MEKANISME HUKUM PENANGANAN TINDAK PIDANA PENIPUAN YANG DILAKUKAN MELALUI INTERNET

Muhammad Yunus Idy
Fakultas Hukum Universitas Islam Makassar (UIM)
Alamat : Jl. Perintis Kemerdekaan Km.9 Makassar

ABSTRAK

Pokok permasalahan yang dibahas dalam penelitian ini adalah tentang pengaturan mengenai tindak pidana penipuan yang dilakukan secara online, serta bagaimanakah upaya penanganan perkaranya sesuai dengan ketentuan hukum yang berlaku, baik berdasarkan KUHP maupun berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Metode penelitian yang digunakan adalah *statuta approach, conseptual approach,* dan *comparative approach*. Tipe penelitiannya adalah *Normative Legal Research*. Hasil penelitian menunjukkan bahwa tindak pidana penipuan yang dilakukan secara *online* pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan sistem elektronik yaitu komputer, internet, maupun perangkat telekomunikasi lainnya. Sehingga berdasarkan ketentuan hukum yang berlaku, penipuan *online* dapat diperlakukan sama sebagaimana delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP), maka proses penanganan perkaranya juga didasarkan baik pada KUHP maupun berdasarkan undang-undang tentang informasi dan transaksi elektronik. Demikian pula dengan hukum acaranya yang didasarkan pada KUHAP.

Kata Kunci : *Cybercrime*, Pidana, penipuan online.

ABSTRACT

Main issues addressed in this study is about the arrangements regarding the criminal acts of fraud online, as well as how the handling of his case in accordance with the legal provisions in force, both by the KUHP and by Act No. 11 of 2008 on Information and Electronic Transactions. The method used is the statutory approach, conceptual approach and comparative approach. Type of research is Normative Legal Research. The results showed that the crime of online fraud in principle the same as a conventional fraud, the difference is in the means of actions that using the Electronic Systems is a computer, internet, or other telecommunications equipment. So by applicable law, online fraud can be treated the same as a conventional offense set out in the Code of Penal (KUHP), then the process of handling the case is also based both on the Criminal Code and the law on information and electronic transactions. Similarly, the procedural law that is based on the KUHAP.

Key words: *Cybercrime, criminal, online fraud.*

1. Pendahuluan

Saat ini istilah *Cyber Law* telah digunakan secara internasional untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi. Hukum siber atau *cyber law*, secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi dan komunikasi. Demikian pula, hukum telematika yang merupakan perwujudan dari konvergensi hukum telekomunikasi, hukum media, dan hukum informatika. Istilah lain yang juga digunakan adalah hukum teknologi informasi *(law of information technology)*, hukum dunia maya *(virtual world law)*, dan hukum mayantara (Ahmad Ramli, 2006). Istilah-istilah tersebut lahir mengingat kegiatan yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet), memanfaatkan teknologi informasi berbasis sistem komputer yang merupakan sistem elektronik yang dapat dilihat secara virtual. Permasalahan hukum yang seringkali dihadapi adalah ketika terkait dengan penyampaian informasi, komunikasi, dan/atau transaksi secara elektronik, khususnya dalam hal pembuktian dan hal yang terkait dengan perbuatan hukum yang dilaksanakan melalui sistem elektronik.

Sistem elektronik adalah sistem komputer dalam arti luas, yang tidak hanya mencakup perangkat keras dan perangkat lunak komputer, tetapi juga mencakup jaringan telekomunikasi dan/atau sistem komunikasi elektronik. Perangkat lunak atau program komputer adalah sekumpulan instruksi yang diwujudkan dalam bentuk bahasa, kode, skema, ataupun bentuk lain, yang apabila digabungkan dengan media yang dapat dibaca dengan komputer akan mampu membuat komputer bekerja untuk melakukan fungsi khusus atau untuk mencapai hasil yang khusus, termasuk persiapan dalam merancang instruksi tersebut. Sistem elektronik juga digunakan untuk menjelaskan keberadaan sistem informasi yang merupakan penerapan teknologi informasi yang berbasis jaringan telekomunikasi dan media elektronik, yang berfungsi merancang, memproses, menganalisis, menampilkan, dan mengirimkan atau menyebarkan informasi elektronik. Sistem informasi secara teknis dan manajemen sebenarnya adalah perwujudan penerapan produk teknologi informasi ke dalam suatu bentuk organisasi dan manajemen sesuai dengan karakteristik kebutuhan pada organisasi tersebut dan sesuai dengan tujuan peruntukannya. Pada sisi yang lain, sistem informasi secara teknis dan fungsional adalah keterpaduan sistem antara manusia dan mesin yang mencakup komponen perangkat keras, perangkat lunak, prosedur, sumber daya manusia, dan substansi informasi yang dalam pemanfaatannya mencakup fungsi *input*, *process*, *output*, *storage*, dan *communication*.

Tindak pidana yang dilakukan melalui dunia maya atau internet disebut dengan istilah cyber crime. Dalam hal ini, *cyber crime* adalah bentuk perbuatan kriminal yang menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakannya (Widodo, 2011). Jadi, *cybercrime* merupakan bentuk kriminal yang menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal. Dalam definisi lain, kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Bagi sebagian kalangan,

kejahatan siber ini hanya dalam ruang lingkup kejahatan penipuan, *hacker*, penyebaran berita palsu maupun penyebaran suatu hal yang mengandung unsur pornografi, tetapi bukan hal tersebut saja yang dapat dikatakan sebagai *Cybercrime*, karena banyak sekali bentuk kejahatan lain yang masih asing dan termasuk dalam kategori *Cyber Crime* (Josua Sitompul, 2012).

Istilah *Cybercrime* juga digunakan untuk jenis kejahatan tradisional dimana komputer atau jaringan komputer digunakan untuk mempermudah atau memungkinkan kejahatan itu terjadi. Salah satu jenis kejahatan tersebut adalah penipuan yang dilakukan secara *online*. Penipuan *online* yang dimaksud adalah penipuan yang menggunakan media internet, baik untuk keperluan bisnis dan perdagangan sehingga tidak lagi mengandalkan basis perusahaan yang konvensional secara nyata (Asril Sitompul, 2001), termasuk jenis penipuan lain yang umumnya berkedok undian berhadiah. Penipuan sendiri memiliki arti sebagai penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita-berita tertentu, iklan atau informasi lainnya yang mengakibatkan ketidaknyamanan atau kerugian bagi pengguna web. Penipuan ini biasanya datang dengan cara bertubi-tubi tanpa diminta dan tidak dikehendaki oleh korbannnya.

Pada awalnya penipuan melalui media internet ini dilakukan dengan menggunakan fasilitas *email*, namun seiring dengan perkembangan teknologi, fasilitas dunia mayapun semakin bervariasi, sehingga penipuan melalui internet tidak hanya terbatas pada *email*, namun juga pada blog maupun situs-situs tertentu. Penipuan melalui internet pada blog biasanya berisi iklan dan mengarahkan pada situs yang berkualitas rendah atau situs berbahaya yang mengandung penipuan atau berita bohong. Biasanya penipuan seperti ini dikirim dengan tujuan tertentu misalnya sebagai media publikasi dan promosi untuk produk-produk perusahaan yang dilakukan oleh pemilik *email* atau *spammer* (Widodo. 2013). Penipuan secara *online* pada prinisipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan Sistem Elektronik yaitu komputer, internet, atau perangkat telekomunikasi lainnya. Sehingga secara hukum, penipuan secara *online* dapat diperlakukan sama sebagaimana delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP).

Selain penipuan melalui internet, terdapat pula penipuan melalui SMS *(Short Message Service*) yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Media yang digunakan dalam penipuan SMS adalah *handphone* yang merupakan salah satu media elektronik, sebagaimana yang dimaksud dalam UU ITE. Hal tersebut sesuai dengan Pasal 1 angka 2 UU ITE bahwa :“ Transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya”. Sebelum diundangkannya UU ITE, pengaturan mengenai penipuan yang dilakukan melalui SMS diatur dalam Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Namun demikian pada masa sekarang ini, penipuan melalui SMS juga mencantumkan *website* dalam isi SMS yang dikirim, sehingga perbuatan demikian diatur baik dalam undang-undang telekomunikasi maupun dalam UU ITE.

Hukum telekomunikasi masuk dalam kerangka hukum telematika.

Perkembangan aspek-aspek telematika bergerak begitu cepat mengikuti perubahan dunia. Aspek-aspek tersebut terus menyesuaikan diri dalam praktik secara substansi, sementara dari sisi aturan main cenderung kurang signifikan, sehingga peran pemerintah dalam hal ini menjadi sangat penting untuk merumuskan kerangka akomodatif terhadap setiap masalah yang dihadapi (Maskun, 2013).

Aturan hukum telematika menjadi landasan bagi para penegak hukum dalam menjalankan tugasnya baik dalam konteks *ius constitutum* maupun *ius constituendum*. Dasar hukum yang digunakan untuk menjerat pelaku penipuan adalah Pasal 378 KUHP, yang menyatakan bahwa: "Barang siapa dengan maksud 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 menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama 4 tahun". Sedangkan berdasarkan Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, lebih spesifik diatur dalam ketentuan Pasal 28 ayat (1) yang menyatakan bahwa “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik”.

