Analisis Yuridis Terhadap Tindak Pidana Penipuan di dalam Penggunaan Media Sosial

Swangga Prabhaswara
Fakultas Hukum
Universitas Islam Batik Surakarta
swnggap@gmail.com

ABSTRAK

Latar belakang ini adalah penipuan yang terjadi di media sosial merupakan salah satu bentuk kejahatan yang berada ditengah masyarakat. Tindak pidana penipuan melalui media sosial saat ini semakin sering terjadi, hal ini mengakibatkan turunnya tingkat kepercayaan media sosial. Penelitian ini mengkaji tidak pidana kejahatan tindak pidana penipuan di media sosial. Penelitian ini menggunakan pendekatan penelitian yang bersifat deskriptif normatif. Jenis data yang digunakan adalah konten di media sosial, dan dokumen-dokumen. Semua orang memiliki kemungkinan untuk melakukan tindak pidana lewat beragam cara dan media, termasuk media sosial. Media sosial merupakan tempat masyarakat saat ini saling berinteraksi satu sama lain, dan tidak terhalang oleh waktu, dan tempat.Media sosial memberikan wadah bagi pengguna nya untuk saling bertukar informasi dan bahkan berdiskusi. Tindak pidana pada dasarnya tindakan yang dilarang oleh suatu aturan hukum larangan dan disertai ancaman (sanksi) yang berupa pidana tertentu, bagi barangsiapa melanggar larangan tersebut. Unsur-unsur tindak pidana dalam KUHP terbagi menjadi dua jenis, yaitu unsur-unsur subjektif dan unsur-unsur objektif. Hal ini sebagaimana pendapat Lamintang yang menyatakan bahwa unsur-unsur subjektif dan unsur-unsur objektif sama-sama menyangkut pada diri si pelaku. Pengertian media sosial itu sendiri adalah sebuah Online Social Networking atau situs jejaring sosial yang diciptakan untuk memberikan fasilitas teknologi dengan maksud pengguna dapat bersosialisasi atau berinteraksi dalam dunia maya. Pengertian yang lain dari media sosial adalah, sebuah situs komunikasi (dimana kita dapat bertemu orang dan bersosialisasi di dunia maya), bisa disebut dengan jejaring sosial atau Social Networking Website. Hasil penelitian menunjukkan bahwa terdapat penipuan di media sosial. Dalam penelitian ini penulis menemukan beberapa bentuk penipuan di media sosial berupa penipuan terhadap anak dibawah umur. Selain itu, berdasarkan penelitian yang telah dilakukan, penipuan di media sosial juga ditemukan dalam hal transaksi elektronik dan dokumen elektronik berupa jaringan penipuan berkedok online shop. Terkait dengan penanggulangan penipuan di media sosial, Kepolisian Indonesia selalu melakukan pengamanan terhadap jaringan penipuan di media sosialsehingga tidak lagi meresahkan masyarakat. Penulis menyarankan adanya penegakan hukum yang lebih baik berupa ketegasan dalam penegakan pasal-pasal yang mengatur berbagai hal tentang tindak pidana penipuan, terutama pasal 378 KUHP dan Pasal 28 ayat (1) tentang Informasi dan Transaksi Elektronik. Penulis menyarankan peningkatan kewaspadaan terhadap penipuan berbasis online dengan caramenggunakan media sosial selektif dan seefektif mungkin.

Kata Kunci: Hukum, Media Sosial; Penipuan; Tindak Pidana.

A. PENDAHULUAN

Teknologi informasi dan komunikasi saat ini telah berkembang dengan pesat, sehingga setiap masyarakat dapat memperluas aktivitasnya melalui dunia teknologi. Dengan munculnya teknologi informasi, setiap orang juga dapat mengakses, memperoleh informasi, serta menambah jaringan yang sangat luas, sehingga tidak dapat dipungkiri bahwa hal ini juga akan menyebabkan pada perubahan sosial yang sangat signifikan. Meski demikian,

munculnya teknologi informasi dan komunikasi tidak hanya memberikan dampak positif semata, melainkan juga banyak dampak-dampak negatif yang muncul disebabkan penyalahgunaan media elektronik hingga menyebabkan munculnya cybercrimes sehingga diperlukan adanya payung hukum dalam penggunaan teknologi informasi dan komunikasi.

Peranan teknologi informasi dan komunikasi di era globalisasi telah menempatkan pada posisi yang amat strategis karena menghadirkan suatu dunia tanpa batas, jarak, ruang, dan waktu, yang berdampak pada peningkatan produktifitas dan efisiensi. Pengaruh globalisasi dengan penggunaan sarana teknologi informasi dan komunikasi telah mengubah pola hidup masyarakat dan berkembang dalam tatanan kehidupan baru dan mendorong terjadi nya perubahan sosial, ekonomi, budaya, pertahanan, keamanan, dan penegakan hukum.

Teknologi informasi dan komunikasi ini, telah dimanfaatkan dalam kehidupan sosial masyarakat, dan telah memasuki berbagai sektor kehidupan baik dari sektor pemerintahan, sektor bisnis, perbankan, pendidikan, kesehatan, dan kehidupan pribadi. Manfaat teknologi informasi dan komunikasi selain memberikan dampak positif juga didasari memberi peluang untuk dijadikan sarana melakukan tindak kejahatan-kejahatan baru *(cybercrimes)* sehingga diperlukan upaya proteksi. Sehingga dapat dikatakan bahwa teknologi informasi dan komunikasi bagaikan pedang bermata dua, dimana selain memberikan kontribusi positif bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, tetapi juga menjadi sarana potensial dan sarana efektif untuk melakukan perbuatan melawan hukum.

Masyarakat Indonesia yang majemuk membuat kondisi sosial masyarakat tidak terhindarkan dari berbagai gejolak. Kemajemukan masyarakat menimbulkan adanya perbedaan sifat dan kepribadian dari masing-masing individu. Hal itu menciptakan interaksi yang berdampak kurang baik bagi masyarakat umum. Interaksi yang kurang baik tersebut merupakan dampak dan norma dari hukum yang dilanggar. Berdasarkan hukum yang berlaku, pelanggaran terjadi ketika seseorang melakukan tindak pidana. Menurut Moeljatno seseorang dianggap melanggar hukum jika seseorang tersebut melakukan tindakan yang melawan aturan dan dapat terkena pidana.

Terkait dengan hal tersebut, semua orang memiliki kemungkinan untuk melakukan tindak pidana lewat beragam cara dan media, termasuk di dalam penggunaan media sosial. Media sosial merupakan tempat masyarakat saat ini sebagai sarana berkomunikasi dan melakukan segala hal, berinteraksi satu sama lain, tidak terhalang oleh waktu dan tempat. Media sosial memberikan wadah bagi para penggunanya untuk saling bertukar informasidan bahkan berdiskusi. Facebook, Twitter, Instagram, Youtube, dan Blog adalah contoh media sosial yang digunakan oleh masyarakat.

Sementara itu, Van Dijk mengidentifikasikan media sosial sebagai sebuah platform yang memberikan penggunanya untuk sekedar menuruti dorongan eksistensi atau bahkan membangun kerjasama antar pengguna. Oleh karena itu, media sosial yang sekarang ini telah menjadi dunia baru atau dunia kedua bagi masyarakat, akan memancing adanya pelanggaran tindak pidana. Salah satu media sosial yang banyak digunakan oleh masyarakat saat ini adalah Facebook. Menurut Wikipedia berbahasa Indonesia, Facebook adalah sebuah layanan jejaring sosial dan situs web yang diluncurkan pada 4 Februari 2004. Facebook didirikan oleh Mark Zuckerberg, seorang mahasiswa Harvard kelahiran 14 Mei 1984. Saat ini pengguna Facebook merupakan paling banyak yang ada di dunia dengan angka 34 juta pengguna aktif di seluruh dunia.

Selain itu, dari tahun ke tahun Facebook juga menjadi media sosial yang paling banyak dikunjungi di dunia dan menjadi sarana media sosial yang sangat berpengaruh.

Karena mudah dijangkau oleh siapa saja, tidak adanya system keamanan yang ketat untuk menyeleksi pengguna yang cakap hukum, serta mampu menggunakannya dengan bijak membuat banyak orang ingin menggunakan sarana media sosial ini untuk melakukan apapun yang mereka inginkan, baik dari segi positif maupun negatif. Perbuatan melawan hukum di dunia maya merupakan sebuah fenomena yang mengkhawatirkan, mengingat ada banyak sekali bullying, hacking, penyebaran informasi destruktif, bahkan sampai penipuan yang dilakukan melalui media sosial telah menjadi aktivitas yang sering dilakukan para pelaku kejahatan di dunia maya.

Kenyataan itu demikian sangat kontras dengan minimnya pengawalan regulasi yang mengatur tentang pemanfaatan teknologi informasi dan komunikasi di berbagai sektor. Adanya media sosial membuat interaksi antar individu dan juga kelompok menjadi lebih mudah dan dapat dilakukan di mana saja. Menurut Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik atau yang biasa disebut dengan UU ITE dalam Pasal 1 ayat (6) menyatakan bahwa:

"Penyelenggaraan system elektronik adalah pemanfaatan system elektronik oleh penyelenggara negara, orang, badan usaha, dan/atau masyarakat".

Serta dalam Pasal 28 ayat (1) juga telah menjabarkan mengenai sanksi yang diberikan kepada perbuatan yang melawan hukum dalam lingkup penggunaan media sosial elektronik yang berbunyi:

"Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik dipidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp.1 miliar".

Atas latar belakang di atas, penulis memiliki ketertarikan untuk mengkaji lebih lanjut akan adanya pelanggaran pidana di media sosial yang diambil dunia maya. Melihat fenomena yang saat ini terjadi telah banyak sekali tindak pidana yang telah dilakukan melalui media sosial, salah satu contoh yang paling banyak di dalamnya adalah Facebook. Karena Facebook merupakan media yang memiliki peluang besar untuk pelaku tindak pidana melancarkan aksi nya. Banyaknya penipuan yang terjadi di media sosial tersebut juga dampak dari masyarakat yang kurang selektif dan teliti dalam bertindak, sehingga banyak sekali korban yang mendapatkan kerugian besar dari hal itu. Oleh karena itu, penulis telah menemukan banyak sekali indikasi mengenai pelanggaran yang terjadi antara lain adalah penipuan yang dilakukan dalam penggunaan media sosial yang mengakibatkan kerugian besar bagi korban nya seperti yang telah dijelaskan tadi yang peristiwanya terus berulang setiap tahun nya dan selalu meningkat.

Pada data Kementerian Informasi dan Informatika telah mencatat dari tahun 2017 sampai dengan tahun 2022 juga menerima laporan dari masyarakat terkait dengan adanya tindak pidana informasi dan transaksi elektronik, yang berjumlah kurang lebih 405.000 laporan mengenai penipuan di dalam penggunaan media sosial. Selain itu, dengan adanya UU ITE dari awal di berlaku kan juga telah semakin menjelaskan bahwa ada banyaknya pelanggaran yang telah dilakukan dalam interaksi yang berada di media sosial. Penulis juga menemukan banyak sekali indikasi bahwa adanya pelanggaran pidana melalui berbagai media sosial yang dapat dianalisis dari segi hukum pidana, sehingga menarik perhatian penulis untuk meneliti fenomena adanya pelanggaran pidana di dalam media sosial. Berdasarkan hal tersebut penulis menyusun penelitian dengan judul: "ANALISIS YURIDIS TERHADAP TINDAK PIDANA PENIPUAN DI DALAM PENGGUNAAN MEDIA SOSIAL".

Berdasarkan latar belakang yang telah penulis uraikan di atas, maka ditemukan

perumusan masalah sebagai berikut: 1. Apakah pengaturan UU ITE telah memberikan jaminan penegakan hukum terhadap penipuan di dalam penggunaan media sosial?, 2. Bagaimanakah upaya yang telah dilakukan dalam menekan angka tindak pidana penipuan di dalam penggunaan media sosial sehingga dapat berkurang dalam pelaksanaannya?. Berdasarkan rumusan masalah yang disusun, maka penelitian ini memiliki tujuan sebagai berikut: Mengetahui penyebab sering terjadinya penipuan dan dasar-dasar hukum yang diberlakukan kepada pelaku tindak pidana penipuan di dalam penggunaan media sosial, mengetahui berbagai macam bentuk upaya yang dilakukan dalam menekan dan menangani tindak pidana penipuan di dalam penggunaan media sosial.

Manfaat yang diharapkan sebagaimana tujuan yang dicapai dari penelitian ini dapat dikemukakan sebagai berikut: Secara teoritis, dalam penelitian ini menjelaskan tindak pidana yang berada di media sosial berupa penipuan. Penelitian ini juga menjelaskan berbagai penyebab terjadinya tindak pidana penipuan yang beredar di media sosial, Secara praktis, hasil dari penelitian ini akan menjelaskan berbagai macam penyebab tindak pidana penipuan yang berada di media sosial dan memberikan referensi bagi peneliti tentang seperti apa upaya yang dapat di lakukan untuk mencegahnya.

B. METODE PENELITIAN

1. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian hukum normatif. Penelitian ini menitikberatkan pada berbagai aspek teori, filosofi, perbandingan, struktur, atau komposisi, serta penjelasan tiap pasal yang berlaku. Metode ini menggunakan kajian yang bersifat kualitatif untuk mengkaji berbagai hal terjadi, berdasarkan teori-teori dan pasal-pasal yang berlaku sehingga menghasilkan data yang valid dan faktual. Penelitian normatif juga memiliki tujuan untuk mengkaji berbagai teori-teori dan peraturan yang tertulis dengan fenomena yang terjadi dilapangan sehingga data yang dihasilkan juga relevan dengan aturan yang berlaku.

Metode penelitian hukum normatif juga merupakan penulisan yang menggunakan bahan atau data sekunder. Data sekunder adalah bahan atau data yang diperoleh dari penelitian kepustakaan (*library research*) bertujuan untuk mendapatkan konsep-konsep, teori-teori dan informasi-informasi serta pemikiran konseptual dari penelitian pendahulu baik berupa peraturan perundang-undangan dan karya ilmiah lainnya. Data sekunder bisa mencakup bahan hukum primer, bahan hukum sekunder dan bahan hukum tersier.

2. Sifat Penelitian

Penelitian ini adalah penelitian deskriptif kualitatif. Penelitian deskriptif kualitatif pada penelitian ini menunjuk pada perbandingan antara fenomena penipuan di media sosial dengan teori dan aturan perundang- undangan yang berlaku. Adapun cara yang biasa dilakukan adalah dengan mengumpulkan data, lalu menyusun nya, lalu mengklasifikasikan nya, lalu menganalisis, dan menginterpretasikan. Penulis ingin mengidentifikasi gejala-gejala yang diteliti dengan teori dan aturan perundang-undangan yang berlaku untuk mendekati objek penelitian maupun permasalahan yang telah dirumuskan sebelumnya.

3. Jenis Data

Jenis data yang digunakan adalah konten yang berada di media sosial, dokumen, dan foto yang terkait dengan fenomena penipuan di media sosial. Data-data tersebut merupakan data sekunder. Peneliti menggunakan data sekunder dikarenakan penelitian

ini merupakan penelitian normatif yang melakukan penelitian bersifat kepustakaan, yaitu melakukan kajian terhadap teori atau peraturan perundang-undangan untuk melakukan kajian lebih mendalam terhadap fenomena yang terjadi di lapangan. Bahan hukum sekunder juga diperinci ke dalam berbagai macam tingkatan, yaitu:

a. Bahan hukum primer, yaitu bahan hukum yang terdiri atas peraturan perundang-undangan, risalah resmi, putusan pengadilan, dan dokumen resmi.
b. Bahan hukum sekunder, bahan hukum yang terdiri atas; buku hukum, jurnal hukum yang berisi prinsip-prinsip dasar (asas hukum), pandangan para ahli hukum (doktrin), hasil penelitian hukum, kamus hukum, ensiklopedia hukum. Wawancara dengan nara sumber ahli hukum untuk memberikan pendapat hukum tentang suatu peristiwa atau fenomena hukum bisa diartikan sebagai bahan hukum sekunder, namun demikian perlu dilihat kapasitas keilmuan dan seyogianya tidak terlibat dengan peristiwa tersebut agar komentar yang diberikan menjadi objektif.
c. Bahan non-hukum, yaitu bahan penelitian yang terdiri atas buku teks bukan hukum, yang terkait dengan penelitian seperti buku politik, buku ekonomi, data sensus, laporan tahunan perusahaan, kamus bahasa, ensiklopedia umum. Bahan non hukum menjadi penting karena mendukung dalam proses analisis terhadap bahan hukum.

4. Sumber Data

Sumber data merupakan tempat dimana sebuah data berasal, adapun sumber data tersebut adalah:

a. Sumber Data Primer

Sumber data primer merupakan hasil dari kajian mendalam terhadap berbagai status, postingan, ataupun berbagai halaman yang ada di dalam media sosial.

b. Sumber Data Sekunder

Sumber data sekunder berasal dari hasil kepustakaan yang terkait dengan delik pidana penipuan. Sumber data ini dapat diperinci sebagai berikut:

(1) Badan hukum primer, yaitu semua bahan atau materi yang mengikat secara yuridis.
   a. Undang-Undang Dasar Negara Republik Indonesia tahun 1945
   b. Kitab Undang-Undang Hukum Pidana (KUHPidana)
   c. Kitab Undang-Undang Hukum Acara Pidana (KUHAP)
   d. Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

(2) Bahan hukum sekunder, yakni bahan hukum yang mendukung bahan hukum primer, antara lain:
   a. Pustaka ilmiah di bidang hukum yang memiliki keterkaitan dengan topik penelitian.
   b. Literatur dan hasil penelitian terdahulu.

(3) Bahan hukum tersier, yakni bahan yang menguatkan bahan hukum primer dan sekunder yang di dapat dari ensiklopedi, internet, ataupun kamus.

5. Teknik Pengumpulan Data

Pada penelitian ini, metode pengumpulan data dengan menganalisis bahan pustaka atau data sekunder sehingga mendapatkan data yang valid. Hal ini didukung oleh studi kepustakaan (buku-buku, literatur, dokumen, majalah, internet, peraturan perundang-undangan) yang di dapat penulis dan bersifat teoritis. Dalam studi kepustakaan ini penulis mendapat data yang bersifat teoritis dari buku-buku, literatur, dokumen, majalah, internet, peraturan perundang-undangan, hasil penelitian serta bahan lain yang berkaitan dengan masalah penelitian.

6. Analisis Data

Penelitian ini menggunakan tahapan-tahapan dalam analisis data sehingga dapat menghasilkan penelitian yang valid, antara lain:

a. Reduksi Data

Adapun reduksi data merupakan proses pengolahan data yang dilakukan setelah semua data diperoleh oleh peneliti. Dalam hal ini peneliti perlu untuk melakukan reduksi secara intens dikarenakan fenomena yang terjadi akan terus mengalami perubahan dikarenakan penelitian ini merupakan penelitian deskriptif kualitatif. Reduksi data perlu dilakukan secara intens dengan tujuan mendapatkan data yang aktual sehingga menciptakan suatu penelitian yang sesuai dengan kondisi yang terjadi di lapangan.

b. Penyajian data

Dalam tahapan ini peneliti mencoba untuk menyusun hasil kajian dari data yang ditemukan dengan Bahasa yang komunikatif agar mampu diketahui oleh pembaca ataupun peneliti lain. Penyajian data harus dilakukan secara terorganisir sehingga mudah dipahami dan dapat dijadikan sebagai rencana kerja penelitian selanjutnya.

C. HASIL DAN PEMBAHASAN

A. Pengaturan UU ITE telah memberikan jaminan penegakan hukum terhadap penipuan di dalam penggunaan media sosial

Terjadinya tindak pidana sangat memungkinkan ada dalam penggunaan media sosial. Dalam penelitian ini, penulis menemukan beberapa pelaku pengguna media sosial yang masiah dibawah umur yang berarti belum memiliki kecakapan dalam mengoperasikan atau menggunakan media sosial dalam melakukan berbagai kegiatan dan bertransaksi. Hal ini membuktikan bahwa media sosial masih sarat dengan berbagai pelanggaran. Beberapa diantaranya terjadi di dalam salah satu aplikasi media sosial Facebook, peneliti juga menemukan banyak kasus penipuan yang terjadi di facebook dalam transaksi jual beli masih rawan sekali dengan berbagai macam bentuk pelanggaran.

Kebanyakan dari pelaku penipuan melakukan aksinya kepada para remaja yang masih duduk dibangku sekolah. Itu berarti masih kurang adanya pemahaman dan pengawasan kepada para remaja yang melakukan transaksi ataupun kegiatan dalam media sosial seperti halnya di dalam facebook sehingga anak dibwah umur banyak menjadi korban penipuan. Berbagai macam tindak pidana yang terjadi di dalam masyarakat salah satunya adalah sebuah kejahatan penipuan di bidang bisnis online yang kerap terjadi dengan berbagai macam bentuk dan perkembangannya menunjukkan pada semakin tingginya intelektualitas dari kejahatan penipuan bisnis online yang semakin kompleks.

Menurut sebagian korban penipuan, yang nmenyadari kecerobohan dalam bertransaksi dengan toko-toko online shop yang memilikik track record buruk dan tidak lebih teliti lagi dalam memilih toko online yang memiliki rating baik, karena tergiur dengan harga yang murah sehingga terjadi kesepakatan seperti dalam contoh kasus yang peneliti temukan berikut. Terkait dengan penipuan yang berada didalam media sosial Facebook, penulis menemukan beberapa modus penipuan yang saat ini sering dilakukan dalam transaksi Facebook, yaitu:

1. Penipuan yang dilakukan oleh seller terhadap buyer, dengan modus seller mengirimkan nomor rekening beserta jumlah uang yang harus ditransfer kan Biasanya dalam kasus ini, seller mengunggah foto barang atau jasa ke dalam akun Facebook Nya, barang atau jasa yang diunggah tersebut biasanya merupakan sebuah

barang atau jasa yang fiktif yang memang dalam praktek nya bertujuan untuk menipu buyer. Dalam beberapa kasus yang telah penulis teliti, kebanyakan *sellller* yang melakukan penipuan semacam ini berakhir dengan tutup akun atau menghapus akun nya *(closed account)*.

2. Penipuan yang dilakukan seller terhadap buyer dengan modus yaitu seller melakukan sebuah penipuan yang berkedok arisan online. Dengan iming-iming mendapat hasil yang menggiurkan. Cara kerja nya yaitu seller meyakinkan korban dengan sangat meyakinkan dan juga memberi iming-iming palsu kepada korban sehingga korban menjadi tergiur dan membayar uang ke seller, lalu kemudian uang tersebut dibawa pergi oleh seller tersebut.
3. Penipuan yang dilakukan seller terhadap buyer dengan modus pembelian menggunakan pulsa. Seller disini tidak meminta uang terhadap korban, tetapi meminta pulsa kepada korban. Dalam kasus seperti ini biasanya pelaku tidak ingin identitas aslinya diketahui.
4. Penipuan yang dilakukan *buyyer* terhadap *seller* dengan modus *buyyer* merupakan pemebli tetap di *online shop* seller, penipuan ini berlandaskan rasa percaya seller terhadap buyyer.
5. Penipuan yang dilakukan oleh pihak ketiga, yaitu: *dropshipper*, dengan modus *buyyer* melakukan transaksi dengan *dropshipper*. *Dropshipper* meminta kepada *buyyer* untuk mentransfer sejumlah uang ke rekening produsen. *Dropshipper* meminta barang tersebut dikirim ke alamat nya sendiri, bukan ke alamat *buyyer* modus ini bertujuan untuk melakukan penipuan dengan menjelekkan reputasi produsen sehingga korban disini beranggapan pemilik nomor rekening yang ia transfer adalah pelaku nya.
6. Penipuan yang dilakukan *buyyer* atau *seller* dengan sistem *barter* atau *trade*. Pelakunya bisa diantara salah satu pihak, dengan moduse melakukan transaksi tukar barang atau jasa, tapi salah satu pihak melakukan wanprestasi.

Dalam praktik transaksi e-comerce melalui media sosial facebook, syarat dalam pembebanan pertanggungjawaban pidana kepada pelaku tindak pidana online adalah terpenuhinya segala unsur tindak pidana dan tujuan dari perbuatan tersebut dapat dibuktikan bahwa memang sengaja dilakukan dengan keadaan sadar akan dicelanya perbuatan tersebut kepada Undang-Undang. Berikut adalah unsur-unsur pada Pasa 378 KUHP, yaitu:

1. Unsur Objektif
    a. Perbuatan menggerakkan
    b. Yang digerakkan adalah orang (naturelijk person)
    c. Tujuan perbuatan nya adalah menyerahkan benda, member dan menghapus piutang
2. Unsur Subjektif
    a. Maksud dari perbuatan tersebut adalah untuk menguntungkan diri sendiri dan/atau orang lain.
    b. Dengan melawan hukum

Meskipun unsur-unsur dalam Pasal 378 KUHP tersebut terpenuhi sepenuhnya, tetapi terdapat unsur dari tindak pidana penipuan online yang tidak terpenuhi dalam pengaturan Pasal 378 KUHP, yaitu:

1. Tidak terpenuhi nya unsur media utama yang digunakan dalam melakukan tindak pidana penipuan online yaitu: media elektronik yang belum dikenal dalam KUHP

maupun KUHAP
2. Cara-cara penipuan yang berbeda antara penipuan konvensional dengan penipuan online
3. Terdapat batasan dalam KUHP yaitu tidak dapat membebankan pertanggungjawaban pidana pada subjek hukum yang berbentuk badan hukum (korporasi) yang melakukan tindak pidana penipuan online.

Berikut adalah unsur-unsur yang terdapat pada Pasal 28 Ayat (1) UU ITE, yaitu:

1. Unsur Objektif
   a. Perbuatan menyebarkan
   b. Yang disebarkan adalah berita bohong dan menyesatkan
   c. Dari perbuatan tersebut timbul akibat konstitutif nya yaitu kerugian konsumen dalam transaksi elektronik
2. Unsur Subjektif
   a. Unsur kesalahan yaitu dengan sengaja melakukan perbuatan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik
   b. Melawan hukum tanpa hak

Terdapat beberapa frasa yang memiliki tafsir serta beberapa unsur yang kurang tepat tercantum dalam pasal tersebut seperti tidak jelas nya kepada siapa keuntungan melakukan tindakan menyebarkan berita bohong dan menyesatkan yang merugikan konsumen dalam transaksi elektronik, adanya frasa tanpa hak yang dapat ditafsirkan adanya pihak yang memiliki hak untuk menyebarkan berita bohong dan menyesatkan.

Melihat perbandingan antara kedua pasal tersebut, maka untuk pembebanan pertanggungjawaban pidana tentu saja akan memiliki perbedaan, yaitu perbedaan sanksi pidana pada pasal 378 KUHP dan pasal 28 ayat (1), bila dalam pasal 378 KUHP hanya terdapat sanksi pidana penjara selama 4 (empat) tahun, sedangkan dalam pasal 28 (1) UU ITE tidak secara langsung mencantumkan sanksi pidana melainkan tertera pada pasal 45 ayat (2) UU ITE yaitu sanksi pidana penjara paling lama 6 tahun, dan juga terdapat sanksi denda sebesar satu milyar rupiah, tidak dikenal nya subjek hukum badan hukum (korporasi) dalam KUHP yang akan berakibat lolos nya subjek hukum tersebut untuk dimintai pertanggungjawaban pidana, beda hal nya dalam UU ITE telah mengenal subjek hukum yang berbentuk badan hukum (korporasi). Setelah melihat perbedaan pengaturan dan pertanggungjawaban pidana antara pasal 378 KUHP dan pasal 28 ayat (1) UU ITE, terdapat beberapa point penting, yaitu:

1. KUHP memiliki unsur menguntungkan diri sendiri dan orang lain, sedangkan dalam Undang-Undang ITE tidak jelas kepada siapa penipuan tersebut ditujukan, yang terpenting adalah adanya kerugian konsumen dalam transaksi elektronik, tidak peduli siapa yang diuntungkan.
2. KUHP belum mengenal subjek hukum badan hukum (korporasi), sedangkan Undang-Undang ITE telah mengenal subjek hukum badan hukum (korporasi).
3. KUHP tidak mengenal transaksi elektronik ataupun media elektronik yang dalam hal ini adalah objek penting sara pelaku kejahatan untuk melakukan tindak pidana penipuan online, pada Undang-Undang ITE telah dikenal adanya informasi, transaksi dan media elektronik.
4. Adanya perbedaan akibat dan tujuan dari perbuatan yang dicantumkan pada dua pasal dalam dua Undang-Undang tersebut. Pasal 378 KUHP tujuan nya menguntungkan diri sendiri dan atau orang lain, akibat yang ditimbulkan adalah adanya penyerahan

benda dari orang yang berhasil di pengaruhi untuk digerakkan sesuai keinginan pelaku, adanya pemberian dan penghapusan utang piutang. Sedangkan dalam pasal 28 ayat (1) UU ITE tidak tercantum nya unsur tujuan untuk keuntungan siapakah pelaku melakukan tindak pidana tersebut, pasal ini hanya mencantumkan akibat terjadi nya tindak pidana tersebut yaitu kerugian konsumen dalam transaksi elektronik.

5. Adanya cara yang jelas dan terperinci untuk melakukan tindak pidana penipuan dalam KUHP yaitu dengan nama palsu, martabat/kedudukan palsu, serta tidak terdapat cara melainkan hanya mencantumkan perbuatan yaitu menyebarkan berita bohong dan menyesatkan.
6. Adanya perbedaan sanksi dalam KUHP dan UU ITE, perbedaan tersebut terlihat oleh adanya sanksi denda dalam UU ITE.

Selain itu, terdapat beberapa Undang-Undang yang dapat dikaitkan dengan transaksi ini seperti Undang-Undang Nomor 8 Tahun 1999 tentang perlindungan konsumen dan juga Undang-Undang Nomor 11 Tahun 2008. Di Indonesia perkembangan teknologi komputer dan informasi serta perkembangan bisnis melalui internet atau e-commerce ini belum diikuti dengan pengaturan hukum yang memadai dalam bentuk perangkat perundang-undangan yang mengatur nya secara khusus. Berdasarkan hal tersebut dapat dilihat bahwa ketidakseimbangan antara produk-produk hukum yang ada dengan kemajuan teknologi modern yang demikian pesat menyebabkan aktivitas di internet khususnya dalam e-commerce menjadi sangat rawan dengan permasalahan hukum.

Berdasarkan penelitian yang telah dilakukan, aturan e-commerce merujuk pada UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dengan munculnya Undang-Undang No. 11 2008 tentang Informasi dan Transaksi Elektronik (ITE) memberikan dua hal penting, yakni pertama, pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin, dan yang kedua diklasifikasikan nya tindakan-tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan TI (Teknologi Informasi) disertai dengan sanksi pidana nya.

Dengan adanya pengakuan terhadap transaksi elektronik dan dokumen elektronik maka setidaknya kegiatan e-commerce mempunyai basis legal nya. Dokumen elektronik untuk kasus penipuan transaksi e-commerce di media sosial seperti facebook itu sendiri yaitu, berupa bukti percakapan dalam PM (Private Message) dalam facebook. Dalam beberapa kasus juga bukti percakapan dalam bentuk SMS (Short Message Service) maupun chat WhatsApp.

Berdasarkan kajian yang dilakukan oleh peneliti, kebanyakan korban penipuan dari media sosial Facebook mencabut laporan nya dikarenakan pelaku telah mengganti dengan sejumlah uang kerugian yang diterima oleh korban itu sendiri. Tetapi ada pula yang lebih memilih untuk melaporkan ke kepolisian agar mendapat surat keterangan dari pihak kepolisian agar bisa dilanjutkan ke pihak bank yang bersangkutan. Menurut berapa korban, mereka beranggapan sanksi sosial juga sangat berjasa untuk membuat efek jera kepada pelaku tindak kejahatan, karena menurut mereka selain sanksi hukum, sanksi sosial juga dapat membantu mereka untuk mendapat kembali hak mereka dan juga untuk memberi informasi terhadap pelaku transaksi e-commerce seperti facebook bahwa misal pelaku penipuan dari online shop A merupakan penipu.

Selain itu, cara pemblokiran rekening bank juga menjadi langkah paling populer yang dilakukan korban penipuan di dalam facebook ini. Seperti yang diungkapkan salah satu

korban penipuan transaksi e-commerce di media sosial facebook yang beranggapan beberapa pelaku tidak hanya diberikan efek jera dengan sanksi sosial, tapi juga harus ada efek jera yang lebih nyata, salah satu nya pemblokiran rekening pelaku, agar si pelaku tidak dapat menggunakan uang yang terdapat di dalam rekening nya. Pelaku hanya bisa kembali menggunakan rekenig nya jika pelaku telah memenuhi kewajiban nya terhadap korban agar korban mencabut laporan pemblokiran di pihak bank.

Terkait dengan tindak pidana penipuan di dalam Facebook, peneliti mendapatkan fakta bahwa aparat penegak hukum kesulitan dalam mengungkap tindak pidana cybercrime, disamping karena terkendala birokrasi perbankan, kurang nya koordinasi penyidik dengan operator seluler atau internet service provider, minim nya personil yang memiliki kemampuan di bidang ITE dan alat-alat khusus untuk kejahatan ITE berdasarkan kenyataan penipuan via facebook kemudian berakhir dengan diundangkan nya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE), yaitu Undang-Undang pertama di bidang Teknologi Informasi dan Transaksi Elektronik sebagai produk legislasi yang sangat dibutuhkan dan telah menjadi pionir yang meletakkan dasar pengaturan di bidang pemanfaatan teknologi informasi dan transaksi elektronik. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik ini kemudian direvisi dan diperbaharui menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Penipuan melalui media sosial facebook berdasarkan pada pasal-pasal dalam Bab XI mengenai Ketentuan Pidana dalam UU ITE, maka dapat diidentifikasi beberapa perbuatan yang dilarang (Unsur Tindak Pidana) yang erat kaitan nya dengan tindak kejahatan penipuan melalui facebook pada tiap pasal-pasalnya. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik termasuk ke dalam Pasal 28 Ayat (1): "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong *dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik."* Dan adapun ketentuan sanksi tindak pidana penipuan bisnis online terdapat pada Pasal 45A Ayat (1) yang berbunyi "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diakses nya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan sebagaimana dimaksud dalam Pasal 28 Ayat (1) di pidana penjara paling lama enam (6) Tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar)"

Ketentuan tentang penipuan facebook yang dapat diatur dalam ketentuan melalui Kitab Undang-Undang Hukum Pidana (KUHP) termasuk ke dalam pasal 378 ayat (1) yaitu "barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan menggunakan nama palsu atau martabat(hakoedaningheid) palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepada nya atau supaya memberi utang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat (4) Tahun". Hukum pidana sebagai alat atau sarana bagi penyelesaian terhadap problematika ini diharapkan mampu memberikan solusi yang tepat. Karena itu, pembangunan hukum dan hukum pidana pada khususnya perlu lebih ditingkatkan dan diupayakan secara terarah danterpadu, antara lain adalah kodifikasi, dan unifikasi, bidang-bidang hukum tertentu serta penyusunan Perundang-Undangan baru yang sangat dibutuhkan guna menjawab tindak pidana.

Kitab Undang-Undang Hukum Pidana (KUHP) sendiri pada Pasal 378 menegaskan bahwa seseorang yang melakukan kejahatan penipuan diancam dengan sanksi pidana.

Walaupun demikian, masih dirasa kurang efektif dalam penegakan terhadap pelanggar nya, karena dalam penegakan hukum pidana tidak hanya cukup dengan diatur nya suatu perbuatan di dalam suatu Undang-Undang, namun dibutuhkan juga aparat hukum sebagai pelaksana atas ketentuan Undang-Undang serta lembaga yang berwenang untuk menangani suatu kejahatan seperti Kepolisian, Kejaksaan, dan Pengadilan, Kasus-kasus penipuan online akhir-akhir ini semakin berkembang dan bertambah banyak meskipun tindak pidana ini telah diatur dalam KUHP Pasal 378, dan Undang-Undang Nomor 19 Tahun 2016 Pasal 28 Ayat (1) Tentang Informasi dan Transaksi Elektronik.

B. Upaya yang telah dilakukan dalam menekan angka tindak pidana penipuan di dalam penggunaan media sosial sehingga dapat berkurang dalam pelaksanaannya

Aturan hukum di Indonesia adalah hasil logis yang membutuhkan lembaga untuk bisa mengawasi penegakan hukum, salah satu nya adalah Kepolisian Republik Indonesia. Semua orang memiliki harapan agar kepolisian bisa menjalankan tugasnya untuk menangani kasus pidana supaya dapat diselesaikan secara optimal. Hal Ini untuk menentukan sejauh mana optimalisasi peran kepolisian dalam proses penanggulangan kejahatan *cyber*.

Dalam menanggulangi terjadinya kejahatan cyber, pihak kepolisian telah melakukan berbagai upaya seperti memberikan himbauan kepada masyarakat melalui media elektronik, maupun berbagai macam media sosial dengan menyebarkan broadcast yang berupa himbauan-himbauan terkait tindak kejahatan cyber crimes untuk diberitahukan ke masyarakat secara luas. Selain itu, dilakukan juga penerangan ke masyarakat melalui media surat kabar, radio, serta pada saat mengisi berbagai acara dari pihak kepolisian juga tidak henti-hentinya memberikan himbauan kemasyarakat.

Dalam melakukan upaya ini, pihak kepolisian telah mengambil tindakan dengan memproses setiap kasus Tindak Pidana Cyber yang ditangani sesuai dengan aturan yang berlaku. Pihak kepolisian juga telah bekerja sama dengan berbagai bentuk stakeholder yang ada, yaitu tentang bagaimana cara menangkap para pelaku tindak kejahatan tersebut yang tertangkap tangan sedang melakukan sebuah kejahatan ataupun melalui laporan masyarakat yang kemudian ditindak lanjuti dengan mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap para tersangka pelaku kasus Tindak Pidana Cyber, setelah dilakukan penangkapan kemudian diproses oleh pihak kepolisian terlebih dahulu sebelum dilimpahkan berkas perkaranya kepada kejaksaan. Pihak kepolisian juga memiliki beberapa peran dalam rangka upaya menanggulangi kejahatan *cyber*, meliputi 3 (tiga) hal, yakni adalah tindakan pre-emtif, tindakan preventif (pencegahan), dan tindakan represif (penegakan hukum).

1. Tindakan Pre-emtif

   Tindakan pre-emtif merupakan sebuah langkah awal yang dilakukan oleh pihak kepolisian untuk mencegah terjadi nya tindak pidana. Usaha-usaha yang dilakukan dalam penanggulangan kejahatan secara pre-emtif adalah menanamkan nilai-nilai atau norma-norma yang baik, sehingga nilai-nilai atau norma-norma tersebut terinternalisasi dalam diri seseorang. Meskipun seseorang ingin melakukan pelanggaran ataupun kejahatan tapi tidak ada niat untuk melakukan hal tersebut maka tidak akan terjadi sebuah kejahatan. Cara pencegahan ini berasal dari teori NKK, yaitu Niat ditambah dengan Kesempatan terjadi sebuah Kejahatan.
2. Tindakan Preventif

   Tindak Preventif merupakan sebuah upaya-upaya preventif yang menjadi

langkah selanjutnya yang akan ditempuh setelah dari upaya pre-emtif telah dilakukan sebelumnya yang masih dalam tataran pencegahan sebelum terjadi adanya kejahatan. Upaya preventif ini merupakan suatu upaya yang sangat mudah dilakukan, karena dapat dilakukan oleh siapa saja bagi mereka yang dapat memberikan pengetahuan-pengetahuan tentang pencegahan suatu kejahatan. Dalam upaya preventif yang paling diutamakan adalah menghilangkan suatu kesempatan untuk melakukan suatu kejahatan.

3. Tindakan Represif

   Tindakan represif dalam hal ini merupakan upaya terakhir yang dapat kita lakukan setelah upaya pre-emtif dan preventif. Upaya represif merupakan suatu upaya yang prosedural sesuai dengan sistem hukum, yaitu sebuah sistem peradilan pidana. Upaya ini dilakukan pada saat telah terjadi tindak pidana atau kejahatan, tindakan ini disebut sebagai penegakan hukum (*law enforcement*) dengan menjatuhkan hukuman sesuai dengan sanksi yang telah ditentukan. Kemudian yang dapat melakukan upaya represif ini hanya orang-orang tertentu saja. Yakni par aparat penegak hukum baik dari pihak kepolisian, kejaksaan, kehakiman, sampai lembaga pemasyarakatan.

Di samping itu, karena tujuan utama nya adalah untuk mencapai kesejahteraan masyarakat pada umumnya, maka kebijakan penegakan hukum termasuk dalam bidang kebijakan sosial, yaitu segala usaha rasional untuk mencapai kesejahteraan masyarakat. Bentuk yang pertama adalah bersifat represif yang menggunakan sarana penal, yang sering disebut sebagai sistem peradilan pidana (criminal justice system). Dalam hal ini secara luas sebenarnya mencakup juga proses kriminalisasi. Lalu, yang kedua berupa sebuah usaha-usaha prevention without punishment (tanpa menggunakan sarana penal). Dan yang ketiga adalah menggunakan usaha-usaha pembentukan opini masyarakat secara luas dan terperinci tentang kejahatan dan sosialisasi hukum melalui media massa secara luas.

Kebutuhan masyarakat terhadap rasa aman dan terlindungi merupakan salah satu hak asasi yang harus diperoleh dan dimiliki oleh semua orang. Rasa aman dan terlindungi tersebut juga merupakan suatu kebutuhan dasar masyarakat yang menjadi hal sangat penting, setelah kebutuhan akan sandang, pangan, dan papan. Hak atas rasa aman dan terlindunginya masyarakat tersebut telah tertuang dalam Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945 yang kemudian disingkat dengan (UUD 1945) Pasal 28G ayat (1), yang menyatakan bahwa:

"Setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang dibawah kekuasaannya, serta berhak atas rasa aman dan perlindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi".

Undang-Undang Dasar Negara Kesatuan Republik Indonesia Tahun 1945 yang selanjutnya disingkat dengan (UUD 1945) tersebut merupakan sebuah landasan konstitusional yang berada didalamnya dan dijiwai oleh Pancasila, merupakan arah politik dari hukum nasional yang dimuat dalam alinea keempat Pembukaan Undang-Undang Dasar Negara Kesatuan Republik Indonesia, yang berbunyi sebagai berikut:

"Untuk membentuk suatu pemerintahan negara Indonesia yang melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial."

Pasal 1 ayat (3) UUD 1945, menyatakan bahwa Negara Indonesia adalah negara hukum. Ketentuan tersebut merupakan landasan bagi arah politik hukum dalam pembangunan hukum nasional negara untuk selalu memberikan pelayanan publik, sehingga sampai saat ini orang bertumpu pada kata segenap bangsa sebagai asas tentang persatuan seluruh bangsa Indonesia, tanpa terkecuali. Artinya, negara turut serta dan bertanggungjawab dalam upaya mengangkat harkat dan martabat seluruh warga indonesia sebagai perwujudan dalam bentuk perlindungan hukum. Pasal ini dapat dikorelasikan dengan pasal-pasal yang mengatur tentang kejahatan penipuan dengan menggunakan media maya yang berupa transaksi elektronik.

Terkait seperti yang sudah dijelaskan tersebut, Kepolisian Republik Indonesia selalu melakukan pengamanan terhadap jaringan penipuan di dalam media sosial, sehingga tidak lagi meresahkan masyarakat. Penipuan yang sangat sering terjadi saat ini banyak yang dilakukan melalui media sosial dalam melancarkan aksinya. Berdasarkan fenomena tersebut, maka penipu telah melanggar Pasal 378 KUHP serta Pasal 28 ayat (1), perbuatan itu dapat digolongkan sebagai perbuatan tipu muslihat dan menyesatkan.

Dalam hal ini kedua cara menggerakkan orang lain sama-sama bersifat menipu atau isinya tidak benar atau palsu, namun dapat menimbulkan kepercayaan atau kesan bagi orang lain bahwa semua itu seolah-olah benar adanya. Namun terdapat sebuah perbedaan, yakni pada tipu muslihat berupa perbuatan, sedangkan pada rangkaian kebohongan berupa ucapan atau perkataan. Tipu muslihat diartikan sebagai suatu perbuatan yang sedemikian rupa dan yang menimbulkan kesan atau kepercayaan tentang kebenaran perbuatan itu, yang sesungguhnya tidak benar adanya. Karenanya, orang bisa menjadi percaya dan tertarik atau tergerak hatinya.

Selain itu, upaya lain juga dilakukan agar tidak terjadi lagi penipuan berbasis internet yang berada didalam media sosial. Berbagai upaya yang dilakukan adalah sebagai berikut: Pengenalan tentang Komputer dan Internet melalui pendidikan. Penandatanganan nota PT. Indosat dan Depdiknas tentang pengembangan Cyber Education di Malang Jawa Timur, merupakan salah satu cara pengenalan komputer dan internet kepada masyarakat sejak usia dini. Prinsip dasar Cyber Education sangat sederhana, yakni memanfaatkan teknologi multimedia internet untuk menyalurkan suatu materi dari satu tempat ke tempat lain. Untuk itu tempat-tempat yang bersangkutan harus tergabung dalam satu jaringan komunikasi berbasis protokol internet. PT. Indonsat melalui anak perusahaannya yaitu Indosat Multi Media, menyediakan infrastruktur sekaligus menyediakan koneksi internet yang menghubungkan antar lokasi dalam satu jaringan. Depdiknas secara bertahap mengembangkan jaringan internet ke sekolah-sekolah dikabupaten atau kota di seluruh wilayah Indonesia. Dengan dibangunnya jaringan antar sekolah tersebut maka data pendukung, referensi ataupun berbagai informasi lain yang relevan dapat diperoleh dengan cepat dan mudah. Selain itu juga dapat dilakukan diskusi dan sebuah pengajaran dari jarak jauh.

Seminar Teknologi dan Informasi, hal tersebut juga dapat membantu pengenalan teknologi komputer kepada masyarakat. Acara-acara seminar teknologi informasi sangat membantu pengenalan teknologi komputer kepada masyarakat. Seminar yang dimaksudkan disini dalam arti luas, dimana bisa juga dalam bentuk diskusi interaktif, bedah buku teknologi informasi, seminar loka karya (SEMINALOKA), workshop, dan sebagainya.

Adapun pasal 378 KUHP juga mengatur tentang segala bentuk penipuan, merumuskan yakni barang siapa dengan maksud sengaja untuk menguntungkan diri sendiri atau orang

lain dengan melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat ataupun dengan rangkaian kebohongan menggerakkan orang lain untuk menyerahkan sesuatu benda kepadanya, atau supaya memberi hutang maupun menghapus piutang, diancam karena penipuan dengan pidana penjara paling lama 4 (empat) tahun.

Pihak kepolisian sendiri pun juga memiliki Subdit Cyber Crimes (Mabes Polri, berada di Subdit V) dan Subdit IV Cyber Crimes Polda Metro Jaya yang khusus menangani tindak pidana yang berhubungan dengan cyber crimes, tindak pidana informasi dan transaksi elektronik. Tugas Pokok dan Fungsi (TUPOKSI) satuan Cyber Crimes berdasarkan Keputusan Kapolri Nomor Pol. : KEP/54/X/2002 tanggal 17 Oktober 2002 adalah unsur pelaksanaan Direktorat Reserse Kriminal Khusus Polda Metro Jaya, tugasnya adalah melakukan penyelidikan dan penyidikan tindak pidana khusus, terutama penyidikan yang berhubungan dengan teknologi informasi, telekomunikasi, serta transaksi elektronik di media sosial.

Bareskrim Kepolisian Republik Indonesia juga membentuk Satgas-commerce yang dikepalai Kasubdit II Direktorat Tindak Pidana Cyber Bareskrim sebagai tempat penerimaan aduan dari pengguna media sosial yang merasa dirugikan dan kedepannya akan meluncurkan sebuah aplikasi yang menjadi wadah laporan masyarakat yang merasa ditipu atau tertipu oleh pelaku usaha atau penjual dalam e-commerce. Terkait dengan penipuan jual beli yang berada di media sosial, pihak pengelola atau penyedia situs jual beli juga telah mengusahakan dan menerapkan berbagai kebijakan guna mencegah dan menanggulangi penipuan dalam situs jual beli di media sosial, diantaranya dengan memberlakukan sistem Cash on Delivery (COD) sebagai salah satu metode pembayarannya untuk menghindari barang yang tidak sampai atau penjual fiktif.

Kebijakan autentifikasi dan verifikasi produk seller dan akun konsumen dalam beberapa situs jual beli dalam media sosial yang terpercaya juga telah banyak dilakukan dan diterapkan. Hal ini diberlakukan untuk menghindari adanya pelaku usaha dan konsumen yang fiktif yang dapat merugikan. Kebijakan pengembalian dan Refund serta pembayaran yang dapat dipusatkan pada satu bank account resmi juga telah diterapkan guna meminimalisir tindak pidana penipuan dalam situs jual beli pada media sosial.

Penerapan transaksi melaui rekening bersama yang merupakan perantara atau pihak ketiga yang membantu keamanan, kenyamanan transaksi online sehingga pembeli tidak perlu ragu lagi dalam bertransaksi atau barang yang sampai tidak sesuai dengan apa yang diharapkan, dan penjual dapat membangun reputasi dan juga terhindar dari kecurigaan-kecurigaan berlebihan yang ada dalam pikiran masyarakat secara luas. Namun, juga tidak dipungkiri bahwa masih terdapat beberapa kendala dalam upaya penanggulangan cyber crime oleh aparat kepolisian khususnya di Unit Cyber Crime. Penulis membagi nya menjadi beberapa aspek, yaitu:

1. Aspek Penyidik (Sumber Daya Manusia)

   Penyidik kepolisian memiliki peran penting dalam upaya penanggulangan *cybercrime*, dimana kemampuan atau kualitas penyidik dan jumlah personil penyidik di setiap unit cybercrime harus memadai dan diperhatikan, karena sangat berpengaruh untuk mengungkap kasus-kasus *cybercrime* yang dilaporkan oleh masyarakat. Adanya unit *cybercrime* di lingkungan kepolisian membuktikan bahwa dibutuhkan nya penyidik khusus yang memiliki kemampuan di bidang informasi dan transaksi elektronik guna menangani kejahatan-kejahatan di dunia maya secara maksimal, dalam hal ini menjelaskan mengenai kendala aspek penyidik. Dimana aspek penyidik dalam penanggulangan kejahatan cybercrime penyidik sendiri memiliki kendala

mulai dari kualitas penyidik dan kuantitas penyidik atau jumlah personil penyidik

2. Aspek Aspek Alat Bukti

Pada tindak pidana *cybercrime* dalam hal alat bukti berbeda dengan alat bukti pada tindak pidana umum, dimana sasaran atau media *cybercrime* merupakan data-data atau sistem elektronik dengan dihubungkan ke internet, dan selain itu masih banyak dan bebas nya warung internet (warnet) dan fasilitas umum lainnya yang mana ini menjadi masalah atau kendala terhadap penyidik *cybercrime*, dalam hal ini menjelaskan secara rinci mengenai kendala aspek alat bukti yang mana dalam penanggulangan kejahatan *cybercrime* itu sendiri memiliki berbagai macam kendala, mulai dari alat bukti digital mudah dihilangkan dan atau dihapus jika tidak ditangani dengan cepat dan tepat, dan pelaku menggunakan fasilitas umum dalam melakukan tindak pidana, yakni penjelasan nya sebagai berikut:

a. Barang Bukti Digital Mudah Dihilangkan Jika Tidak Ditangani Dengan Tepat Waktu.

Barang bukti dalam tindak pidana *cybercrime* sesuai praktek nya berbentuk digital, dikarenakan yang dijadikan sasaran dalam tindak pidana *cybercrime* merupakan data-data atau sistem elektronik dimana misalnya dalam kasus hacking dan lain sebagainya dan/atau melakukan pencemaran nama baik atau penipuan secara online yang mana semua instrument yang digunakan ialah serba elektronik dengan dihubungkan ke internet yang sifatnya mudah diubah, dihapus, atau disembunyikan oleh pelaku kejahatan *cybercrime*, maka dari itu pada praktek nya dalam hal alat bukti dalam tindak pidana ini lebih sulit jika dibandingkan dengan alat bukti pada tindak pidana umum yang pada tindak pidana umum tersebut alat buktinya dalam bentuk fisik dan tidak mudah untuk dihilangkan jejak nya yang mana hal ini sangat bertolak belakang dengan tindak pidana *cybercrime* dalam hal alat bukti khususnya.

b. Pelaku Menggunakan Fasilitas Umum Dalam Melakukan Tindak Pidana

Pada kasus-kasus tindak pidana *cyber crime* tidak sedikit pelaku tindak pidana tersebut dalam melakukan aksinya menggunakan fasilitas umum dalam mengakses dan berbuat sesuatu dengan media elektronik dengan sambungan internet menggunakan fasilitas warung internet (warnet) dan/atau fasilitas umum lainya. Seperti halnya yang diketahui warung internet (warnet) di Indonesia masih dengan bebasnya beroprasi tanpa ada regulasi dan pengawasan dari pemerintah ataupun penegak hukum yang ada. Sedangkan penyidik dalam melakukan penyelidikan dalam tindak pidana *cyber crime* untuk melakukan pelacakan pelaku berdasarkan alamat server atau informasi IP Address dari alat elektronik pelaku, maka dalam hal ini tentu menjadi kendala dalam menangkap pelaku dan mengenai alat bukti akan semangkin rumit. Pelaku-pelaku tindak pidana *cyber crime* juga memanfaatkan hal tersebut agar jejak digitalnya tidak dapat dijadikan alat bukti atau sulit mengenai pembuktian dalam kejahatan cyber crime.

c. Keberadaan Para Saksi Tidak Di Tempat Yang Sama Dengan Korban dan Pelaku

Pada tindak pidana *cybercrime* sangat berbeda dengan tindak pidana umum, khususnya dalam hal alat bukti yang berkaitan dengan saksi-saksi, dimana pada tindak pidana ini saksi-saksi belum tentu keberadaannya di lokasi atau tempat yang sama dengan korban dan atau pelaku. Padahal keterangan saksi merupakan hal yang penting dalam proses penegakan hukum khususnya dalam

kasus tindak pidana cyber crime dan termasuk alat bukti sesuai pasal 184 ayat (1) huruf A dalam KUHAP, dimana keterangan saksi merupakan termasuk dari alat bukti yang sah. Saksi korban dalam kasus *cyber crime* berperan sangat penting dan tapi dalam prakteknya jarang sekali terdapat saksi dalam kasus seperti *cyber crime* dikarenakan saksi korban yang berada di luar daerah atau bahkan berada di luar negeri, hal tersebut tentu mengakibatkan penyidik sulit untuk melakukan pemeriksaan saksi dan pemberkasan hasil penyelidikan.

Penuntut umum juga tidak mau menerima berkas perkara yang tidak dilengkapi dengan berita acara pemeriksaan saksi, khususnya saksi korban dan harus dilengkapi dengan berita acara penyumpahan saksi karena kemungkinan besar saksi tidak dapat hadir di persidangan dikarenakan jarak kediaman saksi yang cukup jauh, karena itu hal tersebut mengakibatkan kurangnya alat bukti yang sah jika berkas perkara tersebut dilimpahkan ke pengadilan untuk disidangkan sehingga terdakwa beresiko akan dinyatakan bebas.

1. Aspek Fasilitas

Pada tindak pidana *cybercrime* dalam mengungkap kasus-kasus dibutuhkan fasilitas yang mampu menunjang kinerja aparat kepolisian atau penyidik, fasilitas tersebut berupa laboratorium forensik komputer yang digunakan untuk mengungkap data-data yang bersifat digital, serta merekam dan menyimpan bukti-bukti yang berupa *softcopy* (gambar, program, html, suara, dan lain sebagainya). Komputer forensik dikenal sebagai digital forensik, adapun tujuan nya ialah untuk mengamankan dan menganalisis bukti digital, serta memperoleh berbagai fakta yang objektif dari sebuah kejadian atau pelanggaran keamanan dari sistem informasi, berbagai fakta tersebut akan menjadi bukti yang akan digunakan dalam proses hukum. Melalui internet forensik, penyidik dapat mengetahui siapa saja orang yang mengirim email, kapan dan dimana keberadaan alamat pengirim berdasarkan server pengirim, dan dalam contoh lain kita bisa melihat siapa pengunjung website secara lengkap dengan informasi *IP Address*, alat elektronik yang dipakai nya dan keberadaan nya serta kegiatan apa yang dilakukan pada website tersebut.

2. Aspek Yurisdiksi

Pada penanggulangan tindak pidana *cybercrime* juga memiliki kendala dalam aspek yurisdiksi, dimana tindak pidana *cybercrime* ini merupakan tindak pidana yang pelaku dan korban tidak hanya di negara yang sama dan juga tidak selalu berkewarganegaraan yang sama, yaitu tindak pidana cybercrime ini juga merupakan tindak pidana transnasional. Pada sistem hukum pidana yang berlaku saat ini, hukum pidana pada umumnya hanya berlaku di wilayah negara nya sendiri (asas teritorial), dan untuk warga negara nya sendiri (asas personal atau nasional aktif). Hanya delik-delik tertentu yang dapat digunakan asas nasional pasif dan asas universal yang mana delik-delik tersebut termasuk kejahatan *cybercrime*. Beberapa aspek yurisdiksi tersebut, yaitu:

a. Pelaku Tindak Pidana *Cyber Crime* Berkewarganegaraan Yang Tidak Menganut Serta Menerapkan Hukum Yang Sama Dengan Indonesia

Pada kendala aspek yurisdiksi khususnya dalam hal pelaku tindak pidana *cybercrime* berkewarganegaraan yang tidak menganut dan menerapkan hukum yang sama dengan Indonesia, hal ini dalam melakukan penanggulangan tindak pidana tersebut yang transnasional atau bisa disebut juga lintas negara akan mengalami kesulitan, sedangkan dalam hal yurisdiksi telah diatur dalam Pasal 2 Undang-undang Nomor 19 tahun 2016 perubahan atas Undang-undang Nomor

11 tahun 2008 tentang informasi dan transaksi elektronik, yang berbunyi: "*Undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia".*

Undang-undang ITE juga memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia (WNI) maupun warga negara asing (WNA), atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi dan transaksi elektronik dapat bersifat lintas teritorial atau universal. Adapun beberapa hal yang mana di Indonesia dilarang dalam undang-undang ITE namun di beberapa negara-negara tidak melarang nya yakni sebagai berikut:

1) Pornografi Online; Pada tindakan pornografi online di Indonesia dilarang pada undang- undang ITE tepatnya pada pasal 27 ayat (1) UU ITE, namun masih banyak negara-negara yang melegalkan pornografi yaitu: Amerika serikat, Belanda, Kolombia, Uruguay, Kanada, Spanyol, dan lainnya.
2) Penistaan Agama; Pada tindakan menistakan agama juga menjadi rumit, dimana Indonesia hal tersebut dilarang pada undang- undang ITE tepatnya pada pasal 28 ayat (2) UU ITE, namun masih banyak negara-negara yang tidak melarang dalam hal penistaan agama yaitu, Amerika serikat, Korea Selatan, Vietnam, Kanada, dan lainnya.

b. Pelaku Tindak Pidana *Cyber Crime* Berkewarganegaraan Yang Tidak Ada Hubungan Diplomatik Dengan Negara Indonesia;

Pada kendala aspek yurisdiksi khususnya dalam hal ini untuk melakukan penanggulangan kejahatan *cybercrime* yang transnasional akan mengalami kesulitan, terutama pada kasus *hacking*, dimana pada tindak pidana tersebut sepakat semua negara di dunia bersepakat melarang dan masing-masing di negara nya membuat hukum untuk mengatur dan melindungi warga negara nya. Dalam hal ini penyidik akan mengalami kesulitan jika menangani kasus tindak pidana hacking yang mana korban nya adalah WNI atau badan hukum di negara Indonesia namun pelaku nya berkewarganegaraan yang tidak ada hubungan diplomatik dengan Indonesia, maka dalam hal tersebut akan menjadi kendala penyidik *cybercrime* dalam melakukan proses hukum. Adapun beberapa negara yang tidak ada hubungan diplomatik dengan negara Indonesia adalah, Israel, Makau, Korea Utara, Georgia, dan lainnya.

D. PENUTUP

A. Kesimpulan

Berdasarkan hasil penelitian yang didapatkan oleh penulis, maka kesimpulan yang dapat disusun adalah sebagai berikut:

1. Dalam praktek transaksi *E-commerce* melalui media sosial, dalam pembebanan pertanggungjawaban pidana kepada para pelaku tindak pidana penipuan di bidang online atau yang biasa disebut dengan Cyber *Crime* adalah terpenuhi nya segala unsur

yang berkaitan dengan tindak pidana dan tujuan dari adanya perbuatan tersebut dapat dibuktikan bahwa memang sengaja dilakukan dengan sadar akan dicela nya perbuatan tersebut oleh undang-undang. Hasil dari penelitian ini menunjukkan bahwa ternyata memang terdapat banyak sekali penipuan yang terjadi di media sosial. Penulis juga menemukan beberapa kasus penipuan di media sosial berupa penipuan dalam bidang transaksi elektronik, dan tidak sedikit juga anak di bawah umur ataupun orang yang tidak memiliki kecakapan hukum yang menjadi korban dari penipuan di bidang internet atau yang biasa disebut dengan *Cyber Crime* dan menjadi sasaran oleh para pelaku tindak pidana dikarenakan ketidaktahuan yang dimiliki oleh orang-orang tersebut.

2. Terkait upaya penanggulangan penipuan di media sosial, Kepolisian Republik Indonesia selalu melakukan berbagai macam pengamanan terhadap jaringan penipuan di media sosial. Dalam melakukan upaya ini, pihak kepolisian telah mengambil tindakan dengan memproses setiap kasus Tindak Pidana *Cyber* yang ditangani sesuai dengan aturan yang berlaku. Dalam menanggulangi terjadi nya kejahatan *cyber*, pihak kepolisian telah melakukan berbagai upaya seperti memberikan himbauan kepada masyarakat melalui media elektronik, maupun berbagai macam media sosial dengan menyebarkan *broadcast* yang berupa himbauan-himbauan terkait tindak kejahatan *cybercrimes* untuk diberitahukan ke masyarakat secara luas. Selain itu, dilakukan juga penerangan ke masyarakat melalui media surat kabar, radio, serta pada saat mengisi berbagai acara dari pihak kepolisian juga tidak henti-henti nya memberikan himbauan ke masyarakat.

Pihak kepolisian juga telah bekerja sama dengan berbagai bentuk *stakeholder* yang ada, yaitu tentang bagaimana cara menangkap para pelaku tindak kejahatan tersebut yang tertangkap tangan sedang melakukan sebuah kejahatan ataupun melalui laporan masyarakat yang kemudian ditindak lanjuti dengan mendatangi tempat kejadian perkara (TKP) guna melakukan penangkapan dan penahanan terhadap para tersangka pelaku kasus Tindak Pidana *Cyber*, setelah dilakukan penangkapan kemudian diproses oleh pihak kepolisian terlebih dahulu sebelum dilimpahkan berkas perkara nya kepada kejaksaan.

Pihak kepolisian juga memiliki beberapa peran dalam rangka upaya menanggulangi kejahatan cyber, meliputi 3 (tiga) hal. Baik secara Pre-emtif, Preventif, dan juga Represif sehingga tindakan penipuan tersebut tidak lagi meresahkan masyarakat. Pihak Kepolisian Republik Indonesia juga telah memiliki Subdit Cyber Crime (Mabes Polri, berada di Subdit V) dan Subdit IV Cyber Crime Polda Metro Jaya yang khusus menanggani tindak pidana di bidang Cyber, walaupun masih memiliki banyak kendala di dalam penanganannya. Akan tetapi, dari pihak kepolisisan sendiri selalu melakukan usaha-usaha yang maksimal untuk memberantas tindak kejahatan penipuan di bidang internet atau yang biasa disebut dengan Cyber Crime, dan berbagai macam kegiatan penyidikan yang berhubungan dengan teknologi informasi, telekomunikasi, serta transaksi elektronik yang berada di dalam media sosial.

B. Saran

Berdasarkan hasil penelitian yang telah disimpulkan, maka penulis dapat menyarankan beberapa hal, antara lain adalah sebagai berikut:

1. Penulis menyarankan untuk lebih dioptimalkan kembali dalam segi penegakan hukum yang lebih baik, berupa ketegasan dalam penegakan pasal-pasal yang mengatur berbagai hal mengenai tindak pidana dalam bidang penipuan yang berbasis internet atau yang biasa disebut dengan *Cyber Crime*, terutama dalam Pasal 378 KUHP dan

Pasal 28 ayat (1) yang mengatur tentang Informasi dan Transaksi Elektronik.

2. Lebih memaksimalkan kembali mengenai pemahaman kepada masyarakat tentang akan adanya berbagai macam hukum yang telah mengatur tentang tindak pidana penipuan, sehingga masyarakat tidak perlu lagi takut berlebih lagi dengan tindak kejahatan tersebut. Pemasifan kembali mengenai bimbingan terhadap masyarakat sejak dini atau kepada orang yang belum cakap dengan hukum dalam penggunaan internet dan media sosial, sehingga dapat meminimalisir agar tidak menjadi korban tindak pidana penipuan yang berbasis internet atau *Cyber Crime.*
3. Meningkatkan kembali kewaspadaan terhadap berbagai macam bentuk penipuan yang berbasis internet atau Cyber Crime dengan cara menggunakan media dengan selektif dan seefektif mungkin agar terhindar dari tindak pidana kejahatan tersebut.

Evaluasi tentang akan adanya kendala yang dialami oleh pihak Kepolisian Republik Indonesia dalam menangani kasus tindak kejahatan Cyber Crime, sehingga dalam waktu yang akan mendatang dari pihak kepolisian sendiri dapat lebih optimal menangani berbagai bentuk kejahatan yang berbasis internet atau Cyber Crime.

E. DAFTAR PUSTAKA

Siswanto Sunarso, “Hukum Informasi dan Transaksi Elektronik”, (Jakarta: Rineka Cipta, 2009), hal.39

Moeljatno, “Asas-Asas Hukum Pidana”, (Jakarta: Rineka Cipta, 2015), hal.60

Pasal 1 ayat (6) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pasal 28 ayat (1) Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Soerjono Soekanto, “Pengantar Ilmu Hukum”, (Jakarta: Rajawali Press, 2007), hal.53

Lexy Moelong, “Metode Penelitian Kualitatif”, (Bandung: Rosdakarya, 2013), hal.11

Soerjono Soekanto dan Sri Mamudji, “Penelitian Hukum Normatif”, (Jakarta: Raja Grafindo Persada, 1999), hal.24

Peter Mahmud Marzuki, “Penelitian Hukum”, (Jakarta: Kencana, 2005), hal.25

Muhaimin, “Metode Penelitian Hukum’, (Mataram: Mataram University Press, 2020), hal.39

Lexy Moelong, “Metodologi Penelitian Kualitatif”, (Bandung: Rosdakarya, 2013), hal.11