INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 2 Tahun 2025 Page 1763-1776
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Penegakan Hukum Terhadap Tindak Pidana *Cyber* dalam Kasus Penipuan Jual Beli Online dalam Perspektif Kriminologi

Marselino Clifer Tuju[1], Suci Ramadani[2✉], Chairuni Nasution[3]
Universitas Pembangunan Panca Budi
Email: suciramadani@dosen.pancabudi.ac.id[2✉]

Abstrak

Penegakan hukum terhadap tindak pidana cyber, khususnya dalam kasus penipuan jual beli online, menjadi isu penting di era digital saat ini. Fenomena ini mencerminkan perkembangan kejahatan yang sejalan dengan kemajuan teknologi informasi. Penelitian ini bertujuan untuk menganalisis proses penegakan hukum terhadap pelaku penipuan jual beli online dari perspektif kriminologi. Pendekatan kriminologi digunakan untuk memahami motif, modus operandi, serta faktor-faktor penyebab terjadinya kejahatan ini. Hasil penelitian menunjukkan bahwa penipuan jual beli online sering dilakukan melalui platform digital seperti media sosial dan marketplace dengan memanfaatkan identitas palsu, iklan fiktif, atau harga yang tidak wajar untuk menarik korban. Penegakan hukum menghadapi tantangan berupa keterbatasan regulasi, minimnya literasi digital masyarakat, dan kesulitan dalam pelacakan pelaku yang sering kali berada di wilayah yurisdiksi berbeda. Upaya penegakan hukum melibatkan tindakan preventif, seperti edukasi publik dan penguatan keamanan siber, serta tindakan represif melalui penyelidikan berbasis digital forensik dan penuntutan berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Dari perspektif kriminologi, kejahatan ini dapat dicegah dengan mengurangi faktor risiko, seperti pengawasan yang lebih ketat terhadap aktivitas daring dan peningkatan kesadaran masyarakat terhadap modus penipuan. Dengan demikian, penanganan penipuan jual beli online memerlukan sinergi antara penegak hukum, penyedia layanan digital, dan masyarakat untuk menciptakan ekosistem digital yang aman.

Kata Kunci: *Penegak Hukum, Tindak Pidana Cyber, Penipuan Jual Beli Online*

Abstract

Law enforcement against cybercrime, especially in cases of online fraud, is an important issue in today's digital era. This phenomenon reflects the development of crime in line with advances in information technology. This study aims to analyze the law enforcement process against perpetrators of online fraud from a criminological perspective. A criminological approach is used to understand the motives, modus operandi, and factors causing this crime. The results of the study show that online fraud is often carried out through digital platforms such as social media and marketplaces by utilizing fake identities, fictitious advertisements, or unreasonable prices to attract victims. Law enforcement faces challenges in the form of limited regulations, minimal digital literacy among the public, and difficulties in tracking perpetrators who are often in different jurisdictions. Law enforcement efforts involve preventive measures, such as public education and strengthening cybersecurity, as well as repressive measures through digital forensic-based investigations and prosecutions based on the Electronic Information and Transactions Law (UU ITE). From a criminological perspective, this crime can be prevented by reducing risk factors, such as stricter supervision of online activities and increasing public awareness of fraud modes. Thus, handling online fraud requires synergy between law enforcement, digital service providers, and the community to create a safe digital ecosystem.

Keywords: *Law Enforcement, Cyber Crime, Online Fraud*

PENDAHULUAN

Perkembangan zaman yang semakin pesat membuat teknologi dan informasi menjadi hal yang sangat dibutuhkan dalam kehidupan masyarakat. Tak hanya menjadi point central, namun teknologi dan informasi sudah menjadi kebutuhan pokok bagi masyarakat untuk meningkatkan produktivitas keseharian mereka dalam mengakses informasi di dalam maupun di luar negeri. Akses teknologi dan informasi yang begitu cepat dan mudah, membuat pola hidup masyarakat berubah bukan hanya dari segi social saja, namun juga dari segi budaya, ekonomi, keamanan bahkan penegakan hukum. Teknologi informasi dan komunikasi tidak hanya digunakan dalam kehidupan sosial masyarakat namun juga telah memasuki berbagai faktor kehidupan mulai dari sektor pemerintahan, bisnis, perbankan, pendidikan, kesehatan bahkan sampai dengan keamanan pribadi (Kominfo, 2015).