Ketentuan dalam Pasal 28 ayat (1) UU No. 11 Tahun 2008 tersebut, dapat dikatakan masih belum sempurna atau masih kabur untuk digunakan sebagai dasar acuan dalam penanganan tindak pidana penipuan, khususnya di dunia maya. Hal ini disebabkan karena tindakan penipuan itu sendiri memiliki berbagai bentuk. Ketentuan Pasal 28 ayat 1 UU No. 11 Tahun 2008, pada dasarnya hanya mengatur tentang tindakan penyebaran berita bohong dan menyesatkan. Jika pasal ini digunakan terhadap tindakan penipuan, maka pasal tersebut masih terlalu kabur dan belum mencukupi untuk menjerat pelaku tindak pidana penipuan yang dilakukan melalui internet. Selain itu definisi penipuan juga belum dicantumkan secara jelas dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang-undang tersebut hanya mencantumkan unsur-unsur dan kualifikasi dari *cybercrime* secara umum, dan belum membedakan apakah kualifikasi dari *cybercrime* tersebut masuk dalam kategori *cracking, hacking, carding, phising, spamming* ataupun yang lainnya.

Berdasarkan uraian tersebut di atas, maka sangat menarik untuk dapat menguraikan problematika yang terkait dengan tindak pidana penipuan, baik yang dilakukan melalui media internet maupun yang dikirim melalui *Short Messages Service* (SMS). Pokok permasalahan yang akan dibahas dalam penulisan ini yaitu tentang pengaturan mengenai tindak pidana penipuan yang dilakukan secara online, serta bagaimanakah upaya penaganan perkaranya sesuai dengan ketentuan hukum yang berlaku, baik berdasarkan KUHP maupun berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

2. Landasan Teori

Karakteristik internet di mana orang dapat berlalu-lalang tanpa identitas *(anonymous)* memungkinkan terjadinya berbagai aktivitas jahat yang sulit untuk tersentuh hukum, seperti *Illegal access* yang melingkupi pelanggaran dasar dari ancaman-

ancaman berbahaya dari serangan terhadap keamanan data dan sistem computer. Indonesia sebagai bagian dari negara bangsa di dunia, termasuk sebagai salah satu negara yang cukup banyak memiliki penyalahgunaan dalam pemanfaatan jaringan internet, khususnya dalam hal pemesanan barang-barang atau perdagangan dengan menggunakan media internet (Ilhamd Wahyudi, 2006). Kondisi ini dapat merugikan pihak Indonesia, khususnya terhadap dunia perdagangan yang dilakukan melalui media internet.

European Convention on Cyber Crime merupakan konvensi tentang *cyber crime* yang disepakati oleh Negara-negara anggota Uni Eropa, namun konvensi ini terbuka bagi Negara lain di luar Uni Eropa untuk mengikutinya. Oleh karena banyak Negara yang mengikuti konvensi tersebut, maka isi perjanjian ini menjadi model bagi banyak pengaturan cyber crime di berbagai negara. Oleh karenanya menjadi penting bagi Indonesia untuk merujuk konvensi ini sebagai salah satu pembanding dalam pengaturan *cyber crime*, terlebih lagi J.E Sahetapy pernah mengungkapkan bahwa hukum pidana di Indonesia, belum siap menghadapi kejahatan komputer, karena tidak segampang itu menganggap kejahatan komputer berupa pencurian data sebagai pencurian. Kalau dikatakan pencurian, tentu harus ada barang yang hilang. Padahal dalam kejahatan komputer, data si pemilik masih ada kendati sudah dicuri orang lain (Widyopramono, 1994). Bagaimana dengan *cybercrime*, tentu tantangan yang dihadapi menjadi lebih berat. Barda Nawawi Arief menyatakan bahwa *cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini. Ada beberapa faktor yang mempengaruhi terjadinya *cybercrime*, yaitu faktor politik, faktor ekonomi dan faktor sosial budaya (Sutarman, 2007).

Berbagai bentuk perbuatan *cyber crime* dalam *European Convention on Cyber Crime* yang dapat menjadi rujukan oleh Indonesia dalam pengaturan tentang *Cyber Crime* adalah :

1) Delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan system computer, yaitu:
   a) Mengakses system computer tanpa hak (*illegal acces*);
   b) Tanpa hak menangkap/mendengar pengiriman dan pemancaran (*illegal interception*);
   c) Tanpa hak merusak data (*data interference*);
   d) Tanpa hak mengganggu system (*system interference*);
   e) Menyalahgunakan perlengkapan (*misuse of device*).
2) Delik-delik yang berhubungan dengan computer, pemalsuan, dan penipuan (*computer related pffences; forgery and fraud*);
3) Delik-delik yang bermuatan pornogrofi anak (*content-related offences, child pornography*);
4) Delik-delik yang berhubungan dengan hak cipta (*offences related of infringements of copyrights*).

Berbagai bentuk delik tersebut di atas menjadi sandaran dalam memahami ketentuan-ketentuan yang terdapat dalam UU ITE, serta menilai sejauhmana terdapat harmonisasi hukum dalam pengaturan tersebut.

3. Metode Penelitian

Penelitian ini adalah penelitian hukum (*legal research*) yang mengkaji ketentuan-ketentuan dan prinsip-prinsip hukum yang mengatur tentang tindak pidana penipuan, khususnya yang dilakukan secara online melalui media

internet maupun yang dikirim melalui fasilitas *Short Messages Service* (SMS). Dalam penelitian ini akan dikaji dan dianalisis tentang teori yang melandasi prinsip-prinsip penegakan hukum terhadap tindak pidana penipuan yang dihubungkan dengan ketentuan-ketentuan sebagaimana yang diatur dalam undang-undang, baik berdasarkan KUHP maupun berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Penelitian ini termasuk dalam kategori tipe penelitian normatif atau *Normative Legal Research*. Pendekatan yang digunakan dalam penelitian ini adalah: *statuta approach*, *conseptual approach*, dan *comparative approach*. Teknik analisis yang digunakan adalah penalaran dan argumentasi hukum untuk menjawab isu-isu penelitian yang diajukan sesuai dengan pendekatan yang digunakan.

4. Hasil Penelitian Dan Pembahasan

4.1 Pengaturan Hukum Tindak Pidana Penipuan Melalui Internet

Penipuan yang dilakukan secara *online* melalui media internet adalah penipuan dengan menggunakan sarana komputer dan jaringannya. Penipuan tersebut merupakan bentuk pelanggaran hukum yang dilakukan dengan cara memodifikasi data atau sistem komputer, menyebarkan berita palsu atau bohong sehingga mengakibatkan kerugian pada pihak lain. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada dasarnya tidak mengatur secara khusus mengenai tindak pidana penipuan. Namun demikian, dasar yuridis untuk melakukan penanganan hukum terhadap perbuatan penipuan melalui komputer, diatur dalam Pasal 28 ayat (1) UU Nomor 11 Tahun 2008.

Tindak pidana penipuan diatur dalam Pasal 378 Kitab Undang-Undang Hukum Pidana, dengan rumusan pasal sebagai berikut : “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun”. Walaupun UU ITE tidak secara khusus mengatur mengenai tindak pidana penipuan, namun terkait dengan timbulnya kerugian bagi salah satu pihak, baik selaku konsumen maupun produsen dalam transaksi elektronik, maka terdapat ketentuan Pasal 28 ayat (1) UU ITE yang menyatakan bahwa “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.” Perbuatan tersebut masuk dalam kategori perbuatan yang dilarang sebagaimana yang diatur dalam Bab VII UU ITE.

Pengertian berita bohong dan menyesatkan sebagaimana yang diatur dalam ketentuan Pasal 28 ayat (1) UU ITE adalah berita yang berisi informasi tidak benar, yang menurut orang pada umumnya dapat membuat konsumen melakukan transaksi mengambil keputusan yang seharusnya tidak dilakukan apabila yang bersangkutan mengetahui sebelumnya bahwa informasi tersebut adalah tidak benar. Contoh informasi tidak benar yang dimaksud antara lain adalah informasi mengenai syarat kontrak, produsen, dan produk yang ditawarkan. Akibat informasi yang tidak benar itu, maka konsumen mengalami kerugian, yang dimaksud kerugian disini haruslah kerugian ekonomis yang dapat

diperhitungkan secara materil. Ketentuan Pasal 28 ayat (1) UU ITE sejalan dengan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen yang bertujuan antara lain, untuk meningkatkan kesadaran dan kemandirian konsumen untuk melindungi dirinya dan menciptakan sistem perlindungan terhadap konsumen dengan memberikan kepastian hukum dan keterbukaan informasi serta akses untuk mendapatkan informasi.

Sesuai dengan ketentuan Pasal 45 ayat (2) UU No.11 Tahun 2008, ditetapkan bahwa "setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)". Terkait dengan tindak pidana penipuan, antara KUHP dan UU ITE terdapat perbedaan, yaitu rumusan Pasal 28 ayat (1) UU ITE tidak mensyaratkan adanya unsur "menguntungkan diri sendiri atau orang lain" sebagaimana diatur dalam Pasal 378 KUHP tentang penipuan. Namun demikian, kedua pasal tersebut juga memiliki kesamaan, yaitu tentang akibat yang timbul oleh tindak pidana penipuan, yaitu dapat mengakibatkan kerugian bagi orang lain. Namun pada prakteknya pihak kepolisian dapat saja mengenakan pasal-pasal berlapis terhadap suatu perbuatan pidana, termasuk pada tindakan penipuan sebagaimana diatur dalam Pasal 378 KUHP dan juga Pasal 28 ayat (1) UU ITE. Artinya, bila unsur-unsur tindak pidananya terpenuhi, maka polisi dapat menggunakan kedua pasal tersebut untuk menjerat pelaku tindak pidana penipuan sepanjang mampu terpenuhi unsur-unsurnya. Secara umum, dengan adanya Undang-Undang No.11 Tahun 2008, yang mengatur tentang Informasi dan Transaksi Elektronik, maka memungkinkan bagi aparat penegak hukum untuk dapat memproses berbagai macam kejahatan yang dilakukan melalui media-media elektronik.

Bentuk upaya penanggulangan *cybercrime* atau kejahatan di bidang komputer dengan menggunakan sarana penal adalah dengan menggunakan kebijakan/politik hukum pidana (*penal policy*) yang lebih sesuai dengan keadaan dan situasi pada saat sekarang dan untuk masa-masa yang akan datang. Oleh karena itu dibentuklah Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Hal ini dimaksudkan untuk mengatasi permasalahan sebelumnya terkait dengan pengaturan tentang penanggulangan *cybercrime* yang masih tersebar di berbagai peraturan perundang-undangan yang berlaku. Pengaturan tersebut lebih bersifat sektoral dan memiliki keterbatasan, misalnya dalam Undang-Undang Telekomunikasi dan Undang-Undang Pers. Pertanggungjawaban pidananya sebagaimana yang diatur dalam undang-undang informasi dan transaksi elektronik dapat dijatuhkan kepada *individu* dan *korporasi.*

4.2 Penanganan Perkara Tindak Pidana Penipuan Melalui Internet

Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawai negeri sipil tertentu yang diberi wewenang khusus oleh undang-undang. Menurut ketentuan Pasal 7 KUHAP wewenang penyidik yaitu :

a) Menerima laporan atau pengaduan dari seorang tentang adanya tindak pidana;
b) Melakukan tindakan pertama pada saat di tempat kejadian;
c) Menyuruh berhenti seorang tersangka dan memeriksa tanda

pengenal dari tersangka;
d) Melakukan penangkapan, penahanan, penggeledahan dan penyitaan;
e) Melakukan pemeriksaan dan penyitaan surat;
f) Mengambil sidik jari dan memotret seorang;
g) Memanggil orang untuk didengar dan diperiksa sebagai tersangka atau saksi;
h) Mendatangkan orang ahli yang diperlukan dalam hubungannya dengan pemeriksaan perkara;
i) Mengadakan penghentian penyidikan;
j) Mengadakan tindakan lain menurut hukum yang bertanggung jawab.

Berdasarkan ketentuan Pasal 15, Peraturan Kepala Kepolisian Negara Republik Indonesia No. 14 Tahun 2012, kegiatan penyidikan dilaksanakan secara bertahap meliputi: penyelidikan; pengiriman SPDP; upaya paksa; pemeriksaan; gelar perkara; penyelesaian berkas perkara; penyerahan berkas perkara ke penuntut umum; penyerahan tersangka dan barang bukti; dan penghentian penyidikan. Secara rinci kegiatan tersebut terjabar dalam uraian berikut:

1. Penyelidikan

Berdasarkan ketentuan Pasal 1 angka 5 KUHAP, pengertian penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang ini. Merujuk pada ketentuan Pasal 1 angka 4 KUHAP, maka penyelidikan perbuatan yang diduga *cybercrime* dilakukan pejabat Polri dan PNS sebagaimana yang diatur dalam undang-undang.

2. Pengiriman Surat Pemberitahuan Dimulainya Penyidikan (SPDP)

Pasal 109 ayat (1) KUHAP mengatur bahwa dalam hal penyidik telah memulai melakukan penyidikan suatu peristiwa yang merupakan tindak pidana, penyidik memberitahukan hal itu kepada penuntut umum. Karena itu, berdasarkan Perkap No 14 tahun 2012 Pasal 1 angka 17, ditentukan bahwa Surat Pemberitahuan Dimulainya Penyidikan adalah surat pemberitahuan kepada Kepala kejaksaan tentang dimulainya penyidikan yang dilakukan oleh penyidik Polri.

3. Upaya Paksa

Merujuk pada ketentuan Pasal 26 Perkap No 14 Tahun 2012, upaya paksa meliputi: a.pemanggilan; b. penangkapan; c. penahanan; d. penggeledahan; e. penyitaan, dan f. pemeriksaan surat. Berdasarkan ketentuan Pasal 43 ayat (6) diatur bahwa dalam hal melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam.

Selanjutnya menurut ketentuan Pasal 43 ayat (3) UU ITE, diatur bahwa Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin ketua pengadilan negeri setempat. Sedangkan dalam ayat (4) diatur bahwa dalam melakukan penggeledahan dan/atau penyitaan, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

4. Pemeriksaan

Pasal 63 Perkap No 14 Tahun 2012, bahwa pemeriksaan dilakukan oleh penyidik atau penyidik pembantu terhadap saksi, ahli, dan tersangka yang dituangkan dalam berita acara pemeriksaan yang ditandatangani oleh penyidik/penyidik pembantu yang melakukan pemeriksaan dan orang yang diperiksa. Tujuannya untuk

mendapatkan keterangan saksi, ahli dan tersangka yang dituangkan dalam berita acara pemeriksaan, guna membuat terang perkara sehingga peran seseorang maupun barang bukti dalam peristiwa pidana yang terjadi dapat diketahui secara jelas.

Berkaitan dengan proses pemeriksaan barang bukti digital baik pada saat penyidikan maupun pemeriksaan di pengadilan, perlu ada kemampuan yang memadai dari penegak hukum. Dalam penanganan data elektronik diperlukan langkah-langkah khusus agar bukti digitalnya tidak berubah. Karena itu, penyidik harus memahami penanganan awal barang bukti elektronik pada komputer di tempat kejadian perkara, penggandaan secara *Physical* sektor per sektor (*forensic imaging*), analisis sistem file (*file system*) dari Program *Microsoft Windows*, mencari dan memunculkan file walaupun sudah dihapus dan diformat, atau data yang tidak pernah disimpan dan hanya di print (*files recovery*), analisis telepon seluler (*mobile forensic*), analisis rekaman suara (*audio forensic*), analisis rekaman video (*video forensic*), dan analisis gambar digital (*image forensic*).

Perkara *cybercime* merupakan perkara khusus yang cara penyidikannya dapat berbeda sebagaimana penyidikan dalam perkara umum. Dalam melaksanakan tugas dan peranannya maka fungsi reserse khususnya satuan *cybercrime* mendasarkan pada beberapa undang-undang yang terkait dengan tindak pidana *cybercrime* yang terjadi. Salah satunya sebagai pedoman alat bukti yaitu ketentuan dalam Pasal 184 KUHAP, dimana yang dimaksud alat-alat bukti adalah keterangan saksi, keterangan ahli, surat, petunjuk, dan keterangan terdakwa. Selain itu penyidik dapat menggunakan penyidik *cybercrime* menggunakan alat bukti yaitu Informasi Elektronik dan atau Dokumen Elektronik dan/atau hasil cetaknya. Namun informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam UU ITE. Selain itu informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk surat yang menurut undang-undang harus dibuat dalam bentuk tertulis. Demikian pula dengan surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta.

Selanjutnya Menurut ketentuan Pasal 6 UU No.11 tahun 2008, diatur pula bahwa dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, informasi elektronik dan/atau dokumen elektronik, maka akan dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan. Dalam ketentuan Pasal 44 UU ITE diatur bahwa, alat bukti penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan undang-undang ini adalah sebagai berikut: a. alat bukti lain berupa Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud dalam Pasal 1 angka 1 dan angka 4 serta Pasal 5 ayat (1), ayat (2), dan ayat (3). Berdasarkan ketentuan tersebut, maka alat bukti dalam *cybercrime* adalah sebagai berikut :

a) Informasi Elektronik yaitu satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta,

rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. Hal ini sesuai dengan ketentuan Pasal 1 angka 1 UU No.11 Tahun 2008.

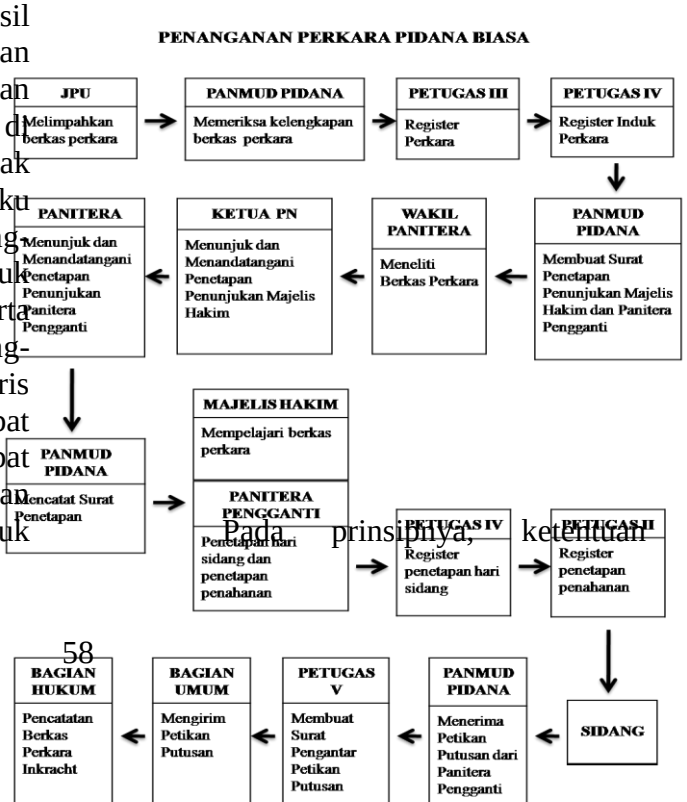
b) Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, Kode Akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. Hal ini didasarkan pada ketentuan Pasal 1 angka 4 UU No.11 Tahun 2008.

Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Informasi Elektronik dan/atau Dokumen Elektronik ataupun hasil cetaknya merupakan bentuk perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia. Namun demikian, hasil cetak dokumen elektronik tidak berlaku untuk: a). surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan b). surat beserta dokumennya yang menurut Undang-Undang harus dalam bentuk akta notaris atau akta yang dibuat oleh pejabat pembuat akta. Dalam hal terdapat ketentuan lain yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

5. Penyerahan Berkas Perkara Ke Penuntut Umum

Sesuai dengan ketentuan Pasal 110 KUHAP diatur bahwa dalam hal penyidik telah selesai melakukan penyidikan, penyidik wajib segera menyerahkan berkas perkara itu kepada penuntut umum. Dalam hal penuntut umum berpendapat bahwa hasil penyidikan tersebut ternyata masih kurang lengkap, maka penuntut umum segera mengembalikan berkas perkara itu kepada penyidik disertai petunjuk untuk dilengkapi.

Dalam hal penuntut umum mengembalikan hasil penyidikan untuk dilengkapi, penyidik wajib segera melakukan penyidikan tambahan sesuai dengan petunjuk dari penuntut umum. Penyidik dianggap telah selesai apabila dalam waktu empat belas hari penuntut umum tidak mengembalikan hasil penyidikan atau apabila sebelum batas waktu tersebut berakhir telah ada pemberitahuan tentang hal itu dari penuntut umum kepada penyidik.



Pada prinsipnya, ketentuan

tentang Penyidikan dan Penuntutan dalam KUHAP di atas menunjukkan hubungan yang erat antara penyidikan dengan penuntutan. Secara ringkas dapat dikatakan bahwa penyidikan merupakan kegiatan untuk mengumpulkan alat bukti mengenai adanya satu tindak pidana beserta pelaku tindak pidana tersebut, sementara penuntutan merupakan kegiatan yang ditujukan untuk mempertanggungjawabkan hasil dari kegiatan penyidikan di forum pengadilan. Dalam hal ini, pelaksanaan dari *integrated criminal justice system* sebetulnya adalah untuk melaksanakan penegakan hukum yang terpadu dan berkesinambungan untuk mendapatkan *out put* yang maksimal. Penyidikan haruslah diarahkan kepada pembuktian di persidangan, sehingga tersangka (pelaku tindak pidana) dapat dituntut dan diadili di persidangan. Penyidikan yang berakhir dengan putusan (*vrisjpraak*) ataupun lepas dari segala tuntutan (*onslag van alle rechtsvervolging*) dari Pengadilan terhadap pelaku tindak pidana akan merugikan masyarakat dan lembaga penegak hukum itu sendiri.

Penipuan secara online masuk dalam kategori perkara pidana biasa. Bilamana terjadi tindak pidana penipuan yang dilakukan secara online, maka pihak korban dapat melaporkannya kepada Aparat Penegak Hukum disertai bukti awal berupa data/informasi elektronik dan/atau hasil cetaknya. Jika kasus tersebut ditindaklanjuti oleh kepolisian dalam suatu proses penyelidikan/penyidikan, maka pihak kepolisian akan menelusuri sumber dokumen elektronik tersebut. Dalam praktek, biasanya yang pertama-tama dilacak adalah keberadaan pelaku dengan menelusuri alamat *Internet Protocol* (*IP Address*) pelaku berdasarkan *log IP Address* yang tersimpan dalam *server* pengelola *web site/homepage* yang dijadikan sarana pelaku dalam melakukan penipuan. Namun demikian, permasalahan yang sering kali timbul adalah, pihak kepolisian akan menemui kesulitan jika *web site/homepage* tersebut pemiliknya berada di luar wilayah yurisdiksi Indonesia. Meskipun saat ini Aparat Penegak Hukum (polisi maupun Penyidik Pegawai Negeri Sipil/PPNS Kementerian Komunikasi dan Informatika) telah bekerja sama dengan beberapa pengelola *website/homepage* di luar wilayah Indonesia, dalam prakteknya tidak mudah untuk mendapatkan *IP address* seorang pelaku yang diduga melakukan tindak pidana dengan menggunakan layanan *web site/homepage* tertentu. Hal ini disebabkan oleh adanya perbedaan prosedur hukum antar negara. Meskipun pemerintah melalui aparat penegak hukum telah membuat perjanjian *Mutual Legal Asistance* atau perjanjian bantuan hukum timbal balik, pada kenyataannya MLA tidak serta merta berlaku dalam setiap kasus yang melibatkan antar negara. Permasalahan yurisdiksi inilah yang seringkali menjadi penyebab tidak dapat diprosesnya atau tertundanya penyelidikan/penyidikan kasus-kasus *cyber crime*. Oleh karena itu, pemerintah dan lembaga lain yang terkait perlu melakukan langkah-langkah tertentu untuk dapat mengatasi hambatan-hambatan yang dihadapi dalam penegakan hukum, khususnya terhadap tindak kejahatan yang dilakukan melalui media internet.

Terkait dengan subjek pelaku tindak pidana, maka pertanggungjawaban pidana dalam Undang-Undang ITE dapat dijatuhkan kepada *individu* dan *korporasi*. Hal ini terlihat dari subjek tindak pidana yang terkandung dalam ketentuan pidananya,

yaitu setiap orang. Pengertian orang dalam Ketentuan Umum Pasal 1 ayat (21) adalah *orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum*. Bahkan secara eksplisit, pertanggungjawaban korporasi dalam tindak pidana UU ITE disebutkan secara tegas dalam Pasal 52 ayat(4).

Dalam Undang-Undang ITE, korporasi juga merupakan subjek tindak pidana. Maka seharusnya diatur pula sistem pertanggungjawaban korporasi yang jelas dan terperinci, khususnya berkaitan dengan kapan korporasi dikatakan melakukan tindak pidana, siapa yang bertanggung jawab dan sanksi pidana yang dapat dijatuhkan. Namun dalam undang-undang ini justru tidak diatur mengenai tiga hal pokok tersebut. Terkait sanksi pidana misalnya, hanya disebutkan pidana pokoknya ditambah dua pertiga. Tidak diatur jenis sanksi lain yang lebih tepat bagi korporasi, seperti tindakan tata tertib penutupan sementara atau selamanya.

5. Kesimpulan

Sebagaimana yang telah diuraikan sebelumnya pada bagian pembahasan, maka dapat dibuat kesimpulan bahwa pengaturan mengenai tindak pidana penipuan yang dilakukan secara online pada prinsipnya sama dengan penipuan konvensional, yang membedakan hanyalah pada sarana perbuatannya yakni menggunakan Sistem Elektronik (komputer, internet, perangkat telekomunikasi). Sehingga secara hukum, penipuan secara *online* dapat diperlakukan sama sebagaimana delik konvensional yang diatur dalam Kitab Undang-Undang Hukum Pidana (KUHP). Dengan demikian dalam proses penanganan perkaranya, aparat penegak hukum dapat menerapkan ketentuan-ketentuan hukum, baik yang terdapat dalam KUHP maupun ketentuan-ketentuan hukum yang terdapat dalam UU No. 11 Tahun 2008. Demikian pula dengan prosedur beracaranya, penipuan secara online secara formal akan diproses dan ditangani oleh penyidik, sesuai dengan ketentuan yang diatur dalam KUHAP. Hal ini juga sesuai dengan ketentuan Pasal 42 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

DAFTAR PUSTAKA

Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara (Cybercrime)*, Refika Aditama, Bandung.

Ahmad Ramli, 2006. *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung.

Asril Sitompul, 2001. *Hukum Internet : Pengenalan Mengenai Masalah Hukum di Cyberspace*, Citra Aditya Bakti, Bandung.

Barda Nawawi Arief, 2006. *Tindak Pidana Mayantara: Perkembangan Kajian Cyber Crime Di Indonesia.* PT. Rajagrafindo Persada, Jakarta.

Council of Europe, *Explanatory Report To The Convention on Cybercrime* (ETS No 185), poin ke 44.

Ilhamd Wahyudi (2006). *Kebijakan Pidana Terhadap Kejahatan Mayantara.* Tesis. Program Pascasarjana Unand-Unri. Padang.

Josua Sitompul, 2012. *Cyberspace, Cybercrimes, Cyberlaw : Tinjauan Aspek Hukum*

Pidana, Tatanusa, Jakarta.

Maskun, 2013. *Kejahatan Siber;Cybercrime Suatu Pengantar*, Kencana, Makasar.

Sutarman, 2007. *Cybercrime (Modus Operandi dan Penanggulangannya)*, LaksBang Pressindo, Yogyakarta.

Volodymyr Golubev, *Cyber-crime and legal problems of Internet usage*, p.1; Zaporizhia Law Institute, Ministry of Interior of Ukraine.

Widodo, 2011. *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law); Telaah Teoritik dan Bedah Kasus*, Aswaja Presindo, Yogyakarta.

Widodo. 2013. *Aspek Hukum Pidana Kejahatan Mayantara*. Aswaja Presindo. Yogyakarta.

Widyopramono, 1994. *Kejahatan di Bidang Komputer*, Pustaka Sinar Harapan, Jakarta.