- Memasukan instruksi yang tidak sah, yaitu dilakukan oleh orang yang berwenang atau tidak, yang dapat mengakses suatu sistem dan memasukkan instruksi untuk keuntungan sendiri dengan melawan hukum (misalnya transfer)
- Mengubah data input, yang dilakukan oleh seseorang dengan cara memasukan data untuk menguntungkan diri sendiri atau orang lain dengan cara melawan hukum;
- Merusak data, adalah dilakukan oleh seseorang untuk merusak printaut atau autput dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan iktikad tidak baik;
- Penggunaan komputer untuk sarana melakukan tindak pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.
- Tindak pidana penipuan, yang sesungguhnya dapat termasuk unsur perbuatan lain, yang pada pokoknya dimaksudkan menghindarkan din dari kewajiban, atau untuk memperoleh sesuatu yang bukan hak atau miliknya melalui sarana komputer dengan tipu daya.

Dari gambaran diatas menunjukan banyak sekali variasi-variasi di dalam tindak pidana penipuan. Di dalam Negara Indonesia sendiri terdapat banyak sekali tindak pidana yang menggunakan sarana komputer dan jaringan internet untuk melakukan penipuan. Penipuan yang dilakukan pada umumnya adalah penipuan melalui jejaring sosial pertemanan atau merchan online.

Pelaku penipuan modusnya adalah membuat akun facebook atau instagram baru atau membobol akun medsos milik orang lain kemudian menambah pertemanan hingga ribuan orang. Kemudian pelaku menawarkan barang-barang elektronik dengan harga murah. Untuk meyakinkan korbannya, pelaku mengaku sebagai bagian marketing dan berusaha meyakinkan bahwa barang akan dikirim melalui TIKI, JNT, JNE atau kurir lain apabila DP surah dikirim ke rekening pelaku. Setelah DP dikirim, seolah-olah ada yang menelepon korban mengaku sebagai bagian pengiriman barang dan mengatakan bahwa barang sudah dikirim. Untuk meyakinkan korbannya, pelaku mengirimkan resi pengiriman. Keesokan harinya korban mendapat telepon mengaku bagian pengiriman dan menginformasikan bahwa telah terjadi kelebihan jumlah item yang dikirimkan dan mengharuskan korban untuk membayar kelebihan barang yang dikirimkan tersebut dengan iming-iming diberikan diskon karena hal tersebut adalah kesalahan bagian pengiriman. Korban pun banyak yang tergiur dengan penawaran pelaku kemudian dengan mudahnya mentransfer uang ke rekening pelaku.

Menurut data yang didapat di regional Jawa Timur, perkara penipuan online atau menggunakan sarana internet yang masuk Polda Jawa Timur di tahun 2021 sebanyak 176 laporan, sedangkan di tahun 2022 kuartal pertama sebanyak 16 laporan. Dalam data tersebut, modus operandi paling populer dalam tindak pidana penipuan online adalah penipuan jual beli online (e-commerce) dan modus paling marak adalah penggunaan sarana medsos yang mengiklankan atau menawarkan berbagai barang murah, yang pada umumnya dilanjutkan dengan korespondensi pesan singkat via direct message atau

chat whatsapp untuk melanjutkan rangkaian tipu muslihat dari pelaku untuk mendapatkan keuntungan secara tidak patut.

Dengan adanya UU ITE segala aktivitas digital yang menyangkut informasi dan transaksi elektronik mempunyai payung hukum dan dapat dijadikan sebagai alat bukti yang sah di pengadilan. Berkaitan dengan hal ini perlu suatu mekanisme pembuktian yang legal dan dapat dipertanggungjawabkan secara hukum dalam penelusuran buktibukti kejahatan khususnya menyangkut teknologi terkini termasuk didalamnya masalah penggunaan percakapan WA / DM medsos sebagai suatu alat bukti Dalam menelusuri bukti digital berupa percakapan WA/ DM Medsos sampai pada proses pengungkapan di pengadilan, digital forensik menerapkan empat tahapan yaitu: Pengumpulan (Acquisition), Pemeliharaan (Preservation), Analisa (Analysis), dan Presentasi (Presentation). Seiring dengan perkembangan teknologi, dimasa depan objek penelitian dan cakupan digital forensik akan menjadi lebih luas lagi, dan keahlian dalam digital forensik tentu akan lebih dibutuhkan.

Jika tersangka atau para tersangka sudah tertangkap, Para tersangka agar diperiksa dengan mengajukan pertanyaan tentang:

- Identitas lengkapnya
- Riwayat hidupnya
- Kronologi perbuatan tersangka dalam hal melakukan penipuan melalui media elektronik.
- Kemampuan menjalankan komputer,gadget dan media elektronik yang terhubung dengan Internet dan lain-lain sesuai dengan kasus.
- Alat apa saja yang digunakan dalam melakukan perbuatan itu. Para tersangka yang memenuhi unsur dalam ketentuan ditahan sesuai dengan KUH Acara Pidana.

Para saksi yang kemungkinan sebagai tersangka dilakukan pemeriksaan yang dituangkan dalam berita acara yang memenuhi persyaratan formal dan materiel, hal-hal yang perlu dipertanyakan:

- Proses saling mengenal dengan tersangka
- Apa saja yang membuat saksi menjadi merasa ditipu
- Apa saja kerugian yang dialaminya
- Melalui media apa perbuatan itu dilakukan;
- Dan lain-lain sesuai dengan kasus.