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 (Dimas Wahyudi et al., 2022).

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* (Achmad Fauzi et al., 2023).

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.

Cybercrime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global (Lustia Wijayanti dan Jawade Hafiz, 2020). Berbeda dengan kejahatan konvensional yang memakai barang terlarang seperti pisau atau senjata api dalam mengancam dan melakukan aksi kejahatannya. Cybercrime hanya menggunakan jaringan komputer dan teknologi (Nur Fadhilah Mappaselleng, 2018). Pada jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang begitu luas. Ruang lingkup yang begitu luas membuat masalah kriminalitas yang terjadi di media sosial *(cybercrime*) tidak mengenal batas waktu dan tempat. Sehingga penanganannya juga memerlukan upaya penanggulangan yang extra serta kompleks. Hal ini dikarenakan tingkat kriminalitas pada internet tidak hanya dapat

membahayakan diri sendiri, namun dapat membahayakan keamanan masyarakat, negara serta tatanan kehidupan global.

Ada bermacam-macam kejahatan yang timbul melalui internet seperti penipuan, penghinaan, pornografi, money laundring, terorisme bahkan kejahatan terhadap keamanan negara, seperti pembocoran rahasia negara. Kejahatan dalam internet dapat dibedakan menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan seperti melakukan penipuan melalui internet (Adi Dharma Aryyaguna, 2017).

Fenomena penggunaan media sosial sebagai alat untuk melancarkan tindak kejahatan sudah kerap kali terdengar, khususnya di kalangan masyarakat Indonesia. Tidak terkecuali, oknum tertentu yang menyalahagunakan pemanfaatan media sosial dalam hal ini (penipuan) sebagai sarana meraup keuntungan pribadi. Kejahatan ini dapat terjadi akibat masyarakat yang tergiur akan harga murah dari suatu barang.

Penipuan melalui internet atau penipuan berbasis online merupakan kejahatan yang marak terjadi saat ini. Penggunaan internet yang semakin meningkat ternyata membuka kesempatan serta ide bagi para scammer (pelaku penipuan berbasis online) untuk meraup keuntungan yang lebih besar melalui internet (Databoks, 2023). Berdasarkan data yang di rilis oleh Kementeriaan Kominfo setidaknya ada sebanyak 115.756 laporan aduan penipuan transaksi online pada tahun 2022, sedangkan pada tahun 2023 berjumlah 167.675 laporan, memang telah terjadi penurunan jumlah laporan di tahun 2022, namun sayangnya jumlah aduannya tetaplah banyak (CNN Indonesia, 2021).

METODE PENELITIAN

Penelitian ini bersifat deskritif analisis yang mana mengungkapkan peraturan perundang-undangan yang berkaitan dengan teori-teori hukum yang menjadi objek penulis, demikian pelaksanaannya di dalam masyarakat yang berkenaan dengan objek penelitian (Zainuddin Ali, 2009). Analisis dilakukan berdasarkan gambaran, fakta yang diperoleh dan akan dilakukan secara cermat bagaimana menjawab permasalahan dalam menyimpulkan suatu solusi sebagai jawaban dari permasalahan tersebut (Burhan Ashshofa, 2008). Jenis penelitian yang dilakukan adalah penelitian yuridis normatif merupakan pendekatan yang dilakukan berdasarkan bahan hukum utama dengan cara menelaah teori-teori, konsep-konsep, asas-asas hukum serta peraturan perundang-undangan yang berhubungan dengan penelitian ini. Pendekatan ini dikenal pula dengan pendekatan kepustakaan, yakni dengan mempelajari buku-buku, peraturan perundang-undangan dan

dokumen lain yang berhubungan dengan penelitian ini (Soerjono Soekanto dan Sri Mamudja, 2001). Metode yang digunakan dalam penelitian ini adalah metode kepustakaan (*library reseach*) dan metode lapangan *(field research)*. Pengumpulan data yang dilakukan dengan teknik wawancara. Dan metode wawancara tersebut akan dilakukan dengan cara (*interviw guid*) yang dimana wawancara ini hampir sama dengan tanya jawab dengan terbuka Metode yang digunakan dalam penelitian ini adalah metode kepustakaan (*library reseach*) dan metode lapangan (*field research*). Pengumpulan data yang dilakukan dengan teknik wawancara. Dan metode wawancara tersebut akan dilakukan dengan cara (*interviw guid*) yang dimana wawancara ini hampir sama dengan tanya jawab dengan terbuka (Mestika Zed, 2008). Jenis data dibedakan menjadi data primer dan data sekunder, dalam penelitian ini peneliti akan menggunakan data sekunder. Data sekunder adalah sumber yang tidak langsung memberikan data kepada pengumpulan data (Sugiyono, 2019). Data-data yang dipergunakan dalam penelitian ini bersumber dari data sekunder yang meliputi halhal berikut:

a. Bahan hukum primer, yaituUndang – Undang ITE Undang – Undang Nomor. 11 Tahun 2008 jo. UU No. 19 Tahun 2016), asal 378 tentang Penipuan, Peraturan terkait perlindungan data pribadi (UU No. 27 Tahun 2022).
b. Bahan hukum sekunder adalah bahan hukum yang memberi penjelasan terhadap bahan hukum primer, seperti buku hukum, skripsi, jurnal hukum, laporan hukum, makalah, dan media cetak atau elektronik yang relevan dengan penelitian ini (Mestika Zed, 2008).
c. Bahan hukum tersier, yaitu bahan yang memberikan petunjuk maupun penjelasan terhadap bahan hukum primer dan bahan hukum sekunder seperti kamus umum, kamus hukum, ensiklopedia, dan lain sebagainya (Nomensen Sinamo, 2015).

Analisis data menurut Bogdan dalam Sugiyono yaitu proses mencari dan menyusun secara sistematik data yang diperoleh dari hasil wawancara, catatan lapangan, dan bahan-bahan lain sehingga dapat mudah dipahami dan temuannya dapat diinformasikan kepada orang lain (Mestika Zed, 2008). Analisis data yang dignakan dalam penelitian ini adalah kualitatif bersifat induktif, yaitu analisis berdasarkan data yang diperoleh.

HASIL DAN PEMBAHASAN

Macam-Macam Bentuk Konkret Penipuan Online Melalui Media Sosial

Media online merupakan segala jenis media yang dapat diakses melalui internet yang berisi teks, foto, suara dan video. Media tersebut juga dapat dimaknai dengan komunikasi yang dilakukan secara online melalui e-mail, website, whatsapp ataupun media sosial (facebook, instagram, twitter, dan lain lain). Media online disebut juga dengan digital media. Media online mempunyai peran penting untuk berinteraksi dengan orang lain. Media sebagai platform digital yang memfasilitasi pengguna untuk bersosialisasi dengan berkomunikasi, membagikan konten tanpa membatasi. Media online mempunyai pengaruh di masyarakat yang menimbulkan terjadinya perubahan yang mempengaruhi pada pola perilaku, pola pikir dan gaya hidup. Masyarakat dapat berinteraksi dan memperoleh informasi sebanyak-banyaknya, sehingga media online memberikan fasilitas untuk semua orang dapat mengakses dan mengekspresikan diri dari sumber informasi yang akurat. Wujud dari penipuan pada masyarakat dipengaruhi dari media sosial. Pesatnya teknologi saat ini, memudahkan masyarakat dalam mengakses apapun secara online. Kurangnya kewaspadaan masyarakat dalam memanfaatkan media sosial mengakibatkan mudah percaya dengan cybercrime. Salah satunya penipuan online yang terjadi di tengah masyarakat. Adanya praktik penipuan terjadi karena adanya pesan persuasif yang sengaja disampaikan oleh pelaku kepada korban yang seolah-olah kejadian fakta. Sejalan dengan hal tersebut, dapat dipahami bahwa platform media rentan terhadap kasus penipuan.

Berdasarkan teori, penipuan dapat dibedakan menjadi dua yakni; secara bahasa dan yuridis. Secara bahasa berasal dari kata tipu yang artinya perkataan atau aktivitas yang tidak jujur (tidak sesuai dengan aslinya) yang dapat menyesatkan orang lain untuk mencari keuntungan. Sementara penipuan diartikan sebagai cara, proses, perbuatan menipu, perkara menipu (mengecoh). Penipuan dapat dilakukan secara individu maupun kelompok dengan membuat kesan seolah olah pernyataan yang diungkapkan benar dan tidak palsu untuk memberikan kepercayaan pada orang lain. Sedangkan dalam pengertian yuridis, penipuan tercantum rumusan tindak pidana dalam KUHP. Akan tetapi, rumusan penipuan dalam KUHP tidak hanya terdiri dari satu definisi melainkan beberapa unsur lainnya yakni pelaku dapat dipidana sesuai dengan perbuatan yang telah dilakukan. Maka, penipuan menurut pasal 378 KUHP yakni: "Penipuan adalah 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 demikian rupa yang merupakan cerita sesuatu yang seakan-akan benar (Anang Sugeng Cahyono, 2016)."

