BAB III

PERKEMBANGAN KASUS, MODUS OPERANDI, DAN CONTOH KASUS TINDAK PIDANA PENIPUAN MELALUI INTERNET DI INDONESIA

A. Perkembangan Kasus Tindak Pidana Penipuan Melalui Internet di Indonesia

Internet di Indonesia dimulai pertama kali pada tahun 1990-an. Masyarakat menggunakan internet pada saat itu masih sangat terbatas, bisanya masyarakat yang berada di kota-kota besar yang menggunakannya. Berbeda dengan sekarang, masyarakat dari segala kalangan dapat menggunakan internet untuk berbagai macam hal. Kalangan tua, muda, sampai anak-anak sekarang mampu menggunakan internet untuk kebutuhannya. Bisnis *online* pada saat sekarang ini semakin marak sekali dilakukan masyarakat untuk memperjualbelikan barang dagangannya.

Banyak hal yang menjadi alasan masyarakat menggunakan internet untuk memperluas usahanya seiring dengan perkembangan internet yang semakin pesat. Di samping banyak kemudahan yang diberikan dalam transaksi jual beli *online,* namun banyak juga kasus-kasus tindak pidana penipuan dalam transaksi jual beli melalui media sosial *online*.

Peringkat Indonesia dalam kejahatan di dunia maya (menggunakan internet) telah menggantikan posisi Ukraina yang sebelumnya menduduki posisi pertama. Indonesia menempati persentase tertinggi dalam hal

kejahatan di dunia maya. Indikasinya dapat dilihat dari banyaknya kasus pemalsuan kartu kredit dan pembobolan sejumlah bank.

Kejahatan di dunia maya yang marak terjadi di Indonesia meliputi penipuan kartu kredit, penipuan perbankan, *defacking*, *cracking*, transaksi seks, judi *online* dan terorisme dengan korban yang berasal dari luar negeri seperti Amerika Serikat, Inggris, Australia, Jerman, Korea, serta Singapura juga beberapa daerah di tanah air.

Saat ini penanganan tindak pidana penipuan dalam transaksi jual beli melalui media sosial *online* di Indonesia masih minim, padahal Indonesia termasuk negara dengan kasus tindak pidana penipuan dalam transaksi jual beli melalui media sosial *online* tertinggi. Penanganan kasus kejahatan jenis ini memang membutuhkan kemampuan khusus dari para penegak hukum. Dari kasus-kasus yang terungkap selama ini, pelaku diketahui memiliki tingkat kepandaian di atas rata-rata. Selain karena motif ekonomi, sebagian *hacker* melakukan tindakan merusak *website* orang lain hanya sekedar untuk pamer kemampuan.

B. Modus Operandi Tindak Pidana Penipuan Melalui Internet di Indonesia

Tindak pidana penipuan melalui internet adalah suatu kejahatan konvensional yang dilakukan di dunia nyata. Namun karena perkembangan teknologi informasi dan komunikasi, maka modus operandi kejahatan penipuan beralih menggunakan pemanfaatan teknologi tersebut dan dampaknya juga ada pada dunia nyata seperti adanya pihak atau

korban yang dirugikan baik manusia orang perorangan maupun organisasi atau instansi.

Kejahatan di dunia maya terjadi dengan berbagai macam cara dengan berbagai macam modus operandi dan istilah, diantaranya adalah:[59]

1. *Carding* yang merupakan kejahatan dengan menggunakan teknologi komputer untuk melakukan transaksi dengan menggunakan kartu kredit orang lain sehingga dapat merugikan orang tersebut baik secara materil maupun non materil dalam artian penipuan kartu kredit secara *online*.
2. *Cracking* yang merupakan kejahatan dengan menggunakan teknologi komputer yang dilakukan untuk merusak sistem keamanan suatu sistem komputer dan biasanya melakukan pencurian.
3. *Joy computing* yaitu pemakaian komputer orang lain tanpa izin.
4. *Hacking* yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
5. *The trojan horse* yaitu manipulasi data atau program dengan jalan mengubah data atau intsruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau, dengan tujuan kepentingan pribadi atau orang lain.
6. *Data leakage* yaitu menyangkut pembocoran data ke luar terutama mengenai data yang harus dirahasiakan.

[59] http://cyberworld-it.blogspot.co.id/2012/11/modus-operandi-jenis-jenis-kejahatan.html, diakses pada tanggal 10 September 2016 pukul 16.58 WIB

7. *Data diddling* yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data atau output data.
8. *To frustate data communication* atau penyia-nyiaan data komputer.
9. *Software piracy* yaitu pembajakan software terhadap hak cipta yang dilindungi hak atas kekayaan intelektual.
10. *Cyber espionage* yang merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem yang *computerized*. Biasanya si penyerang menyusupkan sebuah program mata-mata yang dapat kita sebut sebagai spyware.
11. *Infringements of Privacy*, Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara *computerized*, yang apabila diketahui oleh orang lain maka dapat merugikan korban secara materil maupun immateril, seperti nomor kartu kredit, nomor PIN ATM, cacat atau penyakit tersembunyi dan sebagainya.
12. *Data Forgery* yang merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless*

document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.

13. *Unauthorized Access to Computer System and Service* yang merupakan kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan melakukannya dengan maksud melakukan sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukan hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet/intranet.
14. *Cyber Sabotage and Extortion* yang merupakan kejahatan yang paling mengenaskan, kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada

korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase tersebut, tentunya dengan bayaran tertentu. Kejahatan ini sering disebut sebagai *cyber-terrorism*.

15. *Offense against intellectual property*, kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet.
16. *Illegal contents* yang merupakan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.

C. Contoh Kasus Tindak Pidana Penipuan Melalui Internet di Indonesia

Contoh kasus mengenai tindak pidana penipuan dalam transaksi jual beli melalui media sosial *online* di Indonesia terjadi terhadap Santy Junitha Soekarno yang merupakan seorang penjual barang berupa tas, laptop, sepatu, *handphone*, dan kamera digital, barang-barang tersebut dijual oleh Santy Junitha Soekarno secara *online* melalui media sosial *facebook*. Santy Junitha Soekarno pun berkenalan dengan Nigel Frank melalui media sosial *facebook*, pada waktu berkenalan Nigel Frank mengaku sebagai supplier barang-barang seperti tas, laptop, sepatu, *handphone*, dan kamera digital yang berasal dari Inggris, dan Santy Junitha Soekarno tertarik untuk membeli barang-barang tersebut dari Nigel Frank dengan maksud akan dijual kembali oleh Santy Junitha Soekarno melalui media sosial *facebook*, Santy Junitha Soekarno pun

mengirimkan sejumlah uang kepada Nigel Frank dengan cara transfer ke Bank Mandiri Syariah, setelah uang tersebut ditransfer barang-barang yang dinginkan oleh Santy Junitha Soekarno tidak datang.

Kasus *cyber crime* dengan motif ekonomi terjadi juga pada Rizky Martin, yang berumur 27 tahun, alias Steve Rass, dan Texanto, umur 28 tahun, alias Doni Michael melakukan transaksi pembelian barang atas nama Tim Tamsin Invex Corp, perusahaan yang berlokasi di AS melalui internet. Keduanya menjebol kartu kredit melalui internet *banking* sebesar Rp. 350 juta. Dua pelaku ditangkap aparat *cyber crime* Polda Metro Jaya pada tanggal 10 Juni 2008 di sebuah warnet di kawasan Lenteng Agung, Jakarta Selatan.

Kasus *cyber crime* lainnya terjadi pada awal Mei 2008 lalu, Mabes Polri menangkap *hacker* bernama Iqra Syafaat, umur 24, di satu warnet di Batam, Riau, setelah melacak IP addressnya dengan *nick name* Nogra alias Iqra. Pemuda tamatan SMA tersebut dinilai polisi berotak encer dan cukup dikenal di kalangan *hacker*. Dia pernah menjebol data sebuah website lalu menjualnya ke perusahaan asing senilai Rp. 600 ribu dolar atau sekitar Rp. 6 miliar. Dalam pengakuannya, hacker lokal ini sudah pernah menjebol 1.257 situs jaringan yang umumnya milik luar negeri. Bahkan situs Presiden SBY pernah akan diganggu, tapi dia mengurungkan niatnya.

Kasus lain yang pernah diungkap polisi pada tahun 2004 ialah saat situs milik KPU (Komisi Pemilihan Umum) yang juga diganggu *hacker*.

Tampilan lambang 24 partai diganti dengan nama ‘partai jambu’, ‘partai cucak rowo’ dan lainnya. Pelakunya, diketahui kemudian, bernama Dani Firmansyah, umur 24 tahun, mahasiswa asal Bandung yang kemudian ditangkap Polda Metro Jaya. Motivasi pelaku, konon, hanya ingin menjajal sistem pengamanan di situs milik KPU yang dibeli pemerintah seharga Rp. 200 miliar itu, dan ternyata berhasil.

Data di Mabes Polri, dari sekitar 200 kasus *cyber crime* yang ditangani hampir 90 persen didominasi *carding* (berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara ilegal) dengan sasaran luar negeri. Aktivitas internet memang lintas negara. Yang paling sering jadi sasaran adalah Amerika Serikat, Australia, Kanada dan lainnya. Pelakunya berasal dari kota-kota besar seperti Yogyakarta, Bandung, Jakarta, Semarang, Medan serta Riau. Motif utama adalah ekonomi. Peringkat kedua adalah *hacking* dengan merusak dan menjebol website pihak lain dengan tujuan beragam, mulai dari membobol data lalu menjualnya atau iseng merusak situs tertentu.

Kasus *cyber crime* yang paling baru pada saat ini adalah aksi pembobolan pulsa, penyidik *cyber crime* Bareskrim Polri meringkus tujuh *hacker* server Telkomsel. Aksi pembobolan pulsa ini terbongkar setelah para tersangka menjualnya di situs popular kaskus. Mereka kini ditahan di Rutan Bareskrim Polri. Kasus ini melibatkan keahlian komputer, saat ini masih dikembangkan terus untuk mencari jaringannya yang lain,

pembobol itu awalnya melakukan aksinya untuk kepentingan mereka sendiri.

Tujuh *hacker* pembobol server Telkomsel tersebut berinisial FA, AH, MS, SP, DY, IA, dan LK. Tindak pidana pidana pencurian pulsa tersebut terjadi sejak Oktober 2010 di server provider Telkomsel. Pada awalnya mereka melakukan tindakan tersebut hanya iseng saja, dan dicoba berulang-ulang, setelah berhasil, mereka lantas tergiur untuk menjual pulsa dengan cara memasarkannya melalui situs Kaskus. Pada saat dilakukan audit keuangan di provider tersebut, ternyata jumlah pulsa yang dijual dengan uang yang diterima, jauh berbeda.

Selanjutnya, setelah ditelusuri, Telkomsel melapor ke Bareskrim Polri. Tim *cyber crime* lalu melaksanakan olah TKP (tempat kejadian perkara), bagaimana server Telkomsel bisa jebol dan bagaimana sistem pembayarannya, dan ada juga anggota Kepolisian yang mencoba menyamar sebagai pembeli juga. Sejak tanggal 6 Januari 2012, polisi menangkap tujuh orang tersangka. Penangkapan itu dilakukan di Jakarta dan Bandung.

Setiap tersangka mempunyai peran masing-masing, FA adalah otaknya, dia bertugas menjebol server provider. Sedangkan AH membantu FA dengan mencuri pulsa yang kemudian dijual pelanggan. MS membantu FA menjebol server dan menyiapkan *script* untuk memfasilitasi pencurian. SP juga membantu menjebol server, menyiapkan *script*, dan menjual pulsa. Sedangkan DY membantu, mencuri, menjual

pulsa. IA menjalankan tugas memasarkan pulsa, dan LK membantu AH menjual pulsa, menerima, dan menyimpan sejumlah uang untuk dimasukkan ke dalam rekening.

Kasus *cyber crime* lain yang berkaitan dengan internet *banking* telah diungkapkan oleh pihak Kepolisian Republik Indonesia, satuan *cyber crime* Direktorat Kriminal Khusus Polda Metro Jaya membekuk pelaku pembobol rekening bank swasta melalui media internet *banking*. Pelaku berinisial Eyn dan mengaku telah membobol dua rekening milik nasabah bank dengan total kerugian mencapai Rp. 60 juta.

Modus yang dilakukan tersangka adalah dengan interset (membobol *user id* nasabah di data bank tersebut) dari data tersebut kemudian di dapat *pasword* nasabah yang umumnya menggunakan tanggal lahir. Pelaku sudah beroperasi sejak Agustus 2009, selain pandai di bidang IT juga mengetahui sistem perbankan atau pernah bekerja di bank.

BAB IV

TINDAK PIDANA PENIPUAN MELALUI INTERNET BERDASARKAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

A. Aspek Hukum dan Modus Operandi Terjadinya Tindak Pidana Penipuan Melalui Internet

Kemajuan di bidang sistem jaringan internet dan telekomunikasi menyebabkan komunikasi secara elektronis dari satu negara ke negara lain makin bertambah cepah dan mudah. Peristiwa-peristiwa yang terjadi di belahan dunia yang jauh dapat diketahui dalam hitungan menit melalui jaringan internet. Dalam bentuk tertentu, kemajuan sistem jaringan internet tersebut dapat berupa transaksi di bidang perbankan melalui teknologi jaringan internet. Transfer uang antara bank yang dikenal pula dengan ”*e-cash*” di dalam negeri maupun ke luar negeri dapat dilakukan dengan lebih cepat lagi.

Perdagangan melalui internet di ”*cyber space*” yang dikenal dengan *e-commerce* semakin meningkat. Iklan-iklan untuk segala macam barang dan piranti lunak (*software*) yang dilaksanakan di ”*cyber space*” sudah merupakan hal lazim yang dengan mudah dapat diamati pembayaran untuk pemesanan barang atau program komputer dapat dilakukan dengan menggunakan ”*credit card*” dalam formulir yang telah disediakan oleh penjual yang secara cepat muncul dalam komputer para pembeli.

Transfer uang secara elektronik yang disebut dengan ”*wire transfer*” merupakan cara umum untuk mentransfer uang dengan pesan elektronik (*electronics messages*) antar bank. Betapa besar uang yang ditransfer setiap harinya melalui jaringan internet dapat dilihat dari fakta kegiatan lembaga-lembaga yang memberikan jasa di bidang ini, misalnya transfer uang antar bank yang dilakukan melalui jaringan komputer sistem *Electronics Funds Transfer system*. Demikian pula halnya, betapa besarnya asset yang perlu dilindungi dapat dilihat dari sarana komputer yang dimiliki oleh suatu negara dan dari jumlah uang yang ditransfer dari sistem elektronis seperti yang dimiliki oleh lembaga *EFTS* dan *SWIFT* tersebut ke berbagai penjuru dunia. Berdasarkan penelitian diperkirakan bahwa uang yang ditransfer secara elektronis setiap hari oleh kedua lembaga tersebut lebih banyak dari anggaran negara Amerika Serikat dan Inggris untuk satu tahun.

Mengetahui bahwa segala sesuatu yang dikirim melalui teknologi transfer elektronik itu sangat berharga, maka berbagai organisasi kejahatan pun berusaha untuk mengintersepsi dan mengalihkan uang itu ke bank mereka. Sebagaimana lazimnya pembaharuan teknologi transfer elektronik, internet selain memberi manfaat juga menimbulkan ekses negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Hal itu terjadi pula untuk data dan informasi yang dikerjakan secara elektronik. Dalam jaringan komputer seperti internet, masalah kriminalitas menjadi semakin kompleks karena ruang lingkupnya yang luas.

Kriminalitas di internet atau *cyber crime* pada dasarnya merupakan suatu tindak pidana yang berkaitan dengan *cyber space*, baik yang menyerang fasilitas umum di dalam *cyber space* ataupun kepemilikan pribadi.

Menurut hemat penulis, secara garis besar kejahatan-kejahatan yang terjadi terhadap suatu sistem atau jaringan komputer dan yang menggunakan komputer sebagai instrumen *delicti*, juga dapat terjadi di dunia perdagangan. Terjadinya *cyber crime* dalam transaksi jual beli dalam internet antara lain dapat terjadi dalam layanan pembayaran menggunakan kartu kredit pada situs-situs toko *online* dan layanan perbankan *online* (*online banking*).

Terjadinya tindak pidana penipuan melalui internet terhadap masyarakat dalam transaksi elektronik merupakan kejahatan yang menyerang kepemilikan pribadi secara gradual, karena apabila kejahatan terhadap data komputer atau ”*digital goods*” yang juga mempunyai nilai tinggi yang disebut ”*digital crimes*” sasarannya masih dalam jumlah yang terbatas, maka kini para pelaku tindak pidana penipuan dalam transaksi jual beli telah mengembangkan dengan dimensi dan sasaran yang lebih luas lagi. Swalayan besar di ”*cyber space*” (disebut juga ”*cybernation*”) kini menjadi sasaran empuk para penjahat internasional yang dengan menggunakan teknologi komputer yang canggih dengan lihai melakukan kejahatan ”*cyber*”. Demikian pula halnya, para masyarakat yang ceroboh akan menjadi sasaran empuk penipuan melalui internet (*internet fraud*).

Sudut pandang para pelaku tindak pidana penipuan melalui internet menjadikan pihak bank, *merchant*, toko *online* atau masyarakat sebagai korban yang dapat terjadi karena maksud jahat seseorang yang memiliki kemampuan dalam bidang teknologi informasi, atau seseorang yang memanfaatkan kelengahan pihak bank, pihak *merchant* maupun pihak masyarakat.

Modus operandi pelaku tindak pidana penipuan melalui internet dalam transaksi jual beli melalui media *online* pada awalnya pelaku tersebut menawarkan barang-barang kepada masyarakat yang ditawarkan melalui photo-photo yang di *up load* ke media sosial *online*, apabila ada seseorang yang tertarik terhadap barang yang di *up load* tersebut maka orang tersebut akan disuruh oleh pelaku untuk mentransfer sejumlah uang ke rekening pelaku, setelah pelaku mendapatkan uang yang ditransfer oleh seseorang yang tertarik pada barang tersebut maka situs *web* akan ditutup oleh pelaku dan barang tidak akan pernah datang ke seseorang tersebut, hal ini berkaitan dengan contoh kasus tindak pidana penipuan dalam transaksi jual beli secara *online* yang dituliskan dalam bab III, di mana Santy Junitha Soekarno tertarik untuk membeli barang-barang dari Nigel Frank dengan maksud akan dijual kembali oleh Santy Junitha Soekarno melalui media sosial *facebook*, namun setelah Santy Junitha Soekarno mentrasfer sejumlah uang Nigel Frank tidak pernah mengirimkan barang-barang pesanan Santy Junitha Soekarno.

Fenomena tindak pidana penipuan melalui internet memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain pada umumnya. Tindak pidana penipuan melalui internet dapat dilakukan tanpa mengenal batas teritorial dan tidak diperlukan interaksi langsung antara pelaku dengan korban kejahatan. Bisa dipastikan dengan sifat global internet, semua negara yang melakukan kegiatan internet hampir pasti akan terkena imbas perkembangan tindak pidana penipuan melalui internet ini.

Kegiatan melalui media sistem elektronik, yang disebut juga *cyber space*, meskipun bersifat virtual dapat dikategorikan sebagai tindakan atau perbuatan hukum yang nyata. Secara yuridis kegiatan pada *cyber space* tidak dapat didekati dengan ukuran dan kualifikasi hukum konvensional saja sebab jika cara ini yang ditempuh akan terlalu banyak kesulitan dan hal yang lolos dari pemberlakuan hukum. Kegiatan dalam *cyber space* adalah kegiatan virtual yang berdampak sangat nyata meskipun alat buktinya bersifat elektronik.

Aspek hukum tindak pidana penipuan melalui internet telah sangat terang dan jelas ditegaskan dalam UU ITE, namun UU ITE tidak akan berfungsi secara optimal sebagai alat untuk menjerat para pelaku tindak pidana penipuan melalui internet apabila tidak didukung oleh profesionalisme para aparat penegak hukum. Dengan demikian, subjek pelakunya harus dikualifikasikan pula sebagai orang yang telah melakukan perbuatan hukum secara nyata. Berkaitan dengan hal itu, perlu

diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar dapat berkembang secara optimal. Oleh karena itu, untuk menjaga keamanan di *cyber space*, pendekatan aspek hukum, aspek teknologi, aspek sosial, budaya, dan etika harus diterapkan secara signifikan. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

B. Upaya Yang Dapat Dilakukan Untuk Mencegah Tindak Pidana Penipuan Melalui Internet

Perkembangan internet di Indonesia mengalami percepatan yang sangat tinggi serta memiliki jumlah pelanggan atau pihak pengguna jaringan internet yang terus meningkat sejak paruh tahun 90-an. Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan melihat banyaknya perusahaan yang menjadi provider untuk pengguna jasa internet di Indonesia. Pembaharuan hukum khususnya hukum di dunia *cyber* merupakan faktor dan tindakan yang dapat digolongkan sebagai tindakan yang berhubungan dengan aplikasi hukum tentang *cyber* di Indonesia. Oleh sebab itu ada baiknya didalam perkembangan selanjutnya agar setiap pemberi jasa atau pengguna internet dapat terjamin maka hukum tentang internet perlu dikembangkan serta dikaji sebagai sebuah hukum yang memiliki displin tersendiri di Indonesia.

Upaya yang dapat dilakukan untuk mencegah tindak pidana penipuan melalui internet menurut hemat penulis dapat dilakukan dengan memberikan perlindungan hukum terhadap pemberi jasa atau pengguna internet, hal ini telah mendorong pemerintah untuk melahirkan suatu produk hukum dalam bentuk UU ITE, namun dengan lahirnya UU ITE belum semua permasalahan menyangkut masalah ITE dapat tertangani. Dengan lahirnya UU ITE tidak semata-mata undang-undang ini bisa diketahui oleh masyarakat pengguna teknologi informasi dan praktisi hukum. Kemudian berbagai bentuk perkembangan teknologi yang menimbulkan penyelenggaraan dan jasa baru harus dapat diidentifikasikan dalam rangka antisipasi terhadap pemecahan berbagai persoalan teknis yang dianggap baru sehingga dapat dijadikan bahan untuk penyusunan berbagai Peraturan Pelaksanaan. Pengayaan akan bidang-bidang hukum yang sifatnya sektoral (rejim hukum baru) akan makin menambah semarak dinamika hukum yang akan menjadi bagian sistem hukum nasional.

Disahkannya sebuah UU ITE bukan berarti undang-undang ini telah menjadi sebuah hukum yang mutlak dan tidak bisa lagi dirubah atau diganti. Sebaliknya justru harus adanya perbaikan dan perubahan dilakukan terhadap UU ITE dan Peraturan Pemerintah sebagai pelengkap karena setelah diterapkan diketahui mempunyai kelemahan, terutama kelemahan tersebut fatal sifatnya. Dalam pelaksanaannya,UU ITE banyak menuai pro dan kontra, bahkan kehadiran UU ITE dituding tidak dapat

menurunkan tingkat kejahatan dunia maya secara signifikan, sehingga memunculkan pertanyaan efektifitas UU ITE itu sendiri terutama dari aspek pidananya.

Perlindungan hukum terhadap pemberi jasa atau pengguna internet mutlak diperlukan, perlindungan tersebut dalam bentuk tertentu harus juga diberikan kepada masyakarat pengguna layanan internet yang sering melakukan transaksi jual beli secara *online*, karena pada akhir-akhir ini penggunaan layanan internet untuk transaksi jual beli semakin digemari dengan alasan bahwa jual beli melalui internet tersebut mempermudah transaksi yang biasa dilakukan di dunia nyata dan dapat mengefisiensikan waktu bagi orang-orang yang sibuk.

Aplikasi yang sangat banyak dipakai dari kegiatan *cyber* adalah transaksi-transaksi elektronik, sehingga transaksi secara *online* saat ini menjadi isu yang paling aktual. Dan, sebenarnya hal ini menjadi persoalan hukum semenjak transaksi elektronik mulai diperkenalkan, di samping persoalan pengamanan dalam sistem informasi itu sendiri. Tanpa pengamanan yang ketat dan canggih, perkembangan teknologi informasi tidak memberikan manfaat yang maksimal kepada masyarakat. Teknologi digital memungkinkan penyalahgunaan informasi secara mudah, sehingga masalah keamanan sistem informasi menjadi sangat penting.

Satu langkah yang dianggap penting untuk menanggulangi keamanan sistem informasi adalah telah diwujudkannya rambu-rambu hukum yang tertuang dalam UU ITE. Hal yang mendasar dari UU ITE ini

sesungguhnya merupakan upaya mengakselerasikan manfaat dan fungsi hukum (peraturan) dalam kerangka kepastian hukum. Penegakan hukum pidana dalam *cyber crime* dapat dilakukan oleh penyidik yang terdiri dari Kepolisian Republik Indonesia dan Penyidik Pegawai Negeri Sipil. Penyidikan dilakukan berdasarkan KUHP dan UU ITE. Kewenangan Penyidik Pegawai Negeri Sipil dalam rangka memberikan perlindungan hukum terhadap masyarakat yang mengalami *cyber crime* dalam internet tercantum dalam UU ITE.

Perlindungan hukum terhadap nasabah bank yang mengalami *cyber crime* dalam internet dihubungkan dengan UU ITE terdapat dalam Pasal 45, Pasal 46, Pasal 47, Pasal 48, Pasal 49, Pasal 50, Pasal 51 UU ITE. Namun menurut hemat penulis, ketentuan-ketentuan yang terdapat di dalam UU ITE masih memerlukan penjabaran yang relevan, misalnya ketentuan yang diatur dalam Bab VII Pasal 27 sampai dengan Pasal 37 UU ITE mengenai perbuatan yang dilarang, semua pasal tersebut menggunakan kalimat setiap orang. Padahal perbuatan yang dilarang, seperti *spam*, penipuan, *cracking*, virus, dan *flooding* sebagian besar akan dilakukan oleh mesin oleh program bukan langsung oleh manusia.

UU ITE dipersepsikan sebagai *cyber law* di Indonesia, yang diharapkan bisa mengatur segala urusan dunia Internet (*cyber*), termasuk di dalamnya memberikan jeratan hukum berupa pidana terhadap para pelaku *cyber crime*. UU ITE menjadi bagian penting dalam sistem hukum positif secara keseluruhan. Adanya bentuk hukum baru sebagai akibat

pengaruh perkembangan teknologi dan globalisasi merupakan pengayaan bidang-bidang hukum yang sifatnya sektoral. Hal ini tentunya akan menjadi suatu dinamika hukum tersendiri yang akan menjadi bagian sistem hukum nasional.

Beberapa permasalahan yang terdapat di UU ITE dalam bentuk tertentu dapat berupa adanya pasal-pasal yang kurang lugas dan perlu didetailkan, serta dalam sosialisasi dan penyebaran UU ITE tersebut perlu ditingkatkan secara terpadu, kemudian juga tentang kesiapan aparat dalam implementasi UU ITE tersebut, aparat penegak hukum yang bergerak dalam bidang informasi teknologi harus secara profesional menjalankan UU ITE agar dapat berjalan secara signifikan memberantas, mencegah atau setidak-tidaknya meminimalisir *cyber crime*, dalam hal ini tindak pidana yang terjadi di bidang internet *banking*.

Menurut hemat penulis UU ITE adalah *cyberlaw*-nya Indonesia, kedudukannya sangat penting untuk mendukung lancarnya kegiatan para pebisnis Internet, melindungi akademisi, masyarakat dan mengangkat citra Indonesia di level internasional. Cakupan UU ITE luas, mungkin perlu peraturan di bawah UU ITE yang mengatur hal-hal lebih mendetail (peraturan menteri, dan sebagainya). UU ITE masih perlu perbaikan, ditingkatkan kelugasannya sehingga tidak ada pasal karet yang bisa dimanfaatkan untuk kegiatan yang tidak produktif. Dengan diundangkannya UU ITE, bukan berarti seluruh permasalahan yang terjadi di bidang telematika sudah selesai, masih banyak persoalan yang harus

juga diantisipasi, terutama atas hasil konvergensi yang pastinya menimbulkan berbagai bentuk layanan virtual baru dan berbagai persoalan teknis yang pastinya terus berkembang.

Perkembangan hukum yang sifatnya sektoral sesungguhnya menjadi suatu bagian yang perlu mendapat perhatian kita semua. Dan, sesungguhnya tidak dapat dihindari bahwa perkembangan hukum yang sektoral telah menjadi kenyataan. Bila kita lihat beberapa produk hukum yang ada saat ini, sifat sektoral tersebut nampak sering terlihat, sifat sektoral tersebut karena pengaturannya yang teknis dan spesifik. Sesuatu yang sektoral umumnya sering berjalan tanpa melihat kepentingan sektor-sektor lain. Untuk mengantisipasi dan menghindari pertentangan yang sifatnya tarik menarik antar sektor, sinkronisasi dan harmonisasi dalam tahapan pra legislasi, mulai dari kajian dan penyusunan naskah akademik untuk menunjang dasar pengajuan legislasi menjadi sesuatu yang penting untuk dilakukan.

Saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum *cyber* atau hukum telematika. Hukum *cyber* 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, hukum dunia maya, dan hukum mayantara. Istilah-istilah tersebut lahir mengingat kegiatan

yang dilakukan melalui jaringan sistem komputer dan sistem komunikasi baik dalam lingkup lokal maupun global (Internet) dengan 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.

Pemahaman terhadap hukum penting dilakukan, khususnya terhadap produk-produk hukum yang sifatnya teknis seperti UU ITE, disamping harus dilakukan diskusi-diskusi ilmiah, juga perlu dilakukan pembudayaan hukum melalui sosialisasi yang intens yang ditujukan terhadap seluruh lapisan masyarakat dan aparat penegak hukum.

Dinamika penegakan UU ITE terhadap *cyber crime* terutama masyarakat yang bertransaksi jual beli melalui internet dalam sistem hukum nasional untuk melaksanakan pembinaan hukum nasional yang ditujukan untuk pembentukan sistem hukum nasional, kajian-kajian terhadap berbagai persoalan yang merupakan bagian dari tugas pembinaan hukum terus diupayakan agar hukum dapat berjalan dengan baik. Dalam konteks UU ITE, kajian-kajian yang menyangkut persoalan teknis terus dilakukan mengingat UU ITE memerlukan beberapa peraturan pelaksanaan yang sifatnya teknis seperti persoalan yang menyangkut sertifikasi keandalan, tanda tangan elektronik, penyelenggaraan sistem

elektronik, penyelenggaraan transaksi elektronik, penyelenggaraan agen elektronik, pengelolaan nama domain, masalah intersepsi, pengelolaan data strategis, dan sebagainya.