Setelah melakukan rangkaian pemeriksaan terhadap barang bukti, saksi maupun korban, penyidik meminta keterangan kepada saksi ahli dari Depkominfo:

- Kepada ahli bidang hukum khusus Undang-undang Informasi dan Transaksi Elektronik tentang pemenuhan unsur pasal yang disangkakan.
- Kepada ahli secara teknis tentang permasalahan yang disangkakan.

Setelah mempunyai alat bukti yang sah dari pemeriksaan secara laboratoris terhadap barang bukti digital alat bukti lain, penyidik melanjutkan penyidikan dengan melengkapi berkas dan melakukan serangkaian penyidikan lain.

SIMPULAN

Modus yang digunakan pelaku penipuan jual beli online adalah dengan mengajak pembeli bertransaksi di luar marketplace resmi dan menggunakan nomor rekening pribadi dari pelaku atau rekan pelaku untuk bertransaksi. Modus berikutnya adalah dengan berpura-pura mengatasnamakan merchant online dengan membuat situs palsu yang tujuannya adalah merekam password dan username calon pembeli yang untuk kemudian digunakan penipu untuk mengakses data-data lainnya, seperti nomor rekening dan riwayat transaksi perbankan. Modus berikutnya adalah dengan pura-pura meminta OTP guna membobol rekening korbannya. Selanjutnya ada modus penipu yang berpura-pura dari bea cukai dan meminta tambahan pembayaran pada korbannya agar barangnya tidak disita. Modus penipuan berikutnya adalah dengan mengirimkan barang langsung ke alamat korbannya dan kurir meminta pembayaran pada korbannya dan tentunya barang tersebut tidak sesuai dengan deskripsinya. Adapun penyebab terjadinya penipuan jual beli online lebih dikarenakan oleh kultur budaya

masyarakat yang lambat memahami resiko jual beli online karena peralihan budaya dari konvensional ke digital.

Faktor berikutnya penyebab terjadinya penipuan online adalah belum tersertifikasinya secara menyeluruh setiap proses jual beli melalui media sosial ataupun online serta lemahnya keamanan sistem jual beli melalui media sosial. Faktor berikutnya adalah karena faktor ekonomi, pencarian jati diri serta minimnya resiko tertangkap yang menyebabkan penipuan online marak terjadi.

Adapun mengenai perkara penipuan jual beli online yang ditangani oleh Subdit V Cyber Crime Ditreskrimsus Polda Jatim selalu menggunakan Pasal 28 ayat (1) UU ITE guna menjerat pelaku. Jika dilihat dari konstruksi hukum rumusan Pasal 28 ayat (1) UU ITE maka pada dasarnya Pasal tersebut tidak menggunakan proposisi “penipuan” sebagaimana Pasal 378 KUHP yang jelas menggunakannya.

Walaupun demikian, Pasal 28 ayat (1) UU ITE tetap dapat dijeratkan pada pelaku penipuan jual beli online dikarenakan kandungan proposisi “berita bohong” dikarenakan penipu jual beli online selalu mengiklankan atau memasang penawaran penjualan barang baik di web atau merchant online yang dari stok barang, harga barang dan kewajiban pengiriman mengandung unsur “berita bohong”. Tidak digunakannya pasal 378 KUHP dikarenakan media yang digunakan penipu adalah media online yang merupakan ranah dari UU ITE. Selain itu jika menggunakan KUHP maka akan terjadi dualitas pengaturan dan penanganan.

Mengakibatkan ada kasus penipuan tersebut dapat ditangani Reskrimsus Siber dan ada yang ditangani oleh Reskrim. Sehingga agar tidak terjadi hal demikian maka digunakanlah UU ITE agar kasus benar-benar bisa ditangani oleh Ditreskrimsus.

REFERENSI

- Detik News. Bareskrim Bekuk Sindikat Penipu Online di Bawah Umur. Diakses dari <https://news.detik.com/berita/d-5178806/bareskrim-bekuk-sindikatan-penipu-online-di-bawah-umur>
- Perbandingan Hukum Pidana, PT Raja Grafindo Persada, Jakarta, 2002, hal. 259.
- Huzak, Douglas. Overcriminalization: the Limits of Criminal Law. Oxford, United Kingdom: Oxford University Press, 2008.
- Kholid, Mohamad Nur, Dinda Ajeng Puspanita, and Prawitra Thalib. "Copyright Protection of Art Containing Nudist Elements Under Positive Law In Indonesia." *Law and Justice* 6.2 (2022): 161-173.
- Kholid, Mohamad Nur, Dinda Ajeng Puspanita, and Prawitra Thalib. "Copyright Protection of Art Containing Nudist Elements Under Positive Law In Indonesia." *Law and Justice* 6.2 (2022): 161-173.
- Orin S. Kerr, "Search Warra <https://www.hukumonline.com/berita/a/modus-penipuan-online-lt6172286b2cb57/> <https://www.hukumonline.com/berita/a/modus-penipuan-online-lt6172286b2cb57/>
- Wahyudi, D., Samosir, H. S., & Devi, R. S. (2022). "Akibat Hukum Bagi Pelaku Tindak Pidana Penipuan Online Melalui Modus Arisan Online di Media Sosial Elektronik". *Jurnal Rectum: Tinjauan Yuridis Penanganan Tindak Pidana*, 04, 326-336.