Penipuan online adalah kejahatan yang dilakukan melalui layanan internet atau software dengan akses internet untuk menipu atau mengambil keuntungan. Bentuk penipuan online dapat diartikan sebagai kejahatan yang menggunakan teknologi informasi dalam melakukan perbuatannya. Hal ini adalah suatu bentuk kejahatan yang canggih dan menjadi salah satu contoh dari cybercrime. Penipuan online dapat berupa penggunaan identitas palsu, citra palsu, atau pemberian informasi yang tidak benar untuk mendapatkan keuntungan atau keuntungan dari korban. Penipuan online merupakan suatu bentuk kejahatan yang dapat dilakukan melalui berbagai media sosial dan platform elektronik, sehingga korban dapat terdampak secara finansial, fisik, atau jasmani.

Bentuk Penipuan online dapat terjadi dalam berbagai bentuk, seperti penipuan dalam bisnis online, penipuan dengan citra palsu, penipuan dengan identitas palsu, dan penipuan dengan informasi yang tidak benar. Penipuan dalam bisnis online terjadi ketika pembeli menerima barang atau layanan yang tidak sesuai dengan yang ditawarkan atau tidak ada seharga yang ditawarkan. Penipuan dengan citra palsu terjadi ketika orang menggunakan citra yang tidak asli untuk mendapatkan keuntungan. Penipuan dengan identitas palsu terjadi ketika orang menggunakan identitas yang tidak asli untuk mendapatkan keuntungan. Penipuan dengan informasi yang tidak benar terjadi ketika orang memberikan informasi yang tidak sesuai dengan yang benar untuk mendapatkan keuntungan.

Faktor-faktor yang terjadi dalam penipuan online dilakukan oleh penipu ditandai oleh empat hal; pertama, faktor mempunyai harapan untuk menentukan sebuah keberhasilan dalam penipuan. Kedua, faktor mempunyai tujuan untuk menentukan sulitnya penipuan dengan jangkauan lebih luas dan jangka panjang. Ketiga, memotivasi diri untuk mengidentifikasi penipuan yang berorientasi pada tujuan serta dapat menjaga kerahasiaan dalam menjadi identitas. Keempat, menjalin komunikasi dengan calon korban dengan membangun kepercayaan agar tidak menimbulkan kecurigaan korban sehingga meningkatkan peluang mereka untuk ditipu. Empat faktor tersebut cenderung yang dilakukan oleh pelaku untuk mencapai suatu tujuan. Faktor lain terjadinya penipuan online yakni; a. Tingginya angka kemiskinan dan pengangguran yang disebabkan kurangnya lapangan pekerjaan, b. Mendapatkan uang dengan cara yang mudah, c. Sulit terlacaknya pelaku, d. Mudahnya menghilangkan jejak, e. Minimnya biaya dengan kebutuhan yang meningkat dan f. Kurangnya wawasan bermedia sosial.

Faktor penyebab terjadinya penipuan di atas berdasarkan dari korban. Maka, pelaku maupun korban dapat mendorong terjadinya kasus penipuan online. Dengan demikian, fenomena penipuan online di masyarakat timbul akibat terjadinya interaksi antara pelaku dan korban melalui pesan. Pesan juga menjadi sebuah faktor terpenting untuk menentukan sebuah keberhasilan berkomunikasi. Strategi pada bentuk penipuan online diantaranya; undian berhadiah, penawaran investasi/pinjaman online, minta tolong, kode OTP dan jual beli. Kelima bentuk penipuan yang paling banyak diterima oleh pengguna adalah undian berhadiah. Bentuk penipuan online pada undian berhadiah meskipun banyak digunakan oleh pelaku, namun masyarakat tidak mudah percaya. Sedangkan korban melalui bentuk penipuan pada jual-beli lebih banyak. Penipuan pada jual beli di berbagai platform disebabkan karena adanya sebuah transaksi dalam elektronik yang dapat merugikan orang lain. Secara garis besar terdapat dua kerugian yang dialami oleh pembeli yaitu; Pertama, kerugian yang diakibatkan oleh penjual yang tidak bertanggungjawab sehingga merugikan pembeli. Kedua, kerugian pembeli yang terjadi karena tindakan melawan hukum yang dilakukan oleh pihak ketiga, sehingga konsumen disesatkan dan kemudian dirugikan (Agus Rusmana, 2015). Maka, bentuk penipuan dalam bentuk jual-beli online diantaranya; 1) Ketidaksesuaian barang atau produk yang diterima dengan yang dipesan. Perbedaan barang mencakup beragam bidang, baik yang diterima dengan situs iklan jual-beli, mengalami kerusakan maupun keterlambatan pengiriman. Selain itu penjual memalsukan barang dagangannya atau barang-barang brand ternama ternyata barang KW (tiruan). 2) Identitas pelaku usaha atau konsumen fiktif, merupakan pelaku usaha ataupun konsumen yang memalsukan akunnya dalam proses pendaftaran tersebut. Akun ini biasanya belum terverifikasi oleh situs jual beli online sehingga ketika terjadi komplain dari konsumen akan sulit teridentifikasi karena nama, alamat, ataupun kontak yang diberikan adalah fiktif. 3) Penipuan harga diskon barang atau produk yang ditawarkan, agar dapat menarik konsumen tergiur dengan produk tersebut. Menawarkan berbagai kemudahan dan praktis digunakan, berbelanja melalui situs jual beli online memang seringkali menawarkan harga yang lebih murah dibandingkan berbelanja langsung di toko konvensional. Seringkali, harga yang ditawarkan pun miring atau jauh diluar harga pasaran, terutama untuk barang-barang elektronik.

Selain itu, pelaku juga memiliki banyak cara untuk melancarkan aksi nya dalam melakukan penipuan online, salah satu nya disebut modus penipuan. Ada tiga modus penipuan yang marak terjadi dalam kasus penipuan online, yaitu:

1) Phising

Phising berasal dari kata fishing yang berarti memancing. Phising merupakan perbuatan yang dilakukan oleh pelaku dengan memalsukan data di website palsu yang menyerupai aslinya dengan tujuan untuk mencuri identitas orang lain yang mengatasnamakan perusahaan, lembaga maupun instansi. Modus phising dilakukan dengan pembuatan situs atau website palsu yang disebarkan sebanyak banyaknya untuk mendapatkan korban. Website dibuat semenarik mungkin untuk memikat daya tarik calon korban. Modus phising dapat dikenakan Pasal 28 ayat 1, Pasal 51 ayat 1, Pasal 28 ayat 1 dan Pasal 45A ayat 1. Sejalan dengan hal tersebut, pengaturan hukum terhadap pelaku dalam bentuk phising juga tercantum di Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik. Kebijakan hukum terhadap cyber crime belum merumuskan atau menjelaskan konsep penyebab 38 terjadinya phising yang dapat merugikan orang lain. Maka dari itu, regulasi terhadap kebijakan cybercrime dengan merubah isi dan unsur pada Pasal 35 dapat diterapkan untuk mengurangi penipuan online dalam bentuk phising.

2) Scamming

Scamming diartikan sebagai tindakan manipulasi oleh lembaga atau individual untuk mendapatkan kepercayaan dari calon korban mencapai keberhasilan. Modus scamming mempunyai beraneka ragam jenis, yakni: minta tolong, love scamming dan lain-lain. Love scamming yang identik dengan romance scamming. Jenis penipuan tersebut dengan cara menghancurkan mental calon korban yang mengira perasaan saling suka muncul diantara keduanya. Modus love scamming yang sering dilakukan dengan memberi perhatian lebih kepada calon korban, sehingga calon korban akan menuruti kemauan dari pasangannya. Sebagaimana meminta foto bagian-bagian tubuh yang beralasan untuk koleksi pribadinya. Sejalan dengan hal tersebut, foto akan disebarluaskan dan memberi ancaman kepada calon korban untuk mengirimkan uang agar foto tersebut tidak disebarluaskan. Akan tetapi, hal 39 tersebut sebagai salah satu strategi yang digunakan pelaku untuk mendapatkan untung. Romance scamming pada pasangan digunakan untuk pencurian data, uang dan lain-lain. Modus scamming dapat dilakukan melalui whatsapp, instagram maupun facebook. Di luar kesadaran bagi calon korban, hal tersebut mempermudah pelaku untuk menghasilkan pundi pundi uang. Maka perlu kewaspadaan dalam pemanfaatan media digital.

3) Social Engineering

Social Engineering cara membangun interaksi antara pelaku dan calon korban sebagai teknik manipulasi psikologis yang seakan-akan korban melakukan kesalahan sendiri. Pelaku menipu secara halus melalui chat atau telepon di berbagai platform. Modus sosial engineering yang sering digunakan oleh penipu yaitu; transaksi via online, contact centre bank, SMS penipuan, jual beli dan sebagainya. Salah satu korban oleh mahasiswa di perguruan tinggi Semarang bernama AS mengaku pernah tertipu melalui telepon yang mengatasnamakan ojek online. Saat korban sedang makan di kantin, ia di telfon oleh pelaku yang mengatasnamakan ojek online bahwa mendapatkan hadiah senilai Rp. 3.000.000. 40 Tanpa ia sadari ia memberikan kode dari akun ojek online tersebut. Setelah telpon dimatikan, korban membuka aplikasi ojek online untuk mengecek, akan tetapi saldo dari aplikasi tersebut berkurang Rp. 1.000.000. Korban baru menyadari jika ia sudah tertipu. Pelaku membangun komunikasi dengan baik, agar netizen tidak sadar jika menjadi calon korban. Hal tersebut, dapat dilihat dari rekayasa pesan maupun lisan yang disampaikan oleh pelaku. Ketiga modus tersebut, adanya relevansi antara modus dan media sangat mempengaruhi keberhasilan pada penipuan melalui media digital.

Perlindungan Hukum dan Upaya Pencegahan terjadinya Penipuan Online di Media Sosial

Perkembangan teknologi banyak membawa dampak positif ke dalam aktivitas kehidupan masyarakat, salah satunya adalah dalam melakukan komunikasi antar individu. Media sosial secara keseluruhan memiliki tujuan untuk mempermudah terjadinya komunikasi antar perorangan maupun kelompok tanpa harus bertemu secara langsung atau bertatap muka. Dimana jaringan komunikasi berfungsi sebagai saluran penyampaian pesan antar individu (Wahyuddin et al., 2024). Selain itu, masih banyak manfaat dari hadirnya media sosial dalam kehidupan masyarakat seperti sumber informasi, bisnis, pendidikan, kesehatan dan lain sebagainya yang membantu aktivitas sehari-hari. Hal tersebut jelas membawa dampak positif bagi umat manusia. Namun, dalam prakteknya penggunaan media sosial juga sangat berpotensi untuk memberi peluang kepada para pihak yang memanfaatkannya sebagai media kejahatan, salah satunya adalah penipuan. Tindak pidana yang dilakukan secara online menggunakan jaringan internet dikenal dengan istilah cyber crime. Definisi tentang cybercrime lebih bersifat pada kejahatan umum yang memiliki karakteristik dilakukan oleh pihak- pihak yang menguasai penggunaan teknologi informasi seperti internet dan seluler (Noor Rahmad, 2019). Penipuan online termasuk dalam cyber crime karena menggunakan jaringan internet untuk melakukan tindak kejahatan.

Penipuan yang dilakukan dapat berupa penyebaran informasi palsu sehingga korban mengalami kerugian dengan memodifikasi sistem komputer atau sarana elektronik.

Tindak pidana penipuan terbagi menjadi dua, yaitu penipuan yang bersifat umum dan penipuan yang dilakukan melalui teknologi informasi seperti internet dan seluler. Tindak pidana penipuan secara umum diatur dalam KUHP Pasal 378, dimana penipuan ditafsirkan memiliki beberapa unsur, yaitu tindakan seseorang dengan tipu muslihat, rangkaian kebohongan, nama palsu, dan keadaan palsu dengan maksud menguntungkan diri sendiri dengan tiada hak (R. Sugandhi, 1980). Dalam KUHP, tindak pidana penipuan dapat dipidana paling lama 4 tahun penjara. Selain itu, terdapat suatu tindak pidana penipuan yang diatur di luar KUHP yang menjadi satu kesatuan dengan undang-undang lain, yaitu tindak pidana penipuan secara online. Tindak pidana penipuan secara online diatur dalam Undang-undang No. 19 tahun 2016 atas perubahan Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Secara spesifik terdapat dalam Pasal 28 ayat (1) UU ITE yang mengatur ketentuan penipuan dengan memberikan informasi palsu dalam media elektronik, sehingga barang siapa yang melanggarnya telah melakukan tindak pidana penipuan. Ketentuan pidananya dapat dilihat dalam Pasal 45A ayat (1) UU ITE yaitu pidana penjara paling lama (6) enam tahun dan/atau denda paling banyak Rp. 1.000.000.000,00 (satu miliar rupiah).

Walaupun sudah ada peraturan perundang-undangan tentang penipuan online, kasus tersebut masih marak terjadi di tengah masyarakat. Hal ini timbul karena beberapa faktor seperti penegak hukum yang tidak profesional dan berintegritas dalam menjalankan tugasnya sehingga perlu dioptimalkan agar menjamin perlindungan dan kepastian hukum bagi korban. Faktor lainya adalah kurang kehati-hatian dari masyarakat dalam menggunakan media sosial sehingga penting untuk menciptakan program sosialisasi dan edukasi secara masif kepada masyarakat mengenai penggunaan media sosial agar korban penipuan online dapat diminimalisir. Di Indonesia, penipuan online kerap terjadi melalui beberapa platform media sosial seperti WhatsApp, Facebook, Instagram dan platform lainnya dengan menggunakan modus kejahatan yang bervariasi. Hal tersebut membuat masyarakat merasa khawatir untuk melakukan aktivitasnya di dunia maya. KOMINFO menyatakan bahwa tercatat kurang lebih 1.730 kasus mengenai penipuan online pada tahun 2018 sampai dengan 2023 dan telah membawa kerugian sebesar 18 triliun kepada para korban. Hal tersebut sangat jelas membawa kerugian terhadap masyarakat, terutama bagi para pengguna media sosial yang minim pengetahuan mengenai hal itu.

Modus kejahatan dari penipuan online melalui media sosial yang terjadi dalam masyarakat cukup beragam. Jenis media sosial yang banyak menjerat korban adalah aplikasi WhatsApp, karena hampir seluruh kalangan masyarakat menggunakan aplikasi ini. Berdasarkan survei Ding, platform top up seluler, WhatsApp menjadi layanan pesan instan yang paling banyak digunakan orang Indonesia untuk berkomunikasi dengan yang lain. Dari survei tersebut terungkap 89% responden menyatakan bahwa WhatsApp merupakan media yang orang Indonesia pilih untuk saling berkomunikasi. Setelah itu diikuti Facebook dengan persentase 44% dan Instagram 41%. Salah satu modus yang sering digunakan dari penipuan online melalui aplikasi WhatsApp yaitu berbentuk Sniffing. Bentuk tindakan sniffing yaitu mengarahkan pengguna untuk mendownload file aplikasi tertentu yang berformat apk yang dibuka melalui WA yang secara otomatis dapat mencuri data pribadi (Wahyuddin et al., 2024).

SIMPULAN

Berdasarkan hasil penelitian, penipuan online adalah kejahatan yang dilakukan melalui media internet atau software yang terakses oleh internet. Kejahatan penipuan online merupakan kejahatan yang marak terjadi di zaman modern ini. Para pelaku dalam kejahatan ini sangat memanfaatkan berbagai platform media sosial. Dengan berbagai macam modus yang mereka lakukan, diantaranya seperti mencuri identitas korban untuk disalahgunakan, meretas dan mencuri uang yang ada di rekening korban, maupun melakukan penipuan dengan menjanjikan hadiah bagi korban untuk ditebus menggunakan sejumlah uang. Mereka mampu merugikan korbannya hingga jutaan rupiah. Menurut KOMINFO total kerugian dari korban penipuan online di Indonesia dari tahun ketahun mencapai 18 Triliun rupiah. Peristiwa tersebut membuktikan bahwa kurangnya kewaspadaan dan pengetahuan masyarakat tentang bahaya penipuan online. Perlu adanya sosialisasi secara masif dari pemerintah kepada masyarakat dan terus menerus memberikan pengetahuan tentang bahaya kejahatan penipuan online. Perlu diketahui juga bahwasanya kejahatan penipuan online juga terjadi pada transaksi jual beli online, yang dimana pihak pembeli dirugikan dengan tindakan pihak penjual. Seperti penerimaan barang yang tidak sesuai oleh pembeli atau tidak adanya tanggung jawab dari pihak penjual sehingga merugikan pembeli. Dari seluruh modus kejahatan penipuan online masyarakat juga harus mengetahui jenis jenis kejahatan penipuan online. Diantaranya seperti phising, yaitu dimana pelaku mencuri identitas dengan memalsukan data di website palsu yang menyerupai website aslinya dengan lembaga atau individual

untuk mendapatkan kepercayaan korban, dan ada juga social engineering yaitu pelaku melakukan interaksi dengan korban untuk memanipulasi psikologis korban yang seakan akan korban melakukan kesalahan sendiri. Dengan demikian, perlu adanya peningkatan serta perbaikan profesionalitas dan integritas dari aparatur 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. Sosialisasi tentang regulasi hukum mengenai kejahatan atau tindak pidana penipuan online juga perlu dilakukan agar masyarakat yang terkena dampak kejahatan penipuan online dapat mengetahui upaya hukum yang dilakukan sesuai peraturan perundang-undangan yang berlaku di Indonesia. Tidak hanya itu, sistem peradilan pidana juga perlu menangani kasus kejahatan ini dengan baik, yaitu dengan memproses pelaksanaan putusan pengadilan bagi pelaku kejahatan ini. Hal tersebut dilakukan sebagai wujud nyata adanya kepastian hukum dan jaminan perlindungan hukum bagi korban.

DAFTAR PUSTAKA

Agus Raharjo, 2002, Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi. Bandung: Citra Aditya Bakti.

Budi Suhariyanto, 2012, Tindak Pidana Teknologi Informasi (CyberCrime): Urgensi Pengaturan dan Celah Hukumnya. Jakarta: Rajawali Press.

Peter Mahmud Marzuki, 2016, Penelitian Hukum Edisi Revisi. Jakarta : Prenada Media Group.

Raharjo, Agus, 2002, Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi, PT. Citra Aditya Bakti, Bandung.

Widodo, 2009, Sistem Pemidanaan dalam Cyber Crime, Laksbang Mediatama, Yogyakarta.

Agustin Setyo Wardani. (2020). Headline: Marak Penipuan Online Shop di Medsos, HatiHati Modusnya Makin Canggih. Retrieved from Liputan6 website: https://www.liputan6.com/tekno/read/4157301/headline-marak-penipuan-onlineshop-di-medsos-hati-hati-modusnya-makin-canggih

Cindy Mutia Annur. (2020). Kenali Maraknya Penipuan Online saat Pandemi. Retrieved from Katadata website: https://katadata.co.id/0/analisisdata/5f7c5da0cc927/kenalimaraknya-penipuan-online-saat-pandemi

Prayogi, Arie, Lidya Rahmadhani Hasibuan, and Fitria Ramadhani Siregar. "Legal

Protection For Wives Who Are Victims Of Domestic Violence Based On Law no. 23 of 2004." International Journal Of Humanities Education and Social Sciences 4, no. 1 (2024).

Ramadani, Suci. "Juridical Review Of The Criminal Act Of Online Fraud Is Reviewed From Law Number 19 Of 2016 Concerning Information And Electronic Transactions." International Journal of Society and Law 1.1 (2023): 1-10.

Rianto, R., Zarzani, T. R., & Saragih, Y. M. (2024). Tanggung Jawab Hukum Korporasi Media Online dan Masyarakat Pengguna Media Sosial Atas Penayangan Berita yang di Share Ke Publik Mengandung Tindak Pidana ITE. JIIP-Jurnal Ilmiah Ilmu Pendidikan, 7(1), 393-398.

Sahlepi, Muhammad Arif. "Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik." Innovative: Journal Of Social Science Research 3.6 (2023): 1402-1412.

Saragih, Yasmira Mandasari, et al. "Juridical Study Of The Criminal Acts Of Defense In View From The Ite Law Number 19 Of 2016." International Journal of Educational Review, Law And Social Sciences (IJERLAS) 3.3 (2023): 1100-1106.