PENANGGULANGAN KEJAHATAN PENIPUAN BELANJA ONLINE DI WILAYAH KEPOLISIAN DAERAH JAWA TIMUR

ONLINE SHOPPING FRAUD CRIME COMMITMENT IN EAST JAVA REGIONAL POLICE AREA

Harianto Rantesalu[1]

[1]Sekolah Pascasarjana Universitas Airlangga

ABSTRACK

This study aims to analyze the mode and factors that cause buying and selling fraud through e-commerce facilities and to analyze the handling of online buying and selling fraud and the obstacles that occur in the law enforcement process.This research literature uses the concept of criminal acts, the concept of fraud, criminal provisions in the ITE Law, crime theory, evidence in criminal cases and policies for overcoming criminal acts.The research approach uses qualitative research with the type of empirical research.The mode used by online buying and selling fraud perpetrators is to invite buyers to transact outside the official marketplace, pretending to be on behalf of online merchants, asking for the victim's OTP, fraudsters pretending to be from customs and asking for additional payments to victims, fraudsters sending goods by COD and courier. asking for payment to the victim and of course the item does not match the description. The causes of online buying and selling fraud are more due to community culture, not yet fully certified every buying and selling process through social media or online, economic factors, identity searches and the minimal risk of being caught which causes online fraud to occur.Obstacles faced by investigators in dealing with online fraud cases include: Investigation and Investigation Obstacles, Difficulty opening accounts of perpetrators due to bank bureaucratic licensing, Lack of maximum coordination between the East Java Police investigators with cellular operators or internet service providers, The lack of East Java Police investigators who have informatics background, Inequality of Perception of Online Fraud Crime Handling among Law Enforcers, Jurisdiction Problems, and Positive Legal Substance Constraints.

Keywords: Countermeasures, Crime, Online Fraud

ABSTRAK
Penelitian 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.Pendekatan penelitian menggunakan penelitian kualitatif dengan jenis penelitian empiris.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 pemabayaran 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. Kendala-kendala yang dihadapi penyidik dalam penanggulangan perkara penipuan online antara lain :Kendala Penyelidikan dan Penyidikan, Sulitnya membuka rekening pelaku karena perijinan birokrasi bank, Kurang Maksimalnya koordinasi pihak penyidik Polda Jatim dengan operator selular atau pun internet service provider, Minimnya penyidik Polda Jatim yang memiliki latar belakang informatika, Ketidaksamaan Persepsi Penanganan Kejahatan Penipuan Online antar Penegak Hukum, Masalah Yurisdiksi, serta Kendala Substansi Hukum Positif.
Kata Kunci : Penanggulangan, Kejahatan, Penipuan Online

I. PENDAHULUAN

Jual beli online 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:[1]

1. 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.
2. Iklan Baris Online - Merupakan situs iklan baris, di mana situs yang bersangkutan tidak memfasilitasi kegiatan transaksi online. Contoh: Kaskus, OLX.co.id.
3. 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.[2]

Secara terminologis, kejahatan yang berbasis pada teknologi informasi dengan menggunakan media komputer sebagaimana terjadi saat ini, dapat disebut dengan beberapa istilah yaitu *computer misuse, computer abuse, computer fraud, computer-related crime, computer-assisted crime,* atau *computer crime.* Menurut Barda Nawawi Arief, pengertian *computer-related crime* sama dengan *cybercrime.*[3] Tb. Ronny R. Nitibaskara berpendapat, bahwa kejahatan yang terjadi melalui atau pada jaringan

[1] Satria Nur Fauzi dan Lushiana Primasari, *Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (E-Commerce)*, Recidive Volume 7 No. 3, Sept.- Des. 2018, hal. 251.

[2] Pusat Data dan Sarana Informatika Kementerian Komunikasi dan Informatika, *Laporan Potret Belanja Online di Indonesia*. Pusat Data dan Sarana Informatika Kementerian Komunikasi dan Informatika. Jakarta, 2013, hal. 3

[3] Barda Nawawi Arief, *Perbandingan Hukum Pidana*, PT Raja Grafindo Persada, Jakarta, 2002, hal. 259.

komputer di dalam internet disebut *cybercrime.*[4]Kejahatan ini juga dapat disebut kejahatan yang berhubungan dengan komputer *(computer-related crime)*, yang mencakup 2 kategori kejahatan, yaitu kejahatan yang menggunakan komputer sebagai sarana atau alat, dan menjadikan komputer sebagai sasaran atau objek kejahatan.[5]

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.[6]

Dalam wilayah Polda Jawa Timur sendiri untuk kasus penipuan pembelian barang secara online di tahun 2020 Terdapat 3 kasus, yang pertama tindak pidana penipuan jual beli online rangka sepeda angin merek Trek Slash 99 warna merah yang mana kerugian yang dialami terlapor adalah sebesar Rp. 30.500.000,-. Selanjutnya penipuan jual beli online bawang putih sinca sebanyak 1,5 Ton dengan kerugian Rp. 14.835.090,-. Terakhir penipuan dengan menawarkan masker merek Sensi dengan harga murah yang dijual melalui instagram dengan total kerugian sebesar Rp. 160.330.000.

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

1) Sosial enginering, 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 enginering* sendiri adalah cara mendapatkan identitas korban tanpa diketaui karena pelaku juga ikut bersama dalam aktifitas yang sering dilakukan oleh calon kerban.
2) Membajak akun media sosial, akun bank atau whatsapp yang dimiliki oleh korban, kemudian pelaku mengambil alih dan mengubah pasword, mengambil manfaat dari seluruh akun yg sdh di ambil alih.

[4] Tb. R. Nitibaskara, "Problema Yuridis Cybercrime' Makalah pada Seminar Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, Juli 2000, hal. 2.

[5] Widodo, *Sistem Pemidanaan Dalam Cybercrime*, Laksbang Mediatama, Yogyakarta, 2009, hal. 24

[6] "Bareskrim Bekuk Sindikat Penipu Online di Bawah Umur" https://news.detik.com/berita/d-5178806/bareskrim-bekuk-sindikat-penipu-online-di-bawah-umur, diakses tanggal 11 Oktober 2020.

3) 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 semisil 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 mengirirnkan resi pengiriman. Keesokan harinya korban mendapat telepon mengaku bagian pengiriman dan menginformasikan bahwa telah terjadi kelebihan jumlah item yang dikirirnkan dan mengharuskan korban untuk membayar saja kelebihan barang yang dikirirnkan tersebut dengan iming-irning 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 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.

Dalam hal penegakan hukum guna penanggulangan tindak pidana penipuan jual beli online atau kasus-kasus *cybercrime* lainnya, di jajaran Polda Jatim ditangani oleh Sat *Cybercrime*. Tugas pokok Unit *Cybercrime* berdasarkan Keputusan Kapolri No. Pol.

: KEP/54/X/2002 tanggal 17 Oktober 2002 adalah sebagai unsur pelaksanaan pada Direktorat Reserse Kriminal Khusus Polda Jawa Timur yang bertugas melakukan penyelidikan dan penyidikan tindak pidana khusus, terutama kegiatan penyidikan yang berhubungan dengan tehnologi informasi, telekomunikasi, serta transaksi elektronik.

Dalam rangka melaksanakan tugas tersebut, Unit *Cybercrime* Direktorat Reserse Kriminal Khusus Polda Jawa Timur melaksanakan fungsi-fungsinya sebagai berikut :

1) Penyidikan kasus-kasus yang berhubungan dengan Transaksi elektronik.(*Carding, Money laundering*, Pasar Modal, Pajak, Perbankan, Dll).
2) Penyidikan kasus-kasus yang berhubungan dengan tehnologi komunikasi dan Informasi (Penyadapan Telphon, Penyalahgunaan Voip, Penipuan Melalui telpon genggam)
3) Penyelidikan kejahatan yang menggunakan Fasilitas Internet (*Cyber Gambling, Cyber terrorism,Cyber Fraud Cyber sex, Cyber Narcotism, Cyber Smuggling, Cyber attacks on critical infrastructure, Cyber Balckmail, Cyber Threatening*, pencurian data, pencemaran nama baik, dll).
4) Penyidikan Kejahatan Komputer (Masuk ke System secara Ilegal, Ddos attack, *Hacking,Tracking, Phreacing*, Membuat dan menyebarkan yang bersifat merusak)
5) Penyidikan kejahatan yang berhubungan dengan Hak Atas Kekayaan Intelektual (*Pirated Software*, rekaman Suara, Merubah tampilan Website)

Walaupun sudah ada naungan UU ITE guna penegakan hukumnya tetapi dalam kenyataannya berbagai kendala masih terjadi dalam proses penegakan hukum tersebut. Masalah utama adalah dalam hal pembuktian data elektronik, baik itu data elektonik transaksi, maupun data elektronik kesepakatan yang telah terjadi. Kesulitan ini di karenakan, setiap kegiatan baik itu kegiatan transaksi, dan kesepakatan yang terjadi di dalam *e-commerce* melalui jejaring sosial seperti facebook, Instagram, twitter, dsb sangatlah mudah untuk dihapus. Selain itu data tersebut juga tidak bisa di simpan ataupun dicetak seperti halnya email. Masalah inilah yang menjadi ganjalan dalam hal pembuktian selama proses penegakan hukum. Belum lagi permasalahan dengan lintas batas wilayah yang mana dengan adanya kegiatan *e-commerce* ini menjadi *borderless* atau tak terbatas. Sehingga berdasarkan latar belakang tersebut.

II. 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.[7]

Dengan banyaknya variasi kejahaan siber maka pemerintah dituntut untuk mampu memberikan perlindungan kepada masyarakat dari kejahatan siber. 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 dirubah 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 Analis, 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 :

a. Penyidikan kasus-kasus yang berhubungan dengan transaksi elektronik, money loundring, pasar modal, pajak, perbankan, dll)

[7]Huzak, Douglas. *Overcriminalization: the Limits of Criminal Law*. Oxford, United Kingdom: Oxford University Press, 2008.

b. Penyidikan kasus-kasus yang berhubungan dengan teknologi komunikasi dan informasi (penyadapan telepon, penyalahgunaan Voip, penipuan melalui telepon genggam)
c. 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 theatening, pencurian data, pencemaran nama baik, dll)
d. Penyidikan kejahatan computer (masuk ke system secara illegal, ddos atack, hacking, tracking, phreacing, membuat dan menyebarkan yang bersifat merusak seperti malicous code al viruses, worm, rabbits trojan, dll).
e. Penyidikan kejahatan yang berhubungan dengan Hak atas Intelektual (Pirated Software, rekaman suara, merubah tampilan website)

Dari aspek peralatan dan laboratorium Polda Jawa Timur telah memiliki laboratorium Cyber Crime Investigation Satelit Office (CCISO) yang terdiri :

a. Laboratorium Komputer Forensik
b. Laboratorium Mobile Phone Forensik
c. Laboratorium Audio Video Forensik

Adapun peralatan lain yang dimiliki Polda Jawa Timur, yaitu cellebrite, check post, dan lain-lain. Apabila dilihat dari segi peralatan untuk mengungkap suatu kasus-kasus kejahatan siber, kemampuan peralatannya (material) cukup memadai sebab memiliki mobile direction finder (DF). Seluruh sarana dan prasaran tersebut pada dasarnya digunakan oleh penyidik Subdit V Ditreskrimsus Polda Jatim untuk untuk menunjang penanggulangan kejahatan siber yang saat ini tengah marak yakni penipuan jual beli e-commerce terutama di tengah semakin gencarnya promo dari berbagai merchant online.

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:[8]

a) 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);
b) Mengubah data input, yang dilakukan oleh seseorang dengan cara memasukan data untuk meguntungkan diri sendiri atau orang lain dengan cara melawan hukum;
c) Merusak data, adalah dilakukan oleh seseorang untuk merusak printaut atau autput dengan maksud untuk mengaburkan, menyembunyikan data atau informasi dengan iktikad tidak baik;
d) Penggunaan komputer untuk sarana melakukan tindak pidana, ialah dalam pemecahan informasi melalui komputer yang hasilnya digunakan untuk melakukan kejahatan, atau mengubah program.
e) 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.

Subdit V Cyber Crime kerap mengungkap penipuan melalui media internet dengan modus menawarkan barang-barang elektronik seperti handphone berbagai merk, kamera, laptop berbagai merk dengan harga murah di jejaring sosial facebook ataupun melalui platform instagram.

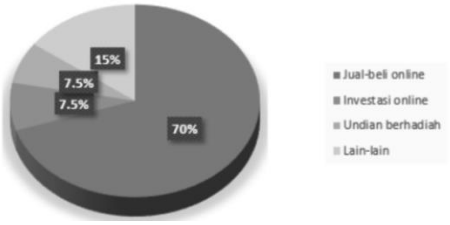
[8] Suparni, Niniek. *Cyberspace Problematika Dan Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009, hal. 5.

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

Berikut gambaran kasus yang ditangani Subdit V Cyber Crime Polda Jatim.



Gambar 1. Grafik Modus Penipuan Online yang Dilaporkan ke Polda Jatim Tahun 2021

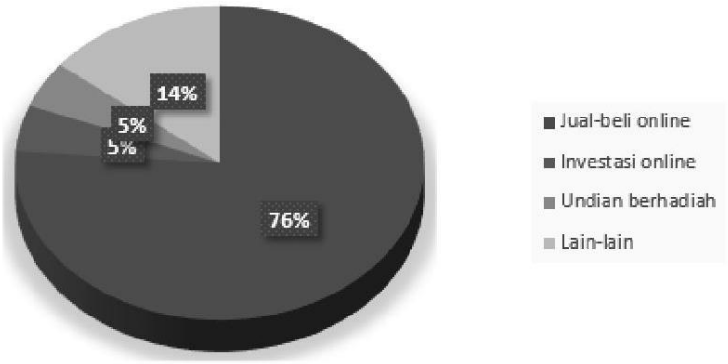
Data yang didapatkan dari penelitian, diketahui dari 176 laporan tindak pidana penipuan daring masuk Polda Jatim di tahun 2021, sejumlah 60 kasus terselesaikan, sedangkan 116 kasus tidak terselesaikan dan sisanya masih dalam tahap penyelidikan dan penyidikan. Di tahun 2022 terdapat 29 laporan tindak pidana penipuan daring yang masuk Polda Jatim, yang pada saat penelitian dilakukan, 5 kasus masih dalam proses penyelidikan dan penyidikan.

Mengenai sarana yang digunakan, data tindak pidana penipuan daring untuk tahun 2021 adalah sebagai berikut:

Tabel 2 Data Kasus Penipuan Online yang Dilaporkan ke Polda Jatim Tahun 2021

No	Jenis Penipuan	Jumlah Laporan yang Masuk
1.	*Web Fraud* (Penipuan dengan media Web/ *Website*)	108 Laporan
2.	*Email Fraud* (Penipuan dengan media Email)	10 Laporan
3.	*Telephone Fraud* (Penipuan dengan media Telepon)	21 Laporan
4.	*SMS Fraud* (Penipuan dengan media SMS)	36 Laporan
5.	*Credit Card Fraud* (Penipuan kartu kredit)	1 Laporan
Total Laporan Tindak Pidana Penipuan Daring yang Masuk		**176 Laporan**

Selain itu, data tindak pidana penipuan online terkait sarana untuk kuartal pertama tahun 2022.



Gambar 2. Statistik Modus Penipuan Online yang Dilaporkan ke Polda Jatim Kuartal Pertama Tahun 2022

Mengenai sarana yang digunakan, data tindak pidana penipuan online atau daring untuk kuartal pertama tahun 2022 adalah sebagai berikut:

Tabel 3 Data Kasus Penipuan Daring yang Dilaporkan ke Polda Jatim Kuartal Tahun 2022

No	Jenis Penipuan	Jumlah Laporan yang Masuk
1.	*Web Fraud* (Penipuan dengan media Web/ *Website*)	15 Laporan
2.	*Email Fraud* (Penipuan dengan media Email)	1 Laporan
3.	*Telephone Fraud* (Penipuan dengan media Telepon)	7 Laporan
4.	*SMS Fraud* (Penipuan dengan media SMS)	6 Laporan
5.	*Credit Card Fraud* (Penipuan kartu kredit)	0 Laporan
Total Laporan Tindak Pidana Penipuan Daring yang Masuk		**29 Laporan**

Penipuan menggunakan media laman situs (terutama medsos dan merchant online) jumlah laporannya mendominasi dibandingkan modus yang lain. Distribusi informasi menggunakan laman situs adalah hal yang sangat umum di era perdagangan daring saat ini. Secara sederhana membuat sebuah laman situs juga tergolong mudah, ada yang versi gratis dan ada juga yang berbayar. Laman situs versi gratis umum disebut dengan blog. Blog yang cukup popular digunakan pelaku penipuan daring adalah blogspot, karena pembuatannya yang relatif mudah.

Website yang digunakan untuk menipu biasanya menggunakan domain gratis atau murah meriah yang harganya 10 – 20 ribu rupiah. Atau bisa juga menggunakan domain luar negeri bukan lokal. Contoh domain murah yang sering digunakan : .xyz; .cf; .ml ; .ga; .gk; .tk. Salah satu contoh blog adalah pindadsenjata.blogspot.co.id, yang adalah website yang beriklan menjual senjata api tetapi menipu konsumennya dengan modus penipuan “non-delivery”. Dulu saat kaskus masih populer maka Laman Kaskus juga merupakan laman jual-beli yang sangat sering digunakan untuk melakukan

penipuan. Bahkan di Kaskus, pembeli dan penjual memiliki istilah khas untuk berkomunikasi.

Di Kaskus, sebenarnya ada mekanisme verifikasi untuk kredibilitas penjual, namun tidak semua pencari informasi mengetahui hal ini. Hal inilah yang dimanfaatkan oleh pelaku penipuan untuk menjaring korban-korban yang kurang terinformasi dengan baik. Laman situs jual beli daring semakin banyak seiring berjalannya waktu, mulai dari yang lokal yaitu tokobagus. com yang berganti nama domain menjadi olx. co.id, bukalapak.com, tokopedia.com, shopee.com dan yang internasional seperti Ebay, Amazon dan lain-lainnya. Hampir semua memiliki cara preventif untuk mencegah penipuan namun tidak semua penggunanya mengerti dengan baik.

Berbelanja secara daring melalui cara selancar laman situs memberikan kenyamanan bagi kebanyakan penggunanya. Pembeli tidak perlu lagi repot-repot pergi ke pusat perbelanjaan dan berkeliling, cukup dengan belanja menggunakan laptop atau ponsel pintar, kemudian menghubungi penjual, transfer pembayaran, dan barang akan muncul di depan pintu kita diantar kurir/jasa pengiriman. Umumnya, setelah korban melihat informasi berupa iklan dalam website, mereka akan menghubungi penjual (yang adalah pelaku) secara personal menggunakan kontak yang dicantumkan penjual di website tersebut.

Segala kegiatan transaksi daring dilakukan menggunakan teknologi informasi komunikasi, termasuk penawaran-penerimaan-kesepakatan. Bahkan semua itu dilakukan tanpa tatap muka. Mengingat karakteristik tindak pidana penipuan daring yang faceless, penyidik menemukan bahwa pelaku penipuan adalah orang yang menggunakan identitas palsu atau dapat dikatakan sebagai subyek hukum fiktif, yang mengakibatkan kasus penipuan daring sulit diteruskan ke proses penuntutan. Oleh karena itu, keberadaan informasi elektronik dan/ atau dokumen elektronik memegang peranan penting sebagai alat bukti.

Shopee, Tokopedia, Lazada yang merupakan merchant online berusaha keras untuk mengatasi berbagai persoalan penipuan yang diantara cara mengatasi penipuan jual beli online adalah dengan menyediakan rekening bersama yang merupakan rekening “penampungan dana sementara” dari pembeli yang kemudian akan diteruskan

pada penjual jika pembeli telah menerima barang dengan baik. Tetapi tetap saja para penipu masih bisa mencari celahnya.

Mekanisme Penanganan Tindak Pidana Penipuan Dalam Transaksi E-Commerce

Adapun tata cara penanganan oleh Subdit V Cyber Crime Ditreskrimsus Polda Jatim terdiri dari beberapa tahapan sebagaimana dijelaskan berikut :

1. **Tahapan Pelaporan**

Pelapor yang merasa telah tertipu dalam bertransaksi jual beli secara online saat melapor ke SPKT Polda Jatim hendaknya menyiapkan bukti transaksi, bukti salinan email, print out direct message, sms atau chat Whatsapp, maupun thread seller di FJB. Pelapor juga sebisa mungkin menyiapkan data pihak yang sudah menipu, seperti nomor rekening dan nama pemilik rekening, jika perlu nomor handphone/telpon, email atau website. Pelapor juga hendaknya menyiapkan bukti transfer bank, sms banking, atau internet banking. Selanjutnya Petugas akan membuat laporan yang berisi identitas pelapor dan terlapor,uraian singkat kejadian dan pasal yang dikenakan. Selanjutnya Pelapor akan menerima sebuah Surat Tanda Penerimaan Laporan (STPL) sebagai bukti anda telah melaporkan tindak pidana yang dialami. Pelapor juga akan dibuatkan Surat Permintaan penutupan rekening atau pemanggilan Pelaku ke Bank.

2. **Tahap Penyelidikan dan Penyidikan**

Kegiatan penyelidikan dapat dilakukan oleh penyidik atau menerima informasi dari pihak pelapor, dilanjutkan dengan pembuatan laporan polisi serta surat perintah tugas dan surat perintah penyelidikan, dan / berkoordinasi dengan pihak ISP (internet service provider), Provider Seluler dan Monitoring Center (bareskrim Polri) untuk meminta data log file dan call detail record dan target yang akan di Lidik. Selanjutnya adalah Membuat laporan polisi model B. disusul kemudian dengan membuat surat perintah penyelidikan dan penyidikan. Proses selanjutnya adalah memeriksa saksi korban dengan meminta bukti adanya penipuan yang dialami. Sesuai dengan modus yang ada, penyidik melakukan penyelidikan dengan cara :

a) Mengaplikasikan metode lidik klasik (konvensional) ke dunia on-line

b) Under cover (penyamaran) on-line, siapkan alamat surel, akun, user ID samaran.
c) Melakukan komunikasi on-line melalui chat, email untuk mendapatkan header pelaku.
d) Lacak header guna mengetahui IP Address pelaku.
e) Menggunakan tools yang tersedia di Internet untuk mengetahui ISP yang digunakan.
f) Merngumpulkan data pelaku sebanyak mungkin, gunakan search engine google, facebook, instagram, telegram, dsb.
g) Untuk koordinasi dengan Pihak Provider, biasanya akan dibutuhkan waktu sampai 2 minggu sampai pihak provider mengeluarkan Call detail Record (CDR).

Permintaan data atau biasa disebut sebagai permintaan "rekaman" atau bisa juga disebut permintaan Call Data Record ("CDR") terkait penggunaan jasa telekomunikasi diatur secara jelas berdasarkan Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (UU Telekomunikasi). Penyelenggara Jasa Telekomunikasi (operator) berdasarkan Pasal 18 UU Telekomunikasi dan Pasal 16 Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi wajib mencatat/ merekam secara rinci pemakaian jasa telekomunikasi yang digunakan oleh pengguna telekomunikasi.

Pemberian rekaman berdasarkan perspektif UU Telekomunikasi dibagi 2 (dua), yaitu pemberian rekaman kepada pengguna jasa telekomunikasi dalam rangka pembuktian kebenaran pemakaian fasilitas telekomunikasi dan pemberian rekaman untuk keperluan proses peradilan pidana.

Berdasarkan Pasal 41 UU Telekomunkasi, terdapat 2 (dua) jenis perekaman yang diatur yaitu:

a) Perekaman Pemakaian Fasilitas Telekomunikasi yaitu perekaman yang dilakukan penyelenggara jasa telekomunikasi yang bersifat wajib (mandatory) untuk keperluan pengguna jasa telekomunikasi itu sendiri, seperti perekaman rincian data tagihan (billing) dan lain-lain.

b) Perekaman Informasi yaitu perekaman informasi tertentu yang diatur sesuai peraturan perundang-undangan, seperti rekaman percakapan antarpihak yang bertelekomunikasi.

Kendali dari Pasal 41 UU Telekomunikasi tersebut terdapat pada Pasal 42 UU Telekomunikasi, yang mana operator telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya. Sanksi jika operator tidak menjaga kerahasiaan tersebut adalah pidana penjara paling lama 2 (dua) tahun dan atau denda paling banyak Rp 200 juta (Pasal 57 UU Telekomunikasi).

Berkaitan dengan perkembangan teknologi informasi dan komunikasi, penggeledahan secara fisik (*physical search*: rumah) dengan penggeledahan digital (*digital search*: komputer atau media teknologi informasi dan komunikasi) dalam beberapa hal mempunyai kesamaan. Dalam keduanya, Penyidik berusaha untuk menemukan dan mengambil informasi yang berguna dan tersembunyi di dalam tempat tertutup. Namun demikian menurut Orin S. Kerr pada saat yang sama, pergeseran dari penggeledahan secara fisik ke penggeledahan digital terdapat beberapa perbedaan prinsipil dengan implikasi penting terhadap aturan hukum. Proses penggeledahan digital jauh berbeda dengan proses penggeledahan secara fisik.[9]

Dalam UU ITE ketentuan mengenai penggeledahan dan penyitaan terhadap sistem elektronik terdapat dalam Pasal 43 ayat (3). Pengaturan tersebut berkaitan dengan prosedur yang harus ditempuh penyidik dalam melakukan penggeledahan dan penyitaan. Pengaturan tersebut dimaksudkan agar tindakan penggeledahan dan penyitaan yang dilakukan oleh penyidik sah menurut hukum dan adanya perlindungan privasi warga masyarakat dari penyalahgunaan wewenang oleh penyidik. Pengaturan penggeledahan dan penyitaan alat bukti digital sangat penting karena alat bukti digital rentan untuk dimanipulasi, hilang atau berubah dan terkait dengan aktivitas sistem elektronik untuk kepentingan publik yang harus terus berjalan.

[9]Orin S. Kerr, "Search Warrants in An Area of Diigital Evidence", *Missisipi Law Journal Vol. 75, Missisipi*, 2005

Prosedur penggeledahan dan penyitaan yang diatur dalam Pasal 43 ayat (3) dan ayat (4) UU ITE adalah: "penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat" dan "dalam melakukan penggeledahan dan/atau penyitaan penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum." Secara umum dalam melakukan penyidikan di bidang teknologi informasi dan komunikasi harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, integritas data, atau keutuhan data.

Dalam KUHAP yang dimaksud dengan penggeledahan sebagaimana diatur dalam Pasal 32 s.d. Pasal 37 adalah penggeledahan terhadap rumah, pakaian atau badan. Dengan demikian maka tata cara penggeledahan yang harus ditempuh oleh penyidik adalah tata cara penggeledahan fisik dan tidak mengatur penggeledahan digital atau elektronik. Walaupun komputer atau perangkat teknologi informasi dan komunikasi yang menyimpan dokumen atau informasi elektronik berada dalam rumah atau suatu tempat atau dibawa tersangka atau seseorang sehingga dapat termasuk objek penggeledahan, namun komputer atau perangkat teknologi informasi dan komunikasi tersebut belum mempunyai nilai sebagai alat bukti karena menjelaskan atau membuktikan sesuatu sampai informasi yang tersimpan dalam perangkat komputer atau teknologi informasi dan komunikasi tersebut diungkap. Untuk menggeledah perangkat komputer atau teknologi informasi dan komunikasi dan mengungkap dokumen atau informasi elektronik yang tersimpan di dalamnya memerlukan prosedur khusus karena sebagaimana diuraikan di atas penggeledahan secara digital/elektronik memiliki karakteristik yang berbeda.

Setelah melakukan upaya paksa berupa penggeledahan, penyitaan dan penangkapan terhadap para pelaku, penyidik melakukan olah TKP terhadap barang bukti digital dengan pemeriksaan barang bukti digital di TKP dilakukan secara digital forensik yang dilakukan oleh petugas dari Unit Cyber Crime dan memperhatikan tata cara dan prosedur permintaan dan penyerahan barang bukti digital.

Mengenai Prosedur permintaan bantuan pemeriksaan bukti digital kepada Laboratorium Forensik Komputer Unit V Cyber Crime, maka prosesnya adalah sebagai berikut:[10]

1) Penyidik membuat surat yang ditandatangani oleh Kepala Kesatuan Kewilayahan dan ditujukan kepada Kabareskrim Polri Up. Dir Tipideksus, perihal permintaan bantuan pemeriksaan laboratoris kriminalistik Barang Bukti Digital;
2) Tembusan surat kepada Kabareskrim dan Kanit V Cyber Crime.
3) Isi surat menjelaskan data yang dibutuhkan oleh Penyidik dari Bukti Digital dengan menyebutkan kata kunci/keyword tertentu. (contoh : jika yang dicari merupakan dokumen elektronik, penyidik harus memberikan nama dokumen elektronik yang akan dicari secara benar).
4) Surat permintaan dilampiri:
    - Laporan Polisi;
    - BA Penyitaan Barang Bukti;
    - BA Pembungkusan/Penyegelan Barang Bukti;
    - Laporan Kemajuan (Resume).
5) Barang bukti dibungkus dengan plastik antistatik dan diantarkan langsung ke Unit V Cyber Crime.

Mengenai tahapan pada proses implementasi pemeriksaan digital pada Laboratorium forensik Polda Jatim, secara garis besar dapat diklasifikasikan kepada empat tahapan, yaitu:

1. Identifikasi bukti digital
2. Penyimpanan bukti digital
3. Analisa bukti digital
4. Presentasi

[10] SOP Penyidikan Kejahatan Siber Polda Jatim

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 bukti-bukti 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:[11]

a) Identitas lengkapnya
b) Riwayat hidupnya
c) Kronologi perbuatan tersangka dalam hal melakukan penipuan melalui media elektronik.
d) Kemampuan menjalankan komputer,gadget dan media elektronik yang terhubung dengan Internet dan lain-lain sesuai dengan kasus.
e) 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:[12]

a) proses saling mengenal dengan tersangka;
b) apa saja yang membuat saksi menjadi merasa ditipu;

[11] SOP Penyidikan Cyber Crime Polda Jatim
[12] SOP Penyidikan Cyber Crime Polda Jatim

c) apa saja kerugian yang dialaminya;
d) melalui media apa perbuatan itu dilakukan;
e) dan lain-lain sesuai dengan kasus.

Setelah melakukan rangkaian pemeriksaan terhadap barang bukti, saksi maupun korban, penyidik meminta keterangan kepada saksi ahli dari Depkominfo:[13]

a) kepada ahli bidang hukum khusus Undang-undang Informasi dan Transaksi Elektronik tentang pemenuhan unsur pasal yang disangkakan;
b) 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.

III. PENUTUP

3.1 Kesimpulan

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 denga 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 berkutnya adalah dengan pura-pura meminta OTP guna membobol rekening korbannya. Selanjutnya ada modus penipu yang berpura-pura dari bea cukai dan meminta tambahan pemabayaran 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

[13] SOP Penyidikan Cyber Crime Polda Jatim

konfensional 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 Reskrimum. Sehingga agar tidak terjadi hal demikian maka digunakanlah UU ITE agar kasus benar-benar bisa ditangani oleh Ditreskrimsus.

DAFTAR PUSTAKA

Bareskrim Bekuk Sindikat Penipu Online di Bawah Umur, https://news.detik.com/berita/d-5178806/bareskrim-bekuk-sindikat-penipu-online-di-bawah-umur, diakses tanggal 11 Oktober 2020.

Barda Nawawi Arief, *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.

Kholiq, 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.

Kholiq, 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 Warrants in An Area of Diigital Evidence", *Missisipi Law Journal Vol. 75, Missisipi*, 2005

Pusat Data dan Sarana Informatika Kementerian Komunikasi dan Informatika, *Laporan Potret Belanja Online di Indonesia*. Pusat Data dan Sarana Informatika Kementerian Komunikasi dan Informatika. Jakarta, 2013, hal. 3

Satria Nur Fauzi dan Lushiana Primasari, *Tindak Pidana Penipuan Dalam Transaksi Di Situs Jual Beli Online (E-Commerce),* Recidive Volume 7 No. 3, Sept.- Des. 2018, hal. 251.

SOP Penyidikan Cyber Crime Polda Jatim

SOP Penyidikan Kejahatan Siber Polda Jatim

Suparni, Niniek. *Cyberspace Problematika Dan Antisipasi Pengaturannya*, Sinar Grafika, Jakarta, 2009, hal. 5.

Tb. R. Nitibaskara, "Problema Yuridis Cybercrime' Makalah pada Seminar Cyber Law, diselenggarakan oleh Yayasan Cipta Bangsa, Bandung, Juli 2000, hal. 2.

Thalib, Prawitra, Faizal Kurniawan, and Mohamad Nur Kholiq. "The Application of Quranic Interpretation, of Sunnah And Ijtihad As The Source Of Islamic Law." *Rechtidee Jurnal Hukum* 15.2 (2020): 193-206.

Thalib, Prawitra, et al. "Bantuan Sosial Sedekah Nasi Bungkus di Masa Pandemi Covid-19 Oleh Pusat Pengelolaan Dana Sosial." *ABDI MOESTOPO: Jurnal Pengabdian Pada Masyarakat* 5.1 (2022): 100-108.

Thalib, Prawitra, Tri Veny Putri, and Mohamad Nur Kholiq. "Board Gender Diversity, Institutional Ownweship, and Divident Policy in Indonesia." (2021): 190-198.

Thalib, Prawitra, AUFAR FADLUL HADY, and Muhammad Nur Kholiq. "Esensi Hukum Bisnis Syariah." (2021).

Thalib, Prawitra, et al. "PEMANFAATAN SUMBER DAYA ALAM YANG BERKESINAMBUNGAN YANG BERORIENTASI PADA PENCAPAIAN PROFIT YANG MEMBAWA KEMASLAHATAN BAGI LINGKUNGAN." *Jurnal Layanan Masyarakat (Journal of Public Services)* 5.2 (2021): 456-462.

Thalib, Prawitra, et al. "PEMANFAATAN SUMBER DAYA ALAM YANG BERKESINAMBUNGAN YANG BERORIENTASI PADA PENCAPAIAN PROFIT YANG MEMBAWA KEMASLAHATAN BAGI LINGKUNGAN." *Jurnal Layanan Masyarakat (Journal of Public Services)* 5.2 (2021): 456-462.

Thalib, Prawitra, et al. "5C Principles in Profit and Loss Sharing Financing on Baitul Maal Wattamwil as Islamic Micro Finance In Indonesia." *Substantive Justice International Journal of Law* 3.2 (2020): 196-210.

Thalib, Prawitra, et al. "THE URGENCE REGULATION OF BUSINESS ACTIVITIES ON ISLAMIC MICROFINANCE INSTITUTION ACCORDING LAW NO. 1 YEAR 2013 OF MICROFINANCE INSTITUTIONS." *Arena Hukum* 14.2 (2021): 207-221.

Thalib, Prawitra, et al. "Company Policy on Termination of Employment at Pandemic Covid-19 From a Fair and Justice Perspective." *The 2nd International Conference of Law, Government and Social Justice (ICOLGAS 2020)*. Atlantis Press, 2020.

Thalib, Prawitra, et al. "Post-Mining Reclamation as An Environmental Policy: A Gold Mining Case Study." *Jurnal Halu Oleo Law Review* 4.2 (2020): 208-218.

Thalib, Prawitra, Eva Diana, and Mohamad Nur Kholiq. "Pengabdian Masyarakat melalui Pemeriksaan Kesehatan Gratis GeNose C19 pada Santri Pondok Pesantren Nurul Khidmah Surabaya." *Janaloka* 1.1 (2022): 28-38.

Thalib, Prawitra, Eva Diana, and Mohamad Nur Kholiq. "Pemeriksaan Kesehatan Gratis GeNose C19 pada Santri Pondok Pesantren Nurul Khidmah Surabaya Oleh Pusat Pengelolaan Dana Sosial Universitas Airlangga."

Wisudanto, Wisudanto, et al. "Social Action Of Student In Achieving Non-Academic Achievements In Interest And Talent-Based School." *Airlangga Development Journal* 6.1 (2022): 55-65.

Winarsi, Sri, et al. "Sharia banking dispute resolution in Indonesia after the verdict of the constitutional court no. 93/puu-x/2012." *Utopía y Praxis Latinoamericana* 26.2 (2021): 408-416.

Wijoyo, Suparto, Prawitra Thalib, and Mohamad Nur Kholiq. "Merekonstruksi Good Corporate Governance Dalam Rangka Mewujudkan Indonesia Incorporated Sebagai Negara Kesejahteraan (Perspektif Regulasi-Deregulasi-Reregulasi Model Jatimnomic)." *Airlangga Development Journal* 6.1 (2022): 44-54.

Widodo, *Sistem Pemidanaan Dalam Cybercrime*, Laksbang Mediatama, Yogyakarta, 2009, hal. 24