PENEGAKAN HUKUM TERHADAP KASUS *INTERNET FRAUD* DENGAN KORBAN BERDOMISILI DI LUAR NEGERI

TESIS

EKA SYARIF NUGRAHA HUSEN
0806447311

UNIVERSITAS INDONESIA
FAKULTAS PASCA SARJANA
PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
JAKARTA
JUNI 2010

PENEGAKAN HUKUM TERHADAP KASUS *INTERNET FRAUD* DENGAN KORBAN BERDOMISILI DI LUAR NEGERI

TESIS
Diajukan sebagai salah satu syarat untuk memperoleh gelar
Magister Ilmu Kepolisian

EKA SYARIF NUGRAHA HUSEN
0806447311

UNIVERSITAS INDONESIA
FAKULTAS PASCA SARJANA
PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
JAKARTA
JUNI 2010

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar

Nama	: Eka Syarif Nugraha Husen
NPM	: 0806447311
Tanda Tangan	:
Tanggal	: 7 Juni 2010

HALAMAN PENGESAHAN

Tesis ini diajukan oleh

Nama	:	Eka Syarif Nugraha Husen
NPM	:	0806447311
Program Studi	:	Kajian Ilmu Kepolisian
Judul Tesis	:	Penegakan Hukum Terhadap Kasus *Internet Fraud* Dengan Korban Berdomisili di Luar Negeri

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan pada yang diperlukan untuk memperoleh gelar Magister Sains pada Program Studi Kajian Ilmu Kepolisian, Program Pascasarjana, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing	: Prof. Mardjono Reksodiputro, SH, MA	( )
Penguji 1	: Dr Petrus Reinhard Golose, MM	( )
Penguji 2	: Drs. Ahwil Lutan, SH, MBA, MM	( )
Penguji 3	: Prof. Indriyanto Seno Adjie, SH.MH	( )

Ditetapkan di : Jakarta

Tanggal : 7 Juni 2010

KATA PENGANTAR

Alhamduillahirabbil 'alamin. Tidak ada ekspresi yang lebih tepat untuk mensyukuri kondisi yang saya rasakan saat ini. Semua tekanan yang dialami selama ini telah berlalu hanya berkat kuasa Allah SWT. Terima kasih juga saya ucapkan kepada keluarga besar saya yang telah mendukung saya selama ini, khususnya untuk istri saya, Ummi-Umar, serta anak-anak saya Abang umar dan "si Adik" yang selalu menjadi inspirasi saya untuk menyelesaikan studi saya tepat waktu.

Saya memulai studi magister ini dengan niat untuk meningkatkan kemampuan saya sebagai seorang abdi negara yang akan mengarungi masa depan yang penuh tantangan. Pada perkembangan berikutnya, setelah saya menyelesaikan masa studi ini, saya sampai pada kesimpulan: masih banyak yang harus saya pelajari supaya mampu mengimbangi dinamika masyarakat yang kita layani. Oleh karena itu, saya berdoa, memohon kepada Allah SWT, agar selalu dalam lindungan dan arahannya dalam mengembangkan dan mengaktualisasikan diri melalui bakti saya kepada masyarakat.

Dalam kesempatan ini saya juga hendak mengucapkan penghargaan kepada Bapak, Ibu serta rekan-rekan yang telah berjasa mendukung saya selama pelaksanaan tugas akhir di program Kajian Ilmu Kepolisian ini, yaitu

1. Profesor H. Mardjono Reksodiputro, SH, MA yang di tengah kesibukannya menyediakan waktu untuk menjadi pembimbing
2. Kombes Pol Dr Petrus R. Golose, MM selaku nara sumber dan penguji.
3. Profesor Dr Indriyanto Seno Adji, .H, MH, yang telah memberi masukan yang berharga untuk tesis ini
4. Komjen Pol (P) Drs Ahwil Luthan, S.H, MBA, MM selaku penguji
5. Kompol I Ketut Budi Hendrawan, yang telah dengan sabar menyediakan waktu untuk menjadi nara sumber utama bagi saya sebagai juniornya

6. Kompol Alexander Sabar, AKBP Parmin, AKBP Faisal Thayeb, Bapak Raharjo Budi Kisnanto, Bapak Faisal Adi dan Bapak Ismail SH sebagai narasumber tesis ini.
7. Kombes Pol Dr Benny Mamoto yang telah menyarankan saya untuk mengangkat tema *cyber crime*
8. Rekan-rekan mahasiswa KIK angkatan XIII yang selalu saling menyemangati satu sama lain selama masa perkuliahan. Semoga persaudaraan kita kekal dan bersama-sama kita memberi bakti terbaik untuk nusa dan bansa
9. Rekan-rekan Angkatan Endra Dharmalaksana yang dengan caranya masing-masing telah memberi dukungan kepada saya untuk meyelesaikan studi saya di program KIK UI ini.

Pada akhirnya, semoga Allah SWT menghitung tulisan ini sebagai amal baik saya, khususnya dalam mencegah keumungkaran

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Nama : Eka Syarif Nugraha Husen
Program Studi : Kajian Ilmu Kepolisian
Judul : Penegakan Hukum Terhadap Kasus *Internet Fraud* Dengan Korban Berdomisili di Luar Negeri

Tesis ini membahas proses penegakan hukum terhadap kasus *internet fraud* dengan korban berdomisili di luar negeri beserta kendala-kendala dan tantangan yang dihadapi oleh para penegak hukum. Penelitian ini menggunakan metode penelitian hukum normatif dengan pengumpulan data dilakukan melalui wawancara, observasi dan studi dokumen. Penelitian ini menghasilkan temuan bahwa a) pasal 378 KUHP dapat diterapkan terhadap kasus *internet fraud*, b) adanya kesulitan penerapan Undang-Undang Informasi dan Transaksi Elektronik, c) penentuan yurisdiksi yang berdasarkan prinsip teritorialitas serta d) kesulitan penegakan hukum yang berhubungan dengan pelaporan. Oleh karena itu, penulis menyarankan amandemen terhadap Undang-Undang Informasi dan Teknologi Informasi serta prosedur pelaporan dalam KUHAP.

Kata Kunci : penegakan hukum, *internet fraud*, yurisdiksi

ABSTRACT

Name : Eka Syarif Nugraha Husen
Study Program : Graduate Program Police Studies
Title : Law Enforcement on Internet Fraud Case with Victim Resides outside Indonesia

This thesis discusses the law enforcement on internet fraud case with victim resides outside Indonesia as well as its obstacles and its challenge. This research is a normative law research while data are collected through documentary study, interview and observation. It is revealed that a) utilization of article 378 of penal code is applicable on internet fraud cases, b) the existence of obstacle on enforcing Information and Electronic Transaction Law c) jurisdiction is determined primarily based on territoriality principle and, d) the existence of obstacle derived from the complaint procedure. In this regard, it is suggested to amend Information and Electronic Transaction Law as well as the penal procedure particularly in complaint making procedure.

Keywords : law enforcement, internet fraud, jurisdiction

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Selama dua dekade terakhir ini, dunia mengalami perubahan yang begitu signifikan sebagai akibat penggunaan teknologi informasi dalam kehidupan sehari-hari. Dengan kemudahan konektivitas yang diberikan, kita tidak hanya dapat berbincang-bincang dengan rekan sejawat atau keluarga di bagian manapun di dunia, kita juga dapat melakukan suatu transaksi yang bernilai trilyunan rupiah secara cepat dan mudah dengan orang lain yang berada sangat jauh dari tempat kita berada. Teknologi informasi juga memberikan ruang bagi seseorang untuk mengekspresikan pendapatnya ketika akses terhadap media konvensional sangat terbatas..

Efisiensi ini telah mengubah gaya hidup masyarakat untuk meninggalkan bentuk-bentuk transaksi fisik dan menggantinya dengan transaksi elektronik yang tidak hanya murah dan cepat, tetapi juga memberikan kesempatan bagi setiap orang untuk dapat melakukan transaksi bisnis dan bersantai secara bersamaan. Salah satu indikatornya adalah omset penjualan barang melalui situs internet yang terus meningkat. Pada tahun 2007, omset penjualan barang melalui situs internet di Amerika telah mencapai US$ 175 milyar dan diproyeksikan akan mencapai US$ 335 milyar pada tahun 2012 (Halstead 2008, 1-2). Angka transaksi berbasis internet ini akan semakin besar jika kita menambahkannya dengannya dengan jumlah transaksi *online banking* dan transaksi keuangan lainnya.

Penggunaan internet yang begitu intens dalam kehidupan sehai-hari bahkan telah menyebabkan timbulnya dunia baru yang disebut *second life*. Disebut dunia karena meskipun *second life* sebenarnya sebuah permainan virtual yang diciptakan Linden Research tahun 2003, ia amat berbeda dengan *game* biasa karena tidak memiliki misi, perolehan nilai, serta akhir permainan. Dalam *second life*, pengguna

internet dapat menjadi penghuni dan memiliki tanah serta rumah virtual, baik secara berbayar maupun gratis. Para penghuni juga bisa saling berinteraksi melalui avatar mereka, karakter tiga dimensi yang merupakan *alter ego* masing-masing penghuni. Tidak hanya sekadar berinteraksi, penghuni *second life* juga bisa bekerja, berbisnis, bermain atau berolahraga bersama, bahkan jatuh cinta, menikah dan selingkuh.[1]

Contoh bisnis dalam *second life* adalah jual beli pakaian, rumah atau kelengkapan lainnya. Transaksi dilakukan dengan menggunakan mata uang khusus yang berlaku di *second life* tetapi dapat digunakan di dunia nyata dengan menukarnya di bank yang ada dalam *second life*. Hal itu dimungkinkan karena setiap pengunjung mempunyai akun yang bisa menyertakan nomor rekening atau kartu kredit.

Saat ini penghuni *second life* terus bertambah. Tidak hanya perorangan, banyak perusahaan besar yang ikut menjadi penghuninya, misalnya Reebok, Adidas, IBM, General Motors, hingga Coca-Cola. Ada juga beberapa media seperti Reuters, BBC, atau The New York Times. Bank serta anjungan tunai mandiri pula tersebar di beberapa wilayah kehidupan kedua. Bahkan Kerajaaan Swedia membuka perwakilannya di dunia kedua ini. Perusahaan-perusahaan sungguhan tadi menjadi anggota premium dan membeli tanah di dunia maya. Di sana, perusahaan bisa melakukan rapat dengan cabangnya di belahan dunia lain. Hal itu tentunya dapat menghemat biaya perjalanan sekaligus menjadi ajang promosi perusahaan-perusahaan itu.

Sayangnya, kemajuan teknologi ini harus diiringi dampak negatif. Teknologi informasi telah memberikan asistensi kepada para pelaku kejahatan untuk melakukan kegiatan ilegalnya. Para pelaku kejahatan juga memperoleh cara dan media baru

---

[1] Salah seorang penghuni yang menikah dalam *second life* adalah Vancy Bailey. Wanita keturunan Indonesia berkewarganegaraan Belanda ini menikah dengan pria Perancis yang belum pernah ditemuinya dalam dunia nyata. Meskipun demikian, interaksi mereka berlangsung setiap hari melalui avatar-avatar mereka. Ikatan batin yang terjalin melalui karakter tiga dimensi itu meyakinkan mereka untuk menikah.

Pada Konferensi Tingkat Tinggi PBB untuk Perubahan Iklim di Nusa Dua, Bali, Edward Markey sebagai salah satu anggota kongres Amerika Serikat yang berhalangan datang menggunakan jasa Second Life untuk menyampaikan pidatonya. Avatar yang ia gunakan menggunakan jas biru tua, dasi hijau, dan kemeja putih dan berdiri dengan latar belakang konferensi di Bali . Ia berkata bahwa ia telah menggunakan teleporter untuk berada di Bali

dalam memperdaya korbannya. Seiring kemajuan teknologi informasi, semakin meningkat pula kualitas dan kuantitas kejahatan berbasis teknologi informasi yang kita kenal sebagai *cybercrime* ini.

Saat ini kita mungkin sudah merasa akrab dengan istilah "*spam*", "*virus*", "*worms*" atau "*hack*". Meskipun motifnya beragam, baik untuk memperoleh keuntungan materi maupun hanya untuk kepuasan diri semata, problema-problema itu baru timbul seiring dengan adanya teknologi informasi. Tidak hanya sebatas itu, teknologi informasi memindahkan bentuk-bentuk kejahatan konvensional dari suatu ruang umum terbuka ke dunia siber. Jika dahulu teroris menakuti targetnya melalui ancaman secara fisik, saat ini mereka mampu meneror targetnya melalui internet. Masih segar dalam ingatan kita, jaringan internet Estonia dilumpuhkan tahun 2007 yang berakibat timbulnya kepanikan di seluruh penjuru negeri.

Pornografi juga mendapatkan media baru. Pada masa lampau, pornografi disajikan melalui media cetak atau media elektronik yang sifatnya terbatas. Sekarang, pornografi dapat diakses kapan saja asalkan tersambung dengan jaringan internet.

Para penipu juga ikut mendapatkan keuntungan dengan kemajuan teknologi. Mereka memperoleh cara baru dalam memikat calon korbannya. Dengan mengeskploitasi kemudahan bertransaksi melalui internet, mereka mengeruk keuntungan secara ilegal dari korbannya itu. Para korban penipuan internet atau *internet fraud* itu baru sadar mereka telah mengalami viktimisasi ketika apa yang seharusnya menjadi hak mereka setelah transaksi, tidak mereka peroleh sesuai perjanjian atau isi rekening mereka berkurang atau berpindah ke tempat lain tanpa persetujuan sebelumnya.

Semakin lama, *cybercrime* berkembang menjadi ancaman yang makin serius. Penyebabnya, gaya hidup serba *online* yang menyebabkan potensi setiap orang ataupun entitas hukum untuk menjadi korban menjadi semakin besar (Wagner 2009, 15). Terlebih lagi, dengan sifatnya yang mampu melintasi batas negara, penanganan tindak pidana ini akan mengalami berbagai kendala yang berhubungan dengan yurisdiksi serta legislasi. Oleh karena itu ASEAN, ICPO-Interpol dan PBB

mengklasifikasikannya sebagai kejahatan transnasional yang hanya dapat diatasi dengan adanya kesungguhan negara dalam memeranginya disertai kerjasama internasional yang baik.

Fenomena peningkatan kejahatan *cyber crime* juga terjadi di Indonesia. Khusus dalam masalah *internet fraud*, Indonesia bahkan dianggap seakan-akan sebagai surga bagi para pelaku kejahatan ini. Selama beberapa tahun terakhir, Indonesia selalu berada pada posisi negara yang wajib diwaspadai jika akan melakukan transaksi secara elektronik. Beberapa korban *fraud* bahkan memberikan peringatan agar berhati-hati untuk bertransaksi dengan seluruh usahawan Indonesia disebabkan oleh lemahnya penegakan hukum di Indonesia.

Salah satu indikator maraknya *internet fraud* yang dilakukan oleh warga negara Indonesia terhadap warga negara asing adalah data komplain yang dimiliki oleh Unit V/ IT dan Cybercrime Dit II Eksus Bareskrim Polri dari tahun 2006 hingga tahun 2009. Data komplain ini dihimpun dari berbagai komplain yang diterima melaui saluran ICPO-Interpol, saluran diplomatik, maupun komplain korban secara langsung kepada petugas Unit V/ IT dan Cybercrime Dit II Eksus Bareskrim Polri . Secara ringkas data itu disajikan sebagai berikut:

TAHUN	JUMLAH KOMPLAIN	JUMLAH KERUGIAN
2006	4	US$ 13,090
2007	11	US$ 55,451.50
2008	63	US$ 607,508.59
2009	100	US$ 1,752,224.85

Tabel 1. Data Komplain *Internet Fraud* Dengan Korban Berdomisili di Luar Negeri Yang Diterima Oleh Unit V/ IT dan Cybercrime Dit II Eksus Bareskrim Polri Tahun 2006-2009

Meskipun tidak dapat memberikan angka yang tepat mengenai jumlah *fraud* yang sesungguhnya, data di atas dapat memberikan gambaran mengenai adanya trend perkembangan kasus *internet fraud* dengan korban berdomisili di luar negeri. Hal itu terlihat dengan adanya peningkatan jumlah komplain yang disampaikan beserta

kerugian yang diderita korban. Gambaran ini selayaknya dapat kita jadikan peringatan untuk segera meningkatkan intensitas penegakan hukum terhadap para pelaku *fraud*.

Atas dasar pertimbangan di atas, saya menarik simpulan pentingnya diadakan sebuah penelitian tentang penegakan hukum terhadap kasus *internet fraud* yang melibatkan korban berdomisili di luar negeri.

1.2. Rumusan Permasalahan

Penegakan hukum pada dasarnya merupakan bentuk pelayanan kepada masyarakat untuk meningkatkan produktivitasnya. Selain itu dengan penegakan hukum, diharapkan korban yang telah dirugikan, dapat dipulihkan hak-haknya. Namun, penegakan hukum terhadap kejahatan *internet fraud* tidaklah sederhana.

Dengan karakteristiknya sebagai kejahatan yang mampu melintas batas negara, penyidik tentu akan mengalami kesulitan dalam menentukan yurisdiksi kasus-kasus *internet fraud* (Yar 2006, 91). Ketika pelaku, korban dan tempat kejadian perkara di Indonesia tentu dengan mudah ditentukan, yurisdiksinya sesuai hukum Indonesia. Namun, ketika si korban warganegara Israel yang berdomisili di Mexico menjadi korban dari pelaku berkewarganegara Indonesia yang bertempat tinggal sehari-hari di Bangkok, yurisdiksi mana yang akan digunakan?

Kesulitan selanjutnya, erat kaitannya dengan sifat anonim dari *cyber crime*. Pelaku tentu tidak akan menggunakan identitas asli dalam melakukan kejahatannya. Identitas fiktif ini mereka gunakan berkaitan dengan nama, alamat, serta nomor rekening yang akan digunakan untuk menampung uang yang dikirimkan oleh korban.

Saat ini Indonesia memang telah memiliki undang-undang yang mengatur tentang informasi dan transaksi elektronik yang memiliki aturan pidana terhadap kejahatan *internet fraud*. Tetapi apakah pelaksanan undang-undang ini berjalan lancar? Lalu bagaimana dengan kejahatan *internet fraud* yang dilakukan sebelum Undang-Undang Informasi dan Transaksi Elektronik (Undang-Undang ITE)? Apakah

penegakan hukum tidak dilakukan terhadap perbuatan kriminal itu? Apa yang harus dilakukan oleh para penegak hukum dalam rangka mengatasi kekosongan hukum itu?

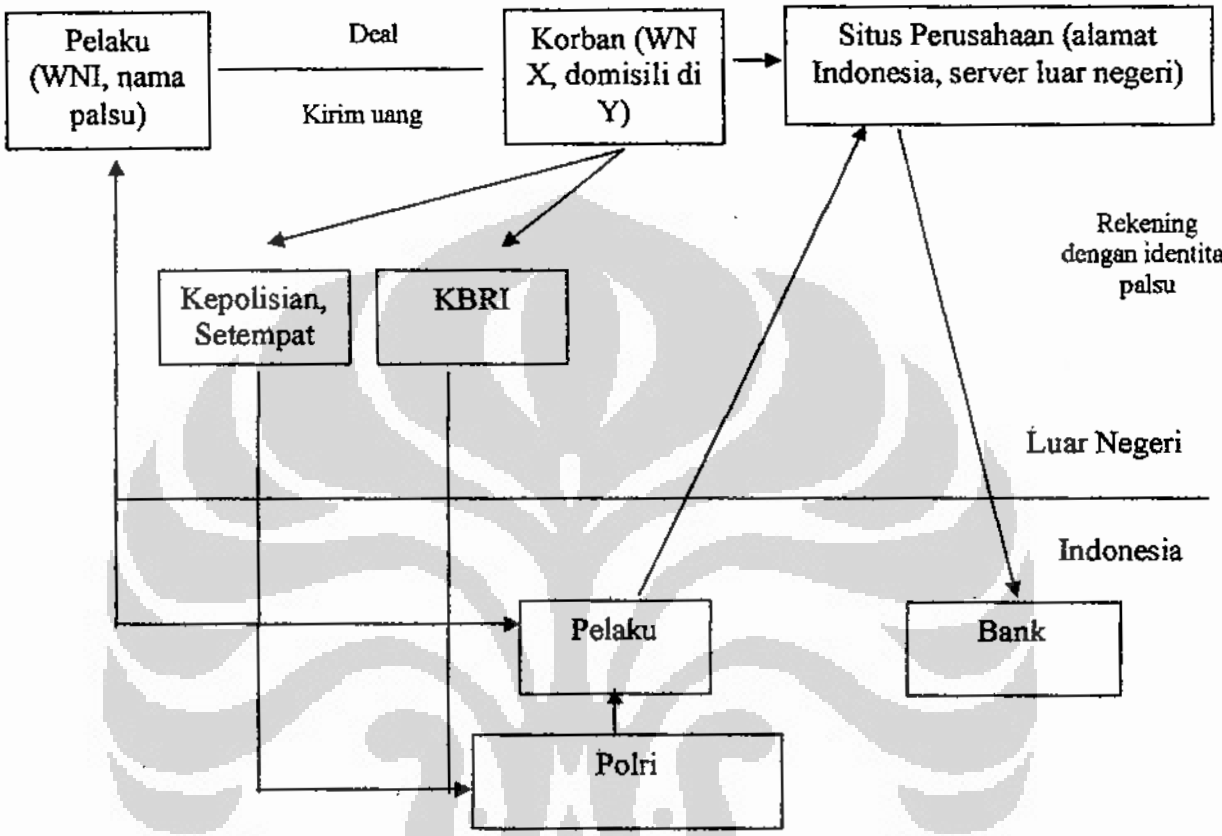
Kesulitan-kesulitan yang dialami petugas dalam menegakkan hukum tentu memberi peluang suburnya tindak kejahatan *internet fraud* di Indonesia. Tingginya angka kejahatan *internet fraud* yang dilakukan di Indonesia dapat menyebabkan hilangnya kepercayaan negara-negara lain terhadap dunia usaha Indonesia yang menggunakan asistensi teknologi informasi. Selain itu, penanganan yang tidak optimal terhadap kasus-kasus itu dapat menimbulkan opini negara lain bahwa Indonesia tidak bersungguh-sungguh menangani kasus yang menimpa warganegaranya. Bukan tidak mungkin pula, warganegara Indonesia tidak ditanggapi dengan baik oleh negara lain ketika mengalami kasus yang serupa. Pada akhirnya, keadaan ini, secara ekstrem, akan membunuh produktivitas bangsa.

Adapun permasalahan utama tesis ini adalah penegakan hukum dalam kasus *intenet fraud* di Indonesia. Permasalahan utama ini difokuskan kepada pertanyaan penelitian (*research questions*) sebagai berikut:

(1) Dapatkah pasal (-pasal) KUHP dipergunakan sekiranya belum ada undang-undang yang secara khusus mengenai kejahatan *cyber crime*

(2) Bagaimana menangani masalah yurisdiksi dalam kasus *internet fraud*?

(3) Apa saja kesulitan yang ditemui dalam menyidik kasus *internet fraud* ?



Gambar 1. Alur Kejahatan *internet fraud* dengan Korban Berdomisili di Luar Negeri

1.3. Tujuan dan Kegunaan Penelitian

Melalui penelitian ini, saya bertujuan untuk menggambarkan proses penegakan hukum terhadap kasus *internet fraud* dengan korban berdomisili di luar negeri beserta kendala-kendala dan tantangan yang dihadapi oleh para penegak hukum. Selain itu, saya juga ingin memberikan suatu pemikiran akademis dalam rangka praktik penegakan hukum terhadap kejahatan *cyber crime* di Indonesia.

Saya berharap penelitian ini bermanfaat, baik secara teoritis maupun praktis. Manfaat teoritis yang hendak saya capai adalah pengembangan konsep-konsep yang akan memperluas cakrawala ilmu pengetahuan, khusunya ilmu kepolisian di

Indonesia. Sementara itu, manfaat praktis yang hendak saya capai adalah tersedianya rujukan bagi para penegak hukum dalam menangani kasus *internet fraud* yang melibatkan korban yang berdomisili di luar negeri.

1.4 Kepustakaan Penelitian

Beberapa penelitian terdahulu telah menghasilkan berbagai temuan dalam penanganan *cyber crime*. Salah satu dari penelitian itu dilakukan oleh Dicky Patrianegara, seorang penyidik Unit V/ IT & Cyber Crime Dit II Bareskrim Polri dalam tesisnya mengenai upaya organisasi Polri dalam menangani kejahatan *cyber crime* pada tahun 2005. Menurutnya, *cyber crime* merupakan kejahatan yang memiliki karakter kompleks yang mengikuti fenomena gunung es (2006, 11). Temuan ini juga ditemukan adalam penelitian Anisah Hikmiyati, mahasiswa pasca sarjana UI yang sehari-hari berprofesi sebagai seorang jaksa (2006, 182).

Ada beberapa masalah yang harus dihadapi dalam penegakan hukum terhadap kejahatan *cyber crime*. Kendala yang pertama adalah kemampuan penegak hukum. Penelitian Dicky Patrianegara yang dilakukan di unit yang secara khusus menangani kejahatan *cyber crime* menunjukkan kemampuan para penyidik bervariasi. Hasil penelitian ini menguatkan temuan hasil penelitian Andi M.Dicky, mahasiswa PTIK angkatan XL khusus, pada unit yang sama yang menyatakan bahwa pekerjaan menangani *cyber crime* masih dianggap oleh sebagian penyidik sebagai pekerjaan yang rumit (2004, 112). Hal serupa juga ditemukan pada penelitian Hafid Ginanjar Nugroho, mahasiswa Universitas Negeri Sebelas Maret Surakarta (2006) pada aparat penegak hukum di wilayah pengadilan Sleman. Temuannya menunjukkan masih sedikit aparat penegak hukum di wilayah penelitiannya yang memahami teknologi informasi.

Patrianegara juga menemukan kendala yang berhubungan dengan saksi. Rumusan saksi dalam KUHAP yang mengharuskannya mengalami, melihat atau

mendengar sendiri menimbulkan mutlaknya keberadaan korban yang bersaksi untuk dimulainya penegakan hukum (2005).

Sementara itu, Hikmiyati yang memfokuskan penelitiannya pada *locus delicti*, menemukan bahwa dalam penentuannya dapat menggunakan teori-teori yang dianut oleh ajaran hukum pidana nasional (2006, 184). Teori-teori itu adalah ajaran tindakan badaniah, ajaran tepat bekerjanya alat, ajaran akibat dari tindakan serta ajaran berbagai tindak pidana. Nugroho yang juga memfokuskan penelitiannya pada penentuan *locus delicti* kejahatan *cyber crime* menemukan bahwa penentuan *locus delicti* dalam penanganan kasus *cyber crime* yang berhasil dituntaskan proses hukumnya oleh aparat diwilayah hukum Pengadilan Negeri Sleman didasarkan pada tempat akses (2006). Temuan ini menunjukkan jika para aparat penegak hukum di Sleman, pada dasarnya telah mengikuti ajaran tindakan badaniah.

Ajaran tindakan badaniah ini juga ditemukan penggunaannya dalam penelitian Andi M. Dicky yang berfokus pada pelayanan terhadap korban *carding* yang berdomisili di luar negeri. Ada beberapa saran yang ia ajukan sebagai hasil dari penelitiannya, antara lain inovasi dengan pemanfaatan laporan polisi secara online serta pemeriksaan saksi yang dilakukan oleh *liasion officer* Polri yang ditempatkan pada kedutaan-kedutaan besar Republik Indonesia tertentu. (2004, 112). Ia juga menyarankan agar kerjasama antar institusi pemerintah yang menangani *cyber crime* dengan korban warga negara asing ditingkatkan (2004, 116). Termasuk di dalamnya, kerjasama antar instansi penegak hukum yang terkadang tidak memiliki kesamaan persepsi dalam penanganan kasus *cyber crime.*

1.5 Kepustakaan Konseptual

Dalam penelitian ini, konsep-konsep yang dijadikan kerangka teori adalah: penegakan hukum, penemuan hukum, konsep *locus delicti* dan yurisdiksi serta konsep *cyber crime* dan *internet fraud*

1.5.1 Penegakan Hukum

Satjipto Rahardjo mendefinisikan penegakan hukum sebagai tahap pelaksanaan hukum secara konkret dalam kehidupan sehari-hari dari sebuah perjalanan panjang mengatur masyarakat (2006,181). Hal ini erat kaitannya dengan fungsi hukum itu sendiri unuk menyeimbangkan ketegangan antara ideal dan kenyataan (Rahardjo 2006, 17) serta sebagai alat rekayasa sosial.

Senada dengannya, Mertokusumo mendefinisikan penegakan hukum sebagai upaya untuk menjadikan hukum sebagai kenyataan. Pelaksanaan hukum dapat berlangsung secara normal dan damai, tetapi juga dapat terjadi juga pelanggaran terhadapnya. Dalam hal ini pelanggaran harus ditegakkan (2002, 145). Dalam penegakannya ada tiga unsur yang selalu harus diperhatikan, yaitu kepastian hukum (*rechtssircheit),* kemanfaatan (*zwekmssigkeit*), dan keadilan (*gerechttikeit*) (2002, 145).

Menurut Soerjono Soekanto, inti dan arti penegakan hukum terletak pada kegiatan menyerasikan hubungan nilai-nilai yang terjabarkan di dalam kaidah-kaidah yang mantap dan mengejawantah dan sikap tindak sebagai rangkaian penjabaran nilai tahap akhir, untuk menciptakan, memelihara, dan mempertahankan kedamaian pergaulan hidup.(2010, 5). Masalah pokok penegakan hukum sebenarnya terletak pada faktor-faktor penegakan hukum. Faktor-faktor itu mempunyai arti yang netral, sehingga dampak positif atau negatifnya terletak pada apa yang ada di dalamnya. Faktor-faktor itu adalah (Soekanto 2010, 8)

a. faktor hukumnya sendiri,
b. faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum,
c. faktor sarana atau fasilitas yang mendukung penegakan hukum,
d. faktor masyarakat, yakni lingkungan dimana hukum itu diterapkan,
e. faktor kebudayaan, yakni sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup.

1.5.2 Penemuan Hukum

Penemuan hukum diartikan oleh Van Eikema Hommes sebagai proses pembentukan hukum oleh hakim atau petugas-petugas hukum lainnya yang diberi tugas melaksanakan hukum terhadap peristiwa-peristiwa konkret. Ini merupakan proses konkretisasi dan individualisasi peraturan hukum yang bersifat umum dengan mengingat peristiwa konkret (Muchsin 2006, 104). Sementara itu, Paul Scolten menyatakannya sebagai sesuatu yang lain daripada hanya penerapan peraturan-peraturan pada peristiwanya. Kadang-kadang, bahkan sangat sering terjadi bahwa peraturannya harus diterjemahkan baik dengan jalan interpretasi maupun dengan jalan analogi maupun *rechtsverijning* (Muchsin 2006, 104).

Awal kelahiran konsep ini, tidak hanya disebabkan oleh kelemahan undang-undang, tetapi juga dikarenakan adanya asas *ius curia novit*, yaitu hakim dianggap mengetahui hukum. Konsekwensi asas ini hakim tidak boleh menolak suatu perkara yang diajukan kepadanya dengan alasan tidak ada aturannya (Muchsin 2006, 104). Asas hukum ini dijabarkan dalam pasal 27 Undang-Undang Nomor 14 tahun 1970 yang digantikan dengan Pasal 16 (1) Undang-Undang Nomor 4 Tahun 2004 tentang Kekuasaan Kehakiman yang berbunyi "Pengadilan tidak boleh menolak untuk memeriksa, mengadili, dan memutus suatu perkara yang diajukan dengan dalih bahwa hukum tidak ada atau kurang jelas,melainkan wajib untuk memeriksa dan mengadilinya". Dengan demikian, suatu perkara tidak jelas aturannya, hakim tetap wajib memeriksa dan memutuskan perkara dengan menemukan hukumnya.

Carl Von Savigny memberi batasan tentang penafsiran yaitu rekontruksi pikiran yang tersimpul dalam undang-undang. Ini bukan metode penafsiran yang dapat dipergunakan semaunya tetapi pelbagai kegiatan yang semuanya harus dilaksanakan bersamaan untuk mencapai tujuan yaitu penafsiran undang-undang. Menurut Von Savigny, dalam penafsiran undang-undang itu, tidak ada metode umum. Semuanya bergantung peristiwa konkret yang dihadapi. Mayor Polak mengemukakan bahwa cara penafsiran ditentukan oleh :

a. Materi peraturan perundang-undangan yang bersangkutan misalnya: perundang-undangan jual beli.
b. Tempat dimana perkara tersebut timbul yaitu memperhatikan kebiasaan setempat.
c. Waktu yaitu berlaku tidaknya peraturan hukum itu.

Beberapa metode penafsiran antara lain (Muchsin 2006, 121)

a. Metode interpretasi menurut bahasa (gramatikal) yaitu suatu cara penafsiran undang-undang menurut arti kata-kata (istilah) yang terdapat pada undang-undang. Hukum wajib menilai arti kata yang lazim dipakai dalam bahasa sehari-hari yang umum.
b. Metode interprestasi secara historis yaitu menafsirkan undang-undang dengan cara melihat sejarah terjadinya suatu undang-undang.
c. Metode interpretasi secara sistematis yaitu penafsiran yang menghubungkan pasal yang satu dengan pasal yang lain dalam suatu perundang-undangan yang bersangkutan, atau dengan undang-undang lain, serta membaca penjelasan undang-undang tersebut sehingga kita memahami maksudnya.
d. Metode interpretasi secara teleologis sosiologis yaitu makna undang-undang itu ditetapkan berdasarkan tujuan kemasyarakatan artinya peraturan perundang-undangan disesuaikan dengan hubungan dan situasi sosial yang baru.
e. Metode interpretasi komparatif, dengan memperbandingkan, hendak dicari kejelasan mengenai suatu ketentuan undang-undang.
f. Metode intrepretasi anstisipatif, pemecahan dicari dalam peraturan-peraturan yang belum mempunyai kekuatan berlaku yaitu dalam rancangan undang-undang
g. Metode interpretasi secara ekstensif yaitu penafsiran dengan cara memperluas arti kata-kata yang terdapat dalam undang-undang sehingga suatu peristiwa dapat dimasukkan ke dalamnya.

h. Metode interpretasi restriktif yaitu penafsiran yang membatasi/mempersempit maksud suatu pasal dalam undang-undang

1.5.3 Locus Delicti

Locus delicti adalah tempat dilakukannya suatu pidana (Lamintang 1997, 230). Pada dasarnya ada empat macam ajaran atau pendapat dalam pengetahuan hukum pidana, yaitu (Lamintang 1997, 230-232):

a. *de leer van de lichamlijke daad* atau ajaran mengenai tindakan secara pribadi atau ajaran tindakan badaniah atau ajaran perbuatan, dimana *locus delicti* adalah tempat dimana seorang pelaku telah melakukan sendiri perbuatannya yang terlarang atau tempat di mana disyaratkan bahwa pelaku itu melakukan perbuatannya secara pribadi;
b. *de leer van heet instrument* atau ajaran mengenai alat, dimana *locus delicti* adalah terutama tempat seorang pelaku itu telah melakukan sendiri perbuatannya yang terlarang oleh undang-undang, akan tetapi apabila untuk melakukan perbuatannya itu si pelaku telah menggunakan sebuah alat, maka tempat di mana alat itu bekerja harus juga dipandang sebagai tempat dilakukannya tindak pidana yang bersangkutan;
c. *de leer van het gevolg* atau ajaran tentang akibat, dimana locus delicti adalah tempat dimana suatu tindak pidana itu telah menimbulkan akibat, baik itu merupakan suatu akibat yang telah ditimbulkan secara langsung oleh sesuatu tindak pidana maupun suatu akibat yang timbulnya itu merupakan syarat untuk selesainya suatu tindak pidana;
d. *de leer van de meervoudige plaats* atau ajaran gabungan tindak pidana, dimana locus delicti adalah semua tempat, baik tempat dimana seorang pelaku telah melakukan sendiri perbuatannya yang dilarang undang-undang maupun tempat dimana alat yang dipergunakannya itu telah menimbulkan akibat, yaitu apabila tindak pidana yang telah dilakukannya itu meliputi beberapa peristiwa yang telah terjadi di beberapa tempat.

Menurut Profesor van Bemellen, kepastian mengenai tempat dilakukannya suatu tindak pidana penting karena (Lamintang 1997, 228):

a. berkenaan dengan kewenangan relatif dari pengadilan, yaitu tentang pengadilan negeri mana yang paling berhak untuk mengadili sesuatu tindak pidana sperti yang dimaksud dalam pasal 84 dari Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana;
b. berkenaan dengan ruang lingkup berlakunya undang-undang pidana Indonesia seperti termaksud dalam pasal 2-9 KUHP;
c. berkenaan dengan pengecualian seperti yang termaksud dalam pasal 9 KUHP yaitu apabila tindak pidana yang bersangkutan telah dilakukan di atas sebuah kapal perang negara asing;
d. berkenaan dengan adanya suatu syarat bahwa sesuatu tindak pidana harus dilakukan di sebuah tempat terlarang;
e. berkenaan dengan adanya suatu syarat bahwa sesuatu tindak pidana itu harus dilakukan di "tempat umum" seperti yang termaksud dalam pasal 160 KUHP;
f. berkenaan dengan adanya suatu syarat bahwa sesuatu tindak pidana itu harus dilakukan di suatu tempat tertentu dimana seorang pegawai negeri sedang menjalankan tugas jabatannya yang sah seperti yang antara lain dimaksud dalam pasal 127 KUHP.

1.5.4 Yurisdiksi

Shaw mendifinisikan Yurisdiksi sebagai kekuasaan atau kompetensi hukum negara terhadap orang, benda, atau peristiwa hukum. Yurisdiksi merupakan refleksi dari prinsip dasar kedaulatan negara, kesamaan derajat negara dan prinsip tidak campur tangan. Yurisdiksi juga merupakan bentuk kedaulatan vital dan sentral yang dimiliki oleh suatu negara untuk mengubah, menciptakan atau mengakhiri suatu hubungan atau kewajiban hukum. (Mansur dan Gultom 2005, 30).

Dalam hukum pidana Indonesia, ada beberapa prinsip umum yang berkaitan dengan yurisdiksi, yaitu

1) Prinsip teritorialitas, yang ditegaskan oleh pasal 2 KUHP dan diperluas oleh pasal 3 KUHP (Prodjodikoro 1989, 47).
2) Prinsip nasional aktif yang dianut dalam pasal 5 KUHP dan diperluas oleh pasal 7 KUHP (Prodjodikoro 1989, 49).
3) Prinsip nasional pasif yang termuat dalam pasal 4 ke-1, ke-2, dan ke-3 KUHP (Prodjodikoro 1989, 52).
4) Prinsip universalitas sebagaimana tercantum dalam pasal 4 ke-4 KUHP (Prodjodikoro 1989, 53).

Berdasarkan karakteristik dunia siber yang khusus, Darrel Menthe menyatakan yurisdiksinya membutuhkan prinsip-prinsip yang jelas dan berakar dari hukum internasional. Menthe menambahkan bahwa hanya melalui prinsip-prinsip yurisdiksi dalam hukum internasional, negara-negara dapat dihimbau untuk mengadopsi pemecahan yang sama terhadap yurisdiksi internet Selanjutnya Menthe menunjuk pada tiga teori yang dapat digunakan sebagai pendekatan terhadap yurisdiksi yaitu (1998)

a. *The Theory of the Uploader and the Downloader*, berdasarkan teori ini suatu negara dapat melarang dalam wilayahnya, kegiatan *uploading* dan *downloading* yang bertentangan dengan kepentingannya.
b. *The Theory of the Law and the Server*, pendekatan ini memperlakukan server dimana webpages secara fisik berlokasi.
c. *The Theory of International Spaces*, menurut teori ini ruang siber dianggap sebagai suatu lingkungan hukum yang terpisah dari hukum konvensional dimana setiap negara memiliki kedaulatan yang sama. Proposisi utama teori ini adalah *nationality, not territoriality, is the basis for the jurisdiction to prescribe in outer space, Antarctica, and the high seas*. Oleh karena itu ruang siber dapat dianggap sebagai *the fourth space*. Analogi ruang ini bukan berdasar kesamaan fisik, melainkan pada sifat internasionalnya, yakni *sovereignless quality*.

Sementara itu, sebagai undang-undang yang mengatur pemanfaatan teknologgi informasi dan komunikasi serta pelanggaran pidananya, Undang-Undang ITE mengatur yurisdiksi yang sedikit berbeda dengan KUHP. Perumusan yurisdiksi ini dapat kita lihat dalam Pasal 2 undang-undang itu 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".

1.5.5 Cyber crime

Problem besar yang dihadapi dalam setiap studi mengenai *cybercrime* adalacdh tidak adanya definisi yang konsisten terhadapnya (Yar 2006, 9; Clifford 2006, 3) serta tidak adanya referensi secara spesifik dalam undang-undang (Yar 2006, 9). Namun, para pakar menyepakati *cybercrime* sebagai kejahatan yang dimediasi oleh komputer dan teknologi informasi (Yar 2006, 10; Thomas dan Loader 200, 3). termasuk di dalamnya yang menjadikan komputer dan isinya sebagai target kejahatan (Jewkes 2003, 502).

Wal mengklasifikasikan *cybercrime* ke dalam empat kategori , yaitu (Yar 2006, 10)

a. *Cyber-trespass*, masuk secara ilegal ke dalam properti orang lain dan atau merusaknya, contohnya *hacking, defacement*, virus.
b. *Cyber-deceptions and theft*, mengambil secara ilegal uang atau properti orang lain seperti penipuan kartu kredit dan pembajakan hak intelektual.
c. *Cyber-pornography* atau pornografi di dunia siber
d. *Cyber-violance* berupa kekerasan secara psikologis ataupun provokasi kekerasan fisik kepada orang lain.

Gottffredson dan Hirschi membuat klasifikasi *cybercrime* berdasarkan caranya. Beberapa jenis *cybercrime* dilakukan dengan *force* (paksaan), sementara ada yang dimulai dengan *fraud* atau tipuan.(Yar 2006, 80). *Fraud* atau tipuan sendiri tentu bukan barang baru. Kita sudah mengenalnya sebagai bentuk kejahatan konvensional. Namun, dengan bantuan internet, si penipu akan mampu mengeruk keuntungan yang lebih besar.

Sementara itu, European Convention on Cyber Crime memberikan batasan akan perbuatan-perbuatan yang diklasifikasikan sebagai *cyber crime* yaitu

a. kejahatan terhadap kerahasiaan, integritas dan ketersedian data dan sistem komputer, yang terdiri dari akses ilegal, penyadapan ilegal, gangguan terhadap data, gangguan terhadap sistem, penyalahgunaan perlengkapan komputer, penyalahgunaan program komputer dan *password*.
b. kejahatan yang berhubungan dengan komputer, yaitu kegiatan manipulasi yang dapat menyebabkan data seolah-olah otentik atau yang dapat menyebabkan kerugian orang lain.
c. kejahatan yang berhubungan dengan konten, seperti pornografi anak
d. kejahatan yang berhubungan dengan hak cipta serta hak-hak terkait lainnya.

1.5.6 Internet fraud

Fraud didefinisikan Oxford Dictionary sebagai *crime of deceiving somebody in order to get money illegally.* Oleh karena itu *fraud* adalah suatu kegiatan penipuan yang dilakukan oleh pelaku demi keuntungan dirinya.

Debra L. Shinder mendefinisikan *internet fraud* sebagai penipuan yang melibatkan pemberian informasi yang tidak benar untuk mendapatkan sesuatu yang berharga atau menguntungkan (Golose 2008, 78). Sementara itu, menurut Yar, *internet fraud* dimulai dengan adanya misinformasi atau informasi palsu yang diakses oleh calon korban di internet. Si calon korban kemudian merasa tertarik dengan tawaran yang disodorkan si pelaku. Ia lalu mengeluarkan sejumlah materi untuk

mendapatkannya. Namun, yang terjadi di akhir cerita, si korban tidak memperoleh sesuatu sesuai yang ia harapkan atau bahkan, bisa jadi tidak mendapat sesuatu sama sekali (2006, 80).

Ada beberapa jenis *internet fraud* menurut Majid Yar, yaitu

a. *internet auction fraud* (2006, 81).
b. *advanced fee fraud* (2006, 84).
c. *phising and spoofing* (2006, 87)

Sementara itu, jenis-jenis *internet fraud* menurut Federal Bureau of Investigation adalah

a. *internet auction fraud*
b. *non delivery of merchandise*
c. *credit card fraud*
d. *investment fraud*
e. *business fraud*
f. *Nigerian Letter Scam*

Pada mulanya *internet fraud* ditangani dengan menggunakan rumusan pasal 378 KUHP yang berbunyi "Barang siapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu atau keadaan palsu, baik dengan akal dan tipu muslihat maupun dengan karangan perkataan-perkataan bohong, membujuk orang supaya memberikan sesuatu barang, membuat utang atau menghapus piutang, di hukum karena penipuan, dengan hukuman selama-lamanya empat tahun". Namun, dengan diundangkannya Undang-Undang Nomor 11 tahun 2008, kegiatan kriminal yang pada dasarnya penipuan ini telah memiliki ketentuan yang mengaturnya. Hal itu diatur dalam Pasal 28 ayat (1) yang berbunyi "Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik" dengan ancaman pidana maksimal sesuai pasal penjara enam tahun dan/atau denda maksimal Rp 1.000.000.000,-

Sebagaima kejahatan *cybercrime* lainnya, salah satu institusi peradilan pidana yang bertugas melakukan penegakan hukum terhadap *internet fraud* adalah

kepolisian. Namun, dalam prakteknya banyak kendala yang harus dihadapi oleh kepolisian. Jewkes mengutarakan kendala-kendala dalam penegakan hukumnya adalah (2003, 510)

1) volume dan ruang lingkup *cybercrime* serta problem berkaitan dengan yurisdiksi,
2) keterbatasan sumber daya,
3) kejahatan *cybercrime* yang tidak dilaporkan,
4) budaya penegak hukum.

Yar menambahkan, hambatan semakin besar dengan sikap institusi penegakan hukum yang cenderung statis dalam menghadapi perkembangan kejahatan. Para penegak hukum lebih suka berpikir dan bertindak secara tradisional serta memfokuskan perhatian mereka pada hal-hal yang mereka kuasai atau mereka sukai. (Yar 2006, 16).

1.6 Metodologi Penelitian

1.6.1 Metode penelitian

Penelitian ini menggunakan metode yuridis normatif yang didasarkan pada data sekunder berupa bahan hukum primer, sekunder maupun tersier (Soekanto 2006, 52) Selain itu dilakukan pula pengkajian terhadap data primer yang dikumpulkan melalui wawancara dan observasi.

1.6.2 Sumber Data

Sumber data dalam penelitian ini sebagai berikut:

a. Data sekunder, berupa data yang diperoleh dari dokumen yang dihasilkan oleh para penegak hukum dalam penanganan kasus www.henbing.com, yaitu
    1) Berkas Perkara

2) Surat Dakwaan
3) Berita Acara Persidangan
4) Putusan Pengadilan

Selain dari sumber di atas, data sekunder juga diperoleh dari buku-buku, peraturan perundang-undangan, teori-teori hukum, pendapat para sarjana hukum terkemuka serta hasil penelitian terdahulu.

b. Data primer yang diperoleh melalui penelitian lapangan yakni melakukan observasi dan wawancara. Observasi dilakukan terhadap kegiatan Unit V/IT & Cyber Crime Bareskim Polri, sementara wawancara dilakukan terhadap pihak pihak yang terkait dengan penelitian ini , yaitu
   1) lima orang penyidik dari Unit V/IT & Cyber Crime Bareskim Polri,
   2) dua orang jaksa penuntut umum
   3) satu orang hakim yang menangani kasus www.henbing.com , serta
   4) satu orang pejabat Sekretariat NCB-Interpol Indonesia.

1.6.3 Penyajian Data

Data primer dan data sekunder yang diperoleh, kemudian disusun secara sistematis dan dianalisis secara kualitatif. Analisa kualitatif dilakukan untuk menganalisis dan mengevaluasi data yang telah diperoleh secara mendalam dan menyeluruh untuk menjawab permasalahan dan memperoleh kejelasan terhadap permasalahan dalam penelitian ini.

1.7 Sistematika Penulisan

Bab 1 Pendahuluan

Dalam bab ini diuraikan maksud dan tujuan penelitian, latar belakang masalah, perumusan masalah, kepustakaan penelitian, kerangka teoritis, metode penelitian dan sistematika penulisan.

Bab 2 Penanganan Kasus www.henbing.com

Dalam bab ini diuraikan ringkasan kasus, proses penyelidikan, penerapan pasal 378 KUHP, penentuan locus delicti dan yurisdiksi serta kendala dalam penegakan hukum

Bab 3 Kerjasama Internasional dalam Penegakan Hukum

Dalam bab ini diuraikan bantuan penegakan hukum, kerjasama ICPO-Interpol, kerjasama Aseanapol, kerjasama AMMTC, ekstradisi, serta bantuan hukum timbal balik dalam perkara pidana

Bab 4 Pembahasan

Bab ini merupakan pembahasan hasil temuan penelitian di bab 2 dan bab 3

Bab 5 Penutup

Bab ini terdiri atas kesimpulan dan penutup.

BAB 2

PENANGANAN KASUS www.henbing.com

2.1 Ringkasan Kasus www.henbing.com

Situs www.henbing.com adalah salah satu situs yang digunakan oleh Ronal Harapan Maju Lubis (Ronal) alias Robby Amalo alias Salomo Harahap alias Jimmy Siahaan alias Dapot Purba alias Deny Dongoran, dalam melaksanakan praktik penipuan melalui internet. Dengan situs itu, ia melakukan penawaran barang secara *online* dari perusahaan fiktif yang ia buat, CV Henbing Electronics.

Situs www.henbing.com diperoleh Ronal dengan bantuan Devvy Bayu Prahasatra (Devvy). Devvy membuatkan Ronal sebuah situs yang akan digunakan Ronal untuk menipu serta membeli domain dan hosting pada www.e-padi.com dengan nama www.henbing.com. Setelah situs selesai dibuat, Devvy mengirimkan login administrator dan login control panel kepada Ronal. Sebaliknya, Ronal mengirimkan uang sebesar Rp 4.000.000,- kepada Devvy melalui rekening ayah Devvy, Henri Susilo.

Salah seorang korban dari penipuan www.henbing.com adalah Chumpon Korp-Phaibun yang berkewarganegaraan Thailand. Ketika ia sedang berada di Hongkong pada awal tahun 2007, ia mengakses www.alibaba.com dengan maksud untuk membeli jet ski. Dari berbagai situs yang dihasilkan dalam pencarian melalui www.alibaba.com, ia tertarik kepada penawaran yang ditawarkan oleh perusahaan CV Henbing Electronics. Alasannya, harga yang ditawarkan tidak terlalu mahal dan dapat mempersingkat waktu pengiriman ke Thailand karena penjual berada di Indonesia.

Korban melakukan pemesanan melalui order@henbing.com sebuah jet ski baru dengan merk Yamaha FX HO 160 HP seharga US$ 19,520. Selanjutnya korban berkomunikasi dengan Ronal yang mengaku bernama Roby Amalo melalui e-mail, serta pesan singkat dan percakapan dengan menggunakan nomor telepon seluler 08126534666 sesuai dengan alamat kontak yang tercantum dalam situs

www.henbing.com. Atas perintah pelaku, korban mengirimkan uang dalam dua tahap. Pada tahap pertama, korban mengirimkan uang sebesar US$ 4,520 kepada Roby Amalo dengan nomor rekening 1280005127953 pada Bank Mandiri Tangerang. Pengiriman ini dilakukan pada tanggal 6 November 2007. Sementara itu pengiriman kedua sebesar US$ 15,000 dilakukan pada tanggal 15 November 2007. Kali ini, tujuan pengiriman adalah Bank Mandiri Sentra Menteng dengan nomor rekening 1280005156457 atas nama Salomo Harahap yang diakui pelaku sebagai istrinya.

Korban lalu mendapatkan nota pengiriman dan *internet tracking system* dari PT Kilat Satu. Tetapi, ia kemudian menyadari jika ia ditipu ketika ia bertemu dengan seorang pejabat dari Indonesia yang menyatakan bahwa perusahaan pelaku tidak bisa dipercaya. Ia mencoba membatalkan pengiriman uang, tetapi tidak berhasil. Chumpon lalu melakukan penelusuran terhadap www.henbing.com dan mengetahui bahwa www.henbing.com merupakan salah satu domain pada www.e-padi.com. Selanjutnya ia mengirim e-mail laporan kepada AF, administrator www.e-Padi.com pada tanggal 24, 25, 28 dan 29 bulan Januari 2008. Sang administrator kemudian menginformasikannya kepada penyidik Unit V/ Cybercrime Diretktorat II Bareskrim Polri pada tanggal 28 Januari 2008.

Agar korban mau membuat laporan resmi, salah seorang penyidik Unit V/ IT & Cybercrime, Kompol I Ketut Budi Hendawan, yang kebetulan sedang mengikuti pelatihan di ILEA Academy Bangkok melakukan pendekatan terhadapnya. Akhirnya pada tanggal 23 April 2008, Cumpon Korp-Paibun mendatangi Mabes Polri untuk membuat laporan resmi atas kejahatan yang menimpa dirinya. Berdasarkan laporan korban ini, dilakukan rangkaian peradilan pidana kepada kedua pelaku. Kedua pelaku dinyatakan bersalah telah melanggar pasal 378 KUHP dan dijatuhi pidana masing-masing tersangka, penjara selama satu tahun delapan bulan.

2.2 Proses Penyelidikan

Dalam menemukan para tersangka, penyidik memerlukan proses yang cukup panjang. Diperlukan waktu sekitar tujuh bulan oleh penyidik untuk menyelidiki

keberadaan tersangka. Proses penyelidikan terhadap kasus www.henbing sendiri diawali dengan maraknya keluhan para pengguna internet yang menjadi korban penipuan, khususnya meraka yang menjadi korban penipuan para pelaku yang membonceng layanan situs www.alibaba.com (Wawancara dengan I Ketut Budi Hendrawan tanggal 1 Maret 2010). Salah satu dari keluhan itu dimuat dalam sebuah laman di www.GoDaddy.com. Laman itu memperingatkan ketidakamanan bertransaksi elektronik dengan warga negara Indonesia. Menurut pemilik laman, pelaku bisnis Indonesia tidak bisa dipercaya serta mengambil keuntungan dari ketiadaan hukum yang mengatur transaksi elektronik. Masih menurutnya, keadaan itu diperparah dengan sikap perbankan Indonesia yang pura-pura tidak tahu akan aktivitas ilegal para penipu itu. Si penulis menceritakan bagaimana dirinya bisa menjadi korban penipuan Deni Dongoran, pemilik www.pitbos.net. Ia berhubungan dengan Deni Dongoran ketika ia mencari barang yang ia inginkan melalui layanan www.alibaba.com dan menemukan barang yang ia inginkan di situs www.pitbos.net. Ia mengirimkan uang sebesar US$ 19,000 dan sebagai balasannya ia dikirimkan konfirmasi pengiriman dari PT Kilat Satu Services yang beralamat di Astina Building M#101-105 Surabaya 60354 tanpa nomor telepon. Tetapi, pada akhirnya ia tidak menerima barang hasil transaksinya dengan Deni Dongoran. Ia juga menyebutkan dua identitas lain yang digunakan oleh Deni Dongoran, yaitu

a. Supriadi (Pitbos Store). Alamat: Jl. Siatas Barita No. 87 Manado, Sulawesi Utara Indonesia 90176 Telepon +628126534666, Email : order@pitbos.net.
b. Jimmy Siahaan (Jimmy Store Online). Alamat Jl. Zainal Abidin, Pagar Alam No. 1 Haji Mena, Bandar Lampung, Propinsi Lampung, Indonesia, 35142. Telepon :62-721-780662, Telepon Seluler : 081386060576

Laman itu juga menyebutkan korban-korban lain yang menghubungi si penulis. Mereka adalah

a. Vizionthing, dengan alamat vizionthing@gmail.com dan kerugian sebesar AU$ 1,200

b. J Roberts, dengan alamat elusiveentertainment@yahoo.com dan kerugian sebesar AU$10,000
c. Aidas Sindaras, dengan alamat jurgitabarda@gmail.com dan kerugian sebesar US$1,012
d. Wayne Martin, dengan alamat jenwayelec@optusnet.com.au dan kerugian sebesar AU$750
e. Maxie Burney, dengan alamat http://denidongoran.info/ maxmotorsportsrchobbies@yahoo.com dan kerugian sebesar $1,072.50 USD
f. Davide Borgonovo, dengan alamat http://denidongoran.info/ 177,%2001%20euro dan kerugian sebesar $1,770 euro

Sementara itu, rekening yang dipakai oleh pelaku untuk menerima kiriman uang para korban adalah

a. Rekening Bank Mandiri Batam nomor 1090006775191 atas nama Supriadi dan Swift Code BEIIIDJA. Alamat bank: Jl Sudirman no 87 Nagoya Batam.
b. Rekening Bank Mandiri Bogor Tajur nomor 1330005812714 atas nama Deni Dongoran dan Swift Code BEIIIDJA. Alamat bank : Jl. Raya Curuk no 38 Jawa Barat 15319.
c. Rekening Bank Mandiri Sentra Menteng nomor 128005286726 dan Swift Code BEIIIDJA. Alamat bank: Jl Raya Serpong no 89 Tangerang Banten.

Dengan adanya pengaduan-pengaduan ini, petugas mengambil langkah untuk mengadakan pendekatan kepada korban dengan tujuan untuk mendapatkan kejelasan atas kasus yang dialami mereka. Sayangnya, pendekatan ini tidak direspon secara positif. Petugas kemudian melakukan penyelidikan itu dilakukan dengan 2 metode, yaitu metode konvensional dan secara *online* (Wawancara dengan I ketut Budi Hendrawan tanggal 2 Februari 2010). Melalui penyelidikan konvensiona,l petugas mencari nama sesuai data yang tertera dalam kontak di domain-domain itu. Namun, hal itu tidak mendapatkan hasil, karena baik nama maupun alamat adalah fiktif.

Dalam penyelidikan *online*, petugas mengumpulkan menggunakan bantuan alat pencari di internet. Penyidik memasukkan data yang diketahui, seperti nama kontak dan nomor telepon, ke alat pencari di internet untuk mengumpulkan informasi. Informasi yang dihasilkan kemudian dimasukkan lagi ke dalam mesin pencari untuk mendapatkan informasi berikutnya. Kegiatan ini dilakukan penyidik secara berulang-ulang. Hasilnya terdapat beberapa website lain yang diduga memiliki hubungan atau diduga dimiliki oleh orang atau jaringan yang sama dengan www.pitbos.net, antara lain www.naboaon.com, www.mardalani.com, www.marsima.com, www.embul.com, dan www.rohohepeng.com. Situs-situs tadi memiliki kesamaan pola, jenis barang yang ditawarkan, harga, dan kontak (Wawancara dengan I ketut Budi Hendrawan tanggal 1 Maret 2010). Kemudian dengan bantuan *tools* yang tersedia, IP Adress dan hostnya diketahui. Situs-situs itu dihosting di www.e-padi.com yang berkedudukan di Aceh.

Petugas kemudian melakukan pendekatan terhadap AF yang merupakan administrator www.e-padi.com. Pendekatan ini direspons positif oleh AF Ia menyatakan siap memberikan bantuan.kepada para penyidik dalam mengungkap pelaku *internet fraud* baik yang di hossting di www. e-padi.com maupun yang dihosting di server lain.

Pada perkembangan berikutnya, AF menyatakan adanya laporan penipuan yang dilakukan oleh domain lain yang memiliki kesamaan pola yaitu www.henbing.com dengan perusahaannya bernama CV. Henbing dan pemilik Nico Henbing Kaunang dan yang beralamat di Jl. Pool Pasir Bantar Panjang RT 7 RW III Bogor Jawa Barat. (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2010). Dari keterangan AF, diketahui www.e-padi.com, domain ini tidak lagi menggunakan server www.e-padi.com melainkan menggunakan server cirtexhosting.com yang berada di luar negeri. www.henbing.com pernah menggunakan server www.e-padi.com, pada periode September- Oktober 2007. Meskipun demikian dari data yang dimiliki hingga Oktober 2007, diketahui bahwa log in terakhir dilakukan oleh komputer dengan IP Adress 66.160.138.130 dengan lokasi IP adalah Fremont Hurricane Electric di Amerika Serikat. Sementara itu lebih

dari 40% login dilakukan dari class IP 221.132.*.*, yaitu 221.132.249.135, 221.132.248.91, 221.132.249.70, 221.132.249.135, 221.132.242.18, 221.132.243.118, 221.132.247.104, 221.132.246.148, 221.132.243.250, 221.132.247.156. IP 221.132.*.*, ini adalah IP yang berada dalam jaringan Telkomsel. Informasi ini memberikan petunjuk kepada petugas bahwa akses internet oleh pelaku kemungkinan dilakukan menggunakan jaringan Telkomsel yang bersifat mobile.

Pada tanggal 23 November 2007, AF melakukan *chatting* dengan orang yang diduga sebagai pemilik akun boatstarship@yahoo.co.id yang diduga sebagai pemilik www.henbing.com. Akun tadi diperoleh AF setelah "chatting" dengan Indra Prahastra yang merupakan pengorder www.embul.com di rumah hostingnya. Dari "chatting" dengan boatstarship ini, AF berhasil mendapatkan gambar wajah tersangka. Petugas kemudian memasukkan alamat email boatstarship@yahoo.co.id ke dalam situs jejaring sosial "friendster". Dari jejaring sosial ini, petugas mendapatkan gambar wajah orang yang diduga sebagai pelaku dan keluarganya.

Pada tanggal 24 Januari 2008, AF mendapatkan laporan dari Chumpon Korp-Paibun yang menyatakan dirinya telah menjadi korban penipuan setelah ia melakukan pemesanan melalui order@henbing.com, Ia telah melakukan pengiriman uang sebesar US$ 19,520 kepada Robby Amalo untuk pembelian sebuah jet ski baru dengan merk Yamaha FX HO 160 HP, tetapi tidak pernah mendapatkan barangnya. Chumpon juga melampirkan bukti transferrya kepada rekening Robby Amalo dan Salomo Harahap. Informasi ini diteruskan AF kepada pada tanggal 28 Januari 2008 Unit V/ IT & Cybercrime.

Pada tanggal 24 Maret 2008, Unit V/IT dan Cyber Crime menerima Berita Faksimil beromor RR-027/Athena/III/08 tanggal 14 Maret 2008 dari KBRI Athena. Surat itu berisikan enam pengaduan yang dibuat oleh para pengusaha Yunani yang mengaku menjadi korban penipuan yang dilakukan baik oleh beberapa perusahaan penyedia barang di Indonesia. Para pengusaha tadi menjadi korban penipuan setelah bertransaksi bisnis dengan perusahaan yang tertera dalam situs www.alibaba.com. Salah seorang dari mereka bernama Nanouris Bill menjadi korban www.henbing.com

setelah memesan Raptor 90 Se RTF with JR 9303 kepada CV Dua Arena Toys dengan alamat Jl. Pandapotan no 90 Manado melalui order@henbing.com dan contact person Robby Amalo. Nanouris telah mengirimkan uang sesesar US$ 460 kepada Robby Amalo, namun tidak mendapatkan barang yang diinginkan.

Pada tanggal 8 April 2008, dengan menyamar sebagai seorang pelaku penipuan internet pemula, AF berhasil melakukan percakapan dengan target. Dalam percakapan kali ini ia mendapatkan nama anak target adalah Matias Lubis, artinya tersangka juga bermarga Lubis.

Pada tanggal 24 April 2008, Chumpon membuat laporan resmi di Mabes Polri. Laporan ini ia buat setelah berkonsultasi dengan Ketut Budi di Bangkok. Laporan Polisi No.Pol : LP/215/IV/2008/Siaga-I ini kemudian ditindaklanjuti dengan Surat perintah Penyidikan No.Pol : SP.Sidik/36/IV/2008/Dit Eksus. Berdasarkan surat perintah ini, dibentuklah tim beranggotakan tujuh orang yang dipimpin oleh AKBP Faizal Thayeb.

Dari informasi yang diperoleh selama penyelidikan, penyidik behasil melakukan pemetaan terhadap www.henbing.com. Hasilnya petugas menemukan beberapa perusahaan dan nomor rekening yang memiliki hubungan dengannya. Perusahaan-perusahaan itu adalah

a. CV.Felix Healthy, dengan nomor telepon 08126534.771
b. CV Kapal Hepeng, alamat, Jl.Sedap Malam 19 Nusa Dua Bali, dengan nomor telepon. 08126534.771
c. CV.Embul Electronic, atas nama .Anak agung,, alamat Jl. TB Simatupang 71 Jogja, dengan nomor telepon. 08126534.771
d. CV.Romaho Electonic, atas nama.Bona Sinaga, alamat Jl.Sedap Malam 105 Denpasar Bali, dengan nomor telepon 08126534.771.
e. CV Mangampuni Electronic. atas nama.Henri Tobing, alamat Jl.Huta Ginjang 73 Makasar, dengan nomor telepon 08126534.771
f. Naboaon electonics inc.. atas nama.Frans Lubis, Jl.Kapten Sutoyo 74 Jawa Barat.

g. Naboaon electronic, Jl.Sam Ratulangi 81 Manado, dengan nomor telepon. 08126534.771.

h. CV.Star Wave Abadi, atas nama. Boru Tobing, dengan nomor telepon 08126534.666, alamat Jl Panglima polim 85 Menado

i. CV Dua Arena Toys dengan alamat Jl. Pandapotan no 90 Manado dengan nomor telepon 08126534.666 .

j. CV.Henbing Electronic, alamat Jl.Kuta 84 Denpasar bali

k. PT.Kilat Satu Service, atas nama .Deni Dongoran, alamat Jl.Raya CurukG38 Jawa Barat atau Jl.Siatas Barita 87 Manado atau Jl Astina Building M 101-105 surabaya, dengan nomor telepon . 08126534.666.

l. Embul Electronic.inc, atas nama.Mr.Anak Agung Diva, Jl.Bakti 15 Makasar

m. Star Electro inc, alamat Jl.Sutomo 74 Palembang, dengan nomor telepon.081381390001.

n. Rohohepeng Elect.inc, Jogja, atas nama .James Purba, Jl.TB Simatupang 71, dengan nomor telepon.081381390001

o. Star Parsiantar inc., atas nama .Manggiring Bastian, alamat Jl. Patimura 86 Palembang, Hp. dengan nomor telepon.081381390001.

p. Global media electronic utama,Jl.Cirebon No.19 Jakarta, dengan alamat email Mankimail@hotmail.com, dengan nomor telepon .081381390001.

q. Alfajerin & Electro & co., dengan alamat email Mankimail@hotmail.com, Jl.Danau singkaraku 39J, dengan nomor telepon.081381390001.

r. Cv,Aneka Games Electronic, An.Deni Dongoran, dengan alamat email Mankimail@hotmail.com

Sementara itu rekening yang digunakan pelaku antara lain;

a. Dapot Purba, Bank Mandiri rek.118.000.530.8845, jl.Raya Serpong 84 Tangerang.

b. Salomo Harahap, Bank Mandiri rek.128.000.515.6457, Mandiri Sentra Menteng, Jl Subakti 74 Tangerang.

c. Roby Amalo, Bank Mandiri rek.128.000.512.7953, Tangerang BSD

d. Anak Agung Diva Saputra, Bank Mandiri Denpasar Merdeka, rek.145.000.0562.6557.
e. Jimmy Siahaan, Bank Mandiri Kramat Raya, rek.123.000.470.9145.
f. Frans Lubis, Bank Mandiri Cikarang, rek.156.000.0240.988.
g. Deni Dongoran, Bank Mandiri Bogor Tajur, rek.133.000.5812.714.
h. Ronal Lubis, Bank Niaga Pondok Indah, rek.017.014.4845.133.

Pada tanggal 8 Mei 2008, penyidik berhasil menangkap tersangka di rumahnya. Penangkapan akhirnya dilakukan setelah penyidik melihat mobil yang gambarnya terpajang di jejaring sosial friendster masuk ke dalam sebuah rumah tersangka. Pada saat tersangka ditangkap sebenarnya tersangka tidak sendirian. Ada beberapa orang lagi yang ada di rumah tersangka yang kemudian diketahui merupakan pelaku *internet fraud* juga. Sayangnya tidak ada laporan dari orang yang pernah menjadi korban kejahatan mereka sehingga terhadap mereka tidak bisa diadakan dan setelah Ronal ditangkap, mereka melarikan diri (Wawancara dengan I Ketut Budi Hendrawan tanggal 1 Maret 2010).

Penyelidikan *online* juga dilakukan dalam pencarian tersangka Devvy. Dengan bantuan AF, penyidik dapat memonitor tersangka. Pada awalnya informasi yang diperoleh adalah nama Prahastra bersaudara yang menjadi pendesain web. Informasi ini kemudian berkembang dengan diperolehnya gambar tersangka Devvy di jejaring sosial friendster. Setelah Ronal ditangkap, ia menyebutkan peran dan bantuan tersangka Devvy. Atas dasar keterangan tersangka Ronal dan hasil penyelidikan *online*, tersangka Devvy ditangkap di rumahnya pada tanggal 21 Mei 2008 (Wawancara dengan I Ketut Budi Hendrawan tanggal 13 April 2010)

2.3 Penerapan Pasal 378 KUHP

Pada saat korban melaporkan kejahatan yang dialaminya, Indonesia telah memiliki peraturan perundang-undangan yang mengatur dunia siber. Aturan itu dituangkan dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan

Elektronik (ITE) yang disahkan pada tanggal 11 April 2008. Undang-undang yang dimuat dalam Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58 ini dibentuk dengan pertimbangan bahwa dinamika yang terjadi dalam masyarakat sebagai akibat perkembangan dan kemajuan Teknologi Informasi sudah seharusnya ditanggapi dengan sebuah peraturan perdundang-undangan yang mampu melindungi kepentingan nasional. Selain itu, keberadaan undang-undang ini diharapkan dapat memberikan direktif pengembangan dan pemanfaatan teknologi informasi. Termasuk di dalamnya, penerapan aturan pidana terhadap penyalahgunaan teknologi informasi.

Namun, meskipun laporan polisi diterima pada tanggal 24 April 2008, Undang-Undang ITE tidak diterapkan pada kasus www.henbing.com. Hal ini disebabkan karena rangkaian perbuatan para tersangka dilakukan sebelum Undang-Undang ITE disahkan (Wawancara dengan Kompol I Ketut Budi Hendrawan tanggal 1 April 2010; Wawancara Jaksa Penuntut Umum Raharjo Budi Kisnanto tanggal 1 April 2010).

Tidak diterapkannya Undang-Undang ITE dalam penegakan hukum kasus www.henbing.com juga berpengaruh terhadap acara pidana yang diberlakukan. Undang-Undang ITE mewajibkan adanya penetapan dari Ketua Pengadilan Negeri dalam setiap upaya paksa yang dilakukan. Dengan tidak diterapkannya Undang-Undang ITE penangkapan dan penahanan tersangka serta penggeledahan dan penyitaan barang bukti dilakukan tanpa dari penetapan Ketua Pengadilan Negeri (Wawancara dengan Kompol I Ketut Budi Hendrawan tanggal 1 April 2010; Wawancara dengan Iptu Maryudi Salempang tanggal 1 April 2010).

Sementara itu, Raharjo mengakui adanya kesulitan dengan belum digunakannya barang bukti digital. Pasal 184 (1) KUHAP hanya mengakui lima alat bukti yang sah di persidangan, yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Oleh karena itu, untuk mendapatkan alat bukti petunjuk, ia menghadirkan barang bukti laptop terdakwa untuk dilihat isinya dalam persidangan. Penuntut umum berupaya memperlihatkan situs www.henbing.com yang dipergunakan oleh terdakwa dalam menjalankan aksinya (Wawancara dengan Raharjo Budi Kisnanto tanggal 15 Maret 2010).

Meskipun demikian, majelis hakim yang terdiri Ismail S.H., sebagai ketua dan beranggotakan Masrudin Chaniago, S.H., dan Retno Pudyaningtyas, S.H., tidak merasa kesulitan dalam mengadili perkara itu. Menurut Ismail, hal itu disebabkan perbuatan para terdakwa itu pada dasarnya tidak berbeda dengan penipuan biasa dan para terdakwa mengakui perbuatannya itu (Wawancara tanggal 16 Februari 2010).

Penerapan pasal 378 KUHP oleh penegak hukum ini termuat dalam dokumen dokumen berikut:

2.3.1 Berkas Perkara Ronal Harapan Maju Lubis

Dalam, analisa yuridisnya, penyidik berkeyakinan bahwa apa yang dilakukan oleh Ronal telah memenuhi unsur-unsur pasal 378 KUHP yang berbunyi : *Barang siapa* dengan maksud hendak *menguntungkan diri sendiri* atau orang lain dengan *melawan hak*, baik dengan memakai nama palsu atau *keadaan palsu*, baik dengan akal dan tipu muslihat maupun dengan karangan perkataan-perkataan bohong, *membujuk* orang supaya *memberikan* sesuatu barang, membuat utang atau menghapus piutang, di hukum karena *penipuan*, dengan hukuman selama-lamanya empat tahun. Rumusan pasal ini terpenuhi karena hal-hal sebagai berikut:

a. Tersangka Ronal dalam keadaan mampu bertanggung jawab atas perbuatannya.
b. Dari perbuatan tersangka menawarkan barang kepada korban, tersangka mendapat keuntungan sehingga harta yang dimiliki tersangka bertambah senilai US$ 19,420
c. Harta tambahan tadi didapat tidak sewajarnya karena tidak ada prestasi apapun yang dirasakan oleh orang lain, khususnya orang yang dirugikan.
d. Tidak ada kebenaran dalam barang-barang yang ditawarkan melalui website www.henbing.com.
e. Tersangka menawarkan barang elektronik kepada saksi Chumpon Korp-Phaibun, sehingga ia tertarik dan memiliki keinginan untuk membeli barang berupa jet ski.

f. Saksi Chumpon Korp-Phaibun melakukan transfer pembelian jet ski sebanyak dua kali. Transfer pertama dilakukan pada tanggal 6 November 2007, ia mengirim uang sebesar USD 4,520 kepada Roby Amalo, Bank Mandiri Tangerang No.Rek. 1280005127953. Pengiriman kedua pada tanggal 15 November 2007, ia transfer kepada Salomo Harahap, Bank Mandiri Jakarta No.Rek. 1280005156457 sebesar USD 15,000.

2.3.2 Berkas Perkara Devvy Bayu Prahastra

Terhadap perbuatan Devv, penyidik berkeyakinan bahwa apa yang dilakukannya telah memenuhi unsur-unsur pasal 378 jo pasal 56 KUHP . Pasal 378 KUHP berbunyi : *Barang siapa* dengan maksud hendak *menguntungkan diri sendiri* atau orang lain dengan *melawan hak*, baik dengan memakai nama palsu atau *keadaan palsu*, baik dengan akal dan tipu muslihat maupun dengan karangan perkataan-perkataan bohong, *membujuk* orang supaya *memberikan* sesuatu barang, membuat utang atau menghapus piutang, di hukum karena *penipuan*, dengan hukuman selama-lamanya empat tahun. Dalam perkara Devvy, perbuatan pidana berupa penipuan telah dilakukan selesai oleh tersangka Ronal Harapan Maju Lubis

Sementara itu, Pasal 56 KUHP berbunyi: Dihukum dengan sengaja membantu melakukan kejahatan itu, sementara ayat (2)-nya berbunyi: Mereka yang sengaja memberikan kesempatan, sarana atau keterangan untuk melakukan kejahatan. Rumusan pasal ini terpenuhi karena hal-hal berikut:

a. Tersangka Devvy Bayu Prahastra yang dalam keadaan mampu bertanggung jawab atas perbuatannya
b. Devvy Bayu Prahastra mengetahui bahwa website www.henbing.com dibuatnya dapat digunakan sebagai sarana kejahatan penipuan. Akan tetapi tersangka Devvy Bayu Prahastra tetap membiarkan website www.henbing.com diberikan kepada Ronal Harapan Maju Lubis yang akan melakukan tindak pidana penipuan

c. website www.henbing.com merupakan alat atau sarana yang berisikan penawaran barang-barang elektronik kepada khalayak

d. Tanpa adanya sarana berupa website www.henbing.com, Ronal Lubis tidak akan dapat melakukan tindak pidana penipuan.

2.3.3 Surat Dakwaan Ronal Harapan Maju Lubis

Dalam Surat Dakwaan: NO. REG. PERK: PDM-705/TNG/07/2008 tanggal 14 Juli 2008, Jaksa mendakwa Ronal Harapan Maju Lubis alias Roby Amalo alias Salomo Harahap alias Dapot Purba alias Jimmy Siahaan alias Deny Dongoran dengan dua dakwaan. Dalam dakwaan pertama, ia beserta Devvy Bayu Prahastra, bertempat di rumah saksi Devvy Bayu Prahastra yang terletak di Jalan Trijata Gang Flamboyan nomor 24 Denpasar dan rumahnya di Giri Loka III Blok Z 1 Nomor 17 BSD City Tangerang, atau sekitar tempat itu, oleh karena terdakwa bertempat tinggal, berdiam terakhir dan ditahan di Tangerang, maka berdasarkan pasal 84 ayat 2 KUHAP termasuk dalam kewenangan mengadili Pengadilan Negeri Tangerang, dengan maksud untuk menguntungkan diri sendiri atatu orang lain secara melawan hukum dengan memakai nama palsu dengan tipu muslihat ataupun rangkaian kebohongan menggerakkan orang lain untuk menyerahkan barang kepadanya. sebagaimana diatur dan diancam pidana dalam pasal 378 KUHP jo pasal 55 ayat 1 ke-1 KUHP.

Perbuatan itu dilakukan terdakwa dengan jalan, bertemu saksi Devvy Bayu Prahastra dan meminta untuk dibuatkan website www.henbing.com. Saksi kemudian menyanggupi untuk membuatkan website dimaksud dengan cara membeli domain dan hosting dengan nama yang diinginkan terdakwa yang telah menunjukkan contoh website yang diperlihatkan kepada saksi yang telah dicahtting kemudian saksi meng-upload konten image dan database ke nama website terdakwa yang telah dipesan sebelumnya dnegan mengubah tampilan logo dan menambah kata-kata ke nama website baru. setelah jadi saksi menghubungi terdakwa melalui SMS bahwa website sudah jadi sekaligus memberikan login admin dan login control panel menggunakan

server e-padi network kemudian terdakwa membayar saksi sebesar Rp 4.000.000,-. Selanjutnya website www.henbing.com oleh terdakwa dengan tipu muslihat seolah-olah menjual barang secara *online* dengan menggunakan fasilitas internet banking di www e-padi.com, emailnya yaitu order@henbing.com dengan paswordnya bujanginam, menwarkan satu unit jetski Yamaha FX HO 160 HP tahun 2007 seharga US$ 19,520. Setelah barang ditawarkan melalui internet teernyata saksi korban Chumpon Korp-Phaibun tertarik untuk membeli barang yang ditawarkan terdakwa itu, kemudian saksi korban melakukan komunikasi melalui email order@henbing.com maupun SMS kepada terdakwa melalui nomor HP 08126534666. Saat itu terdakwa mengaku bernama Robby Amalo. Kemudian saksi korban sepakat membeli jetski dimaksud dan terdakwa meminta agar pembayaran ditransfer melalui rekening Bank Mandiri. Atas rangkaian kebohongan terdakwa itu, tergeraklah hati saksi korban untuk mentransfer uang sejumlah US$ 19,520 kepada terdakwa melalui dua kali masing-masing pada tanggal 6 November 2007 sebesar US$ 4,520 melalui Bank Mandiri Tangerang no rekening 1280005127953 atas nama Robby Amalo dan pada tanggal 15 November 2007 sesesar US$ 15,000 melalui Bank Mandiri Jakarta no rekening 1280005156457 atas nama Salomo Harahap. Setelah menerima transfer dimaksud, terdakwa mengambil uang itu melalui ATM BSD Pasar Modern Tangerang. Setelah menerima uang dari saksi korban, terdakwa tidak pernah mengirim barang yang dipesan saksi korban, sehingga akibat perbuatannya, terdakwa telah memperoleh keuntungan sebsesar US$ 19,520. Uang itu habis dipergunakan untuk memenuhi kebutuhan hidupnya, sementara saksi korban telah menderita kerugian sebesar US$ 19,520 atau setidak-tidaknya lebih dari Rp 250,-.

Dalam dakwaan kedua jaksa mendakwa Ronal bertempat di rumah saksi Devvy Bayu Prahastra yang terletak di Jalan Trijata Gang Flamboyan nomor 24 Denpasar dan rumahnya di Giri Loka III Blok Z 1 Nomor 17 BSD City Tangerang, atau sekitar tempat itu, oleh karena terdakwa bertempat tinggal, berdiam terakhir dan ditahan di Tangerang, maka berdasarkan pasal 84 ayat 2 KUHAP termasuk dalam kewenangan mengadili Pengadilan Negeri Tangerang, dengan sengaja memberikan

bantuan kepada saksi Devvy Bayu Prahastra dengan maksud maksud untuk menguntungkan diri sendiri atatu orang lain secara melawan hukum dengan memakai nama palsu dengan tipu muslihat ataupun rangkaian kebohongan menggerakkan orang lain untuk menyerahkan barang kepadanya sebagaimana diatur dan diancam pidana dalam pasal 378 KUHP jo pasal 56 ayat 1 ke-1 KUHP.

Perbuatan itu dilakukan terdakwa dengan bertemu saksi Devvy Bayu Prahastra, meminta untuk dibuatkan website www.henbing.com, kemudian saksi itu menyanggupi untuk membuatkan website dimaksud dengan cara membeli domain dan hosting dengan nama yang diinginkan terdakwa yang telah menunjukkan contoh website yang diperlihatkan kepada saksi yang telah dichatting kemudian saksi meng-upload konten image dan database ke nama website terdakwa yang telah dipesan sebelumnya dengan mengubah tampilan logo dan menambah kata-kata ke nama website baru. Setelah jadi, saksi menghubungi terdakwa melalui SMS bahwa website sudah jadi sekaligus memberikan loginadmin dan login control panel menggunakan server e-padi network. Kemudian terdakwa membayar saksi sebesar Rp 4.000.000,-. Selanjutnya website www.henbing.com oleh terdakwa dengan tipu muslihat seolah-olah menjual barang secara *online* dengan menggunakan fasilitas internet banking di www.e-padi.com, emailnya adalah order@henbing.com dengan password bujanginamm, yaitu menawarkan satu unit jetski yamaha FX HO 160 HP tahun 2007 seharga US$ 19,520. setelah barang dimaksud ditawarkan melalui internet ternyata saksi korban Chumpon Korp-Phaibun tertarik untuk membeli barang yang ditawarkan terdakwa, keudian saksi korban melekukan beberapa komunikasi melalui email order@henbing.com maupun SMS. Kemudian saksi korban melakukan beberapa kali komunikasi melalui email itu maupun SMS kepada terdakwa melaui nomor HP 08126534666. Saat itu terdakwa mengaku bernama Robby Amalo, kemudian saksi korban sepakat membeli jetski dimaksud dan terdakwa meminta agar pembayaran ditransfer melalui rekening Bank Mandiri. Atas serangkaian kebohongan terdakwa, tergeraklah hati saksi korban untuk mentransfer uang sejumlah US$ 19,520 kepada terdakwa sebanyak dua kali masing-masing pada tanggal 6 November 2007 sebesar US$ 4,520 melalui Bank Mandiri Tangerang no rekening 1280005127953 atas nama

Robby Amalo dan pada tanggal 15 November 2007 sesesar US$ 15,000 melalui Bank Mandiri Jakarta no rekening 1280005156457 atas nama Salomo Harahap. Setelah menerima transfer dimaksud, terdakwa mengambil uang itu melalui ATM BSD Pasar Modern Tangerang. Setelah menerima uang dari saksi korban, terdakwa tidak pernah mengirim barang yang dipesan saksi korban, sehingga akibat perbuatannya, terdakwa telah memperoleh keuntungan sebsesar US$ 19,520. Uang itu habis dipergunakan untuk memenuhi kebutuhan hidupnya, sementara saksi korban telah menderita kerugian sebesar US$ 19,520 atau setidak-tidaknya lebih dari Rp 250,-.

2.3.4 Surat Dakwaan Devvy Bayu Prahastra

Dalam Surat Dakwaan : NO. REG. PERK: PDM-950/TNG/07/2008 tanggal 28 Juli 2008, Jaksa mendakwa Devvy Bayu Prahastra beserta Ronal Harapan Maju Lubis alias Roby Amalo alias Salomo Harahap alias Dapot Purba alias Jimmy Siahaan alias Deny Dongoran dengan dua dakwaan. Dalam dakwaan pertama, ia beserta beserta Ronal Harapan Maju Lubis alias Roby Amalo alias Salomo Harahap alias Dapot Purba alias Jimmy Siahaan alias Deny Dongoran, bertempat di rumah Devvy Bayu Prahastra yang terletak di Jalan Trijata Gang Flamboyan nomor 24 Denpasar dan rumah saksi di Giri Loka III Blok Z 1 Nomor 17 BSD City Tangerang, atau sekitar tempat itu, oleh karena sebagian besar saksi yang dipanggil lebih dekat pada Pengadilan Negeri Tangerang dan terdakwa ditahan di Tangerang, maka berdasarkan pasal 84 ayat 2 KUHAP termasuk dalam kewenangan mengadili Pengadilan Negeri Tangerang, dengan maksud untuk menguntungkan diri sendiri atatu orang lain secara melawan hukum dengan memakai nama palsu dengan tipu muslihat ataupun rangkaian kebohongan menggerakkan orang lain untuk menyerahkan barang kepadanya, sebagaimana diatur dan diancam pidana dalam pasal 378 KUHP jo pasal 55 ayat 1 ke-1 KUHP.

Perbuatan itu dilakukan dengan kronologis saksi Ronal Harapan Maju Lubis alias Robby Amalo alias Salomo Harahap alias Dapot Purba alias Jimmy Siahaan

alias Deny Dongoran bertemu dengan terdakwa meminta untuk dibuatkan website www.henbing.com. Terdakwa menyanggupi untuk membuatkan website dimaksud. Terdakwa kemudian membeli domain dan hosting dengan nama yang diinginkan saksi Ronal Harapan Maju Lubis yang telah menunjukkan contoh website yang diperlihatkan kepada terdakwa yang telah dichatting, kemudian terdakwa meng-upload konten image dan database ke website saksi yang telah dipesan sebelumnya dengan mengubah tampilan logo dan menambah kata-kata ke website baru. setelah jadi website itu, terdakwa menghubungi saksi Ronal harapan Maju Lubis melalui SMS bahwa SMS sudah jadi sekaligus memberikan login admin dan login control panel menggunakan server e.padi network. Kemudian saksi Ronal Harapan Maju Lubis membayar terdakwa sebsera Rp 4.000.000,-. Selanjutnya website www.henbing.com oleh saksi Ronal Harapan Maju Lubis dengan tipu muslihat seolah-olah menjual barang secara *online* dengan menggunakan fasilitas internet banking di www.e-padi.com, emailnya order@henbing.com dengan password bujanginam yaitu menawarkan satu unit jetski Yamaha FX HO 160 HP tahun 2007 seharga US$ 19,520. Setelah barang dimaksud ditawarkan melalui internet temyata saksi korban Chumpon Korp-Phaibun tertarik untuk membeli barang yang ditawarkan saksi Ronal Harapan Maju Lubis. Kemudian saksi korban melakukan beberapa komunikasi melalui email order@henbing.com maupun SMS kepada saksi Ronal Harapan Maju Lubis melalui nomor hp 08126534666. Saat itu saksi Ronal Harapan Maju Lubis mengaku bernama Robby Amalo, kemudian saksi korban sepakat membeli jetski dimaksud dan terdakwa meminta agar pembayaran ditransfer melalui rekening Bank Mandiri. Atas serangkaian kebohongan saksi Ronal Harapan Maju Lubis , tergeraklah hati saksi korban untuk mentransfer uang sejumlah US$ 19,520 kepada terdakwa sebanyak dua kali masing-masing pada tanggal 6 November 2007 sebesar US$ 4,520 melalui Bank Mandiri Tangerang no rekening 1280005127953 atas nama Robby Amalo dan pada tanggal 15 November 2007 sesesar US$ 15,000 melalui Bank Mandiri Jakarta no rekening 1280005156457 atas nama Salomo Harahap. Setelah menerima transfer dimaksud, saksi Ronal Harapan Maju Lubis mengambil uang itu melalui ATM BSD Pasar Modern Tangerang. Setelah menerima

uang dari saksi korban, terdakwa tidak pernah mengirim barang yang dipesan saksi korban, sehingga akibat perbuatannya, saksi Ronal Harapan Maju Lubis telah memperoleh keuntungan sebsesar US$ 19,520. Uang itu habis dipergunakan untuk memenuhi kebutuhan hidup saksi Ronal Harapan Maju Lubis , sementara saksi korban telah menderita kerugian sebesar US$ 19,520 atau setidak-tidaknya lebih dari Rp 250,-.

Dalam dakwaan kedua, jaksa mendakwa Devvy dengan sengaja memberikan bantuan kepada saksi Ronal bertempat di rumahnya yang terletak di Jalan Trijata Gang Flamboyan nomor 24 Denpasar dan rumah saksi Ronal di Giri Loka III Blok Z 1 Nomor 17 BSD City Tangerang, atau sekitar tempat itu, oleh karena sebagian besar saksi yang dipanggil lebih dekat pada Pengadilan Negeri Tangerang dan terdakwa ditahan di Tangerang, maka berdasarkan pasal 84 ayat 2 KUHAP termasuk dalam kewenangan mengadili Pengadilan Negeri Tangerang, dengan sengaja memberikan bantuan kepada saksi Ronal , dengan maksud untuk menguntungkan diri sendiri atatu orang lain secara melawan hukum dengan memakai nama palsu dengan tipu muslihat ataupun rangkaian kebohongan menggerakkan orang lain untuk menyerahkan barang kepadanya, sebagaimana diatur dan diancam pidana dalam pasal 378 KUHP jo pasal 56 ayat 1 ke-1 KUHP.

Perbuatan itu dilakukan dengan cara: saksi saksi Ronal Harapan Maju Lubis bertemu dengan terdakwa meminta untuk dibuatkan website www.henbing.com, kemudian terdakwa menyanggupi untuk membuatkan website dimaksud, selanjutnya terdakwa membeli domain dan hosting dengan nama yang diinginkan saksi saksi Ronal Harapan Maju Lubis yang telah menunjukkan contoh website yang diperlihatkan kepada terdakwa yang telah dichatting. Kemudian terdakwa meng-upload konten image dan database ke website saksi Ronal Harapan Maju Lubis yang telah dipesan sebelumnya dengan mengubah tampilan logo dan menambah kata-kata ke website baru. Setelah jadi website itu jadi, terdakwa menghubungi saksi Ronal Harapan Maju Lubis melalui SMS bahwa website sudah jadi sekaligus memberikan login admin dan login control panel menggunakan serever e-padi network. Kemudian saksi Ronal Harapan Maju Lubis membayar terdakwa sebesar Rp 4.000.000,-.

Selanjutnya website www.henbing.com oleh saksi Ronal Harapan Maju Lubis dimaksud dengan tipu muslihat seolah-olah menjual barang secara *online* dengan menggunakan fasilitas internet banking di www.e-padi.com, emailnya order@henbing.com dengan password bujanginam yaitu menawarkan satu unit jetski Yamaha FX HO 160 HP tahun 2007 seharga US$ 19,520. Setelah barang dimaksud ditawarkan melalui internet ternyata saksi korban Chumpon Korp-Phaibun tertarik untuk membeli barang yang ditawarkan saksi Ronal Harapan Maju Lubis. Kemudian saksi korban melakukan beberapa komunikasi melalui email order@henbing.com maupun SMS kepada saksi Ronal Harapan Maju Lubis melalui nomor hp 08126534666. Saat itu saksi Ronal Harapan Maju Lubis mengaku bernama Robby Amalo, kemudian saksi korban sepakat membeli jetski dimaksud dan terdakwa meminta agar pembayaran ditransfer melalui rekening Bank Mandiri. Atas serangkaian kebohongan saksi Ronal Harapan Maju Lubis , tergeraklah hati saksi korban untuk mentransfer uang sejumlah US$ 19,520 kepada terdakwa sebanyak dua kali masing-masing pada tanggal 6 November 2007 sebesar US$ 4,520 melalui Bank Mandiri Tangerang no rekening 1280005127953 atas nama Robby Amalo dan pada tanggal 15 November 2007 sesesar US$ 15,000 melalui Bank Mandiri Jakarta no rekening 1280005156457 atas nama Salomo Harahap. Setelah menerima transfer dimaksud, saksi Ronal Harapan Maju Lubis mengambil uang itu melalui ATM BSD Pasar Modern Tangerang. Setelah menerima uang dari saksi korban, terdakwa tidak pernah mengirim barang yang dipesan saksi korban, sehingga akibat perbuatannya, saksi Ronal Harapan Maju Lubis telah memperoleh keuntungan sebsesar US$ 19,520. Uang itu habis dipergunakan untuk memenuhi kebutuhan hidup saksi Ronal Harapan Maju Lubis , sementara saksi korban telah menderita kerugian sebesar US$ 19,520 atau setidak-tidaknya lebih dari Rp 250,-.

2.3.5 Putusan Pidana Terhadap Ronal Harapan Maju Lubis

Atas tuntutan Penuntut Umum, melalui Putusan Nomor : 1964/ PID.B./ 2008/ PN/ TNG tanggal 10 November 2008, majelis hakim memutuskan :

a. Menyatakan terdakwa Ronal Harapan Maju Lubis terbukti secara sah dan meyakinkan bersalah melakukan kejahatan penipuan yang dilakukan secara berlanjut.
b. Menghukum terdakwa dengan hukuman penjara 1 tahun 8 bulan dikurangi masa tahanan.
c. Memerintahkan agar barang bukti berupa :
   1) 1 (satu) buah buku tabungan BNI Taplus atas nama Ronal Harapan Maju Lubis,
   2) 1 (satu) buah buku tabungan Mandiri atas nama Andi Firmansyah,
   3) 1 (satu) buah ATM BCA,
   4) 1 (satu) buah ATM Lippo Bank,
   5) 1 (satu) buah ATM BNI,
   6) 4 (empat) buah ATM Mandiri,
   7) 1 (satu) lembar SIM A,
   8) 2 (dua) lembar KTP,
   9) 1 (satu) lembar Log IP Henbing.com,
   10) 1 (satu) bundel print out data statistic,
   11) 4 (empat) keping kartu telepon simpati,
   12) 1 (satu) unit HP Nokia 9500,
   13) 1 (satu) unit HP Nokia 5300, dan
   14) 1 (satu) unit laptop merk Apple warna hitam.

   dirampas untuk negara.
d. Menghukum terdakwa untuk membayar ongkos perkara sebesar Rp 1000,- (seribu rupiah)
e. Memerintahkan terdakwa supaya tetap ditahan.

Hal yang memberatkan adalah sifat dari perbuatan tersebut dan perbuatan terdakwa meresahkan masyarakat. Sementara itu, hal yang meringankan adalah terdkwa belum pernah dihukum dan menaku terus terang dan bersikap sopan di persidangan.

2.3.6 Putusan Pidana Terhadap Devvy Bayu Prahastra

Atas tuntutan Penuntut Umum, melalui Putusan Nomor : 1965/ PID.B./ 2008/ PN/ TNG tanggal 10 November 2008, majelis hakim memutuskan

a. Menyatakan terdakwa Devvy Bayu Prahastra terbukti secara sah dan meyakinkan bersalah melakukan kejahatan penipuan secara bersama-sama
b. Menghukum terdakwa dengan hukuman penjara 1 tahun 8 bulan dikurangi masa tahanan.
c. Memerintahkan agar barang bukti berupa :
   1) 1 (satu) buah buku tabungan BCA atas nama Mario G,
   2) 1 (satu) buah buku tabungan BCA atas nama Herry S,
   3) 1 (satu) buah buku tabungan BCA atas Devvy BP,
   4) 1 (satu) buah buku tabungan BCA atas nama Supriyanti,
   5) 1 (satu) buah buku tabungan Mandiri atas nama Herry S,
   6) 1 (satu) buah buku tabungan Mandiri atas nama Devvy BP,
   7) 1 (satu) buah buku tabungan Britama atas nama Andini W,
   8) 4 (empat) buah ATM BCA,
   9) 1 (satu) buah ATM BRI,
   10) 3 (tiga) buah ATM Mandiri,
   11) 1 (satu) lembar SIM C,
   12) 1 (satu) lembar identitas sementara atas nama Devvy BP,
   13) 1 (satu) kartu anggota Ovida Video Rental Chain Shop,
   14) 1 (satu) keping kartu As,
   15) 1 (satu) keping kartu Explore
   16) 2 (dua) lembar form setoran Bank Mandiri,

   dirampas untuk dimusnahkan, sedangkan,

   17) 1 (satu) unit HP Samsung,
   18) 1 (satu) unit HP Nokia 2626,
   19) 1 (satu) unit laptop merk Sony Vaio.

   dirampas untuk negara.

d. Menghukum terdakwa untuk membayar ongkos perkara sebesar Rp 1000,- (seribu rupiah)

e. Memerintahkan terdakwa supaya tetap ditahan.

Hal yang memberatkan adalah sifat dari perbuatan tersebut dan perbuatan terdakwa meresahkan masyarakat. Sementara itu, hal yang meringankan adalah terdkwa belum pernah dihukum dan menaku terus terang dan bersikap sopan di persidangan.

2.4 Penerapan Undang-Undang ITE

Menurut Undang-Undang ITE, perbuatan yang dilakukan oleh Ronal dan Devvy merupakan pelanggaran terhadap pasal 28 ayat (1) undang-undang ini. Pasal itu melarang setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. Perbuatan ini diancam pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah). Jika dibandingkan dengan isi pasal 378 KUHP, undang-undang ini memiliki ancaman lebih besar ditambah dengan adanya ancaman pidana baru berupa denda.

Namun, kemajuan yang paling besar sesungguhnya adalah diterimanya informasi elektronik dan dokumen elektronik sebagai alat bukti yang sah sebagaimana ketentuan Pasal 5 Undang-Undang ITE, yang berbunyi:

(1) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

(2) Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia.

(3) Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini.

(4) Ketentuan mengenai informasi elektronik dan/atau dokumen elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

a. surat yang menurut undang-undang harus dibuat dalam bentuk tertulis; dan

b. surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Penegasan Undang-Undang ITE ini memberikan jawaban atas permasalahan mengenai keabsahan informasi dan dokumen elektronik sebagai alat bukti hukum yang sah. Penggunaan informasi dan dokumen elektronik sebagai alat bukti hukum sendiri tidak terbatas kepada penegakan hukum terhadap pasal-pasal pidana dalam Undang-Undang ITE, melainkan meliputi semua penegakan hukum dimana di dalamnya terdapat penggunaan sistem elektronik. Dari sisi pembuktian, aplikasi undang-undang ini juga lebih praktis, karena hasil cetak dari dokumen elektronik pun dapat diakui sebagai alat bukti yang sah (Wawancara dengan Raharjo Budi Kisnanto tanggal 5 Februari 2010).

Meskipun demikian, penerapan pasal pidana Undang-Undang ITE bukanlah tanpa masalah. Dari hasil wawancara dengan para nara sumber, peneliti juga menemukan adanya kemungkinan hambatan dalam penerapan yang berasal dari perbedaan penafsiran Undang-Undang ITE. Masalah pertama adalah anggapan bahwa undang-undang ini belum berlaku (Wawancara dengan Raharjo Budi Kisnanto tanggal 5 februari 2010). Anggapan ini disebabkan oleh penafsiran terhadap pasal 54 ayat 2 Undang-Undang ITE yang menyatakan keharusan adanya peraturan pemerintah dalam tempo sebagai peraturan pelaksana Undang-Undang ITE. Padahal tidak semua pasal Undang-Undang ITE mempersyaratkan adanya peraturan pelaksana. Bentuk penafsiran seperti ini bisa kita lihat dari pertimbangan putusan sela Prita Mulyasari oleh Pengadilan Negeri Tangerang. Setelah mendapat perlawanan dari penuntut umum, putusan sela ini dianulir Pengadilan Tinggi Banten yang menyatakan bahwa Undang-Undang ITE sudah berlaku.

Selain itu, penyidik menyatakan terkendala dengan rumusan pasal 43 ayat (6) Undang-Undang ITE yang mewajibkan penyidik melalui penuntut umum wajib meminta penetapan penangkapan dan penahanan dari ketua pengadilan negeri setempat dalam waktu satu kali dua puluh empat jam (Wawancara dengan I Ketut Budi Hendrawan tanggal 1 Maret 2010 ; Wawancara dengan Petrus Golose tanggal 12 Februari 2010). Atas dasar pasal ini penyidik setelah melakukan upaya paksa harus meminta penetapan Ketua Pengadilan Negeri guna sahnya tindakan hukum itu. Permasalahannya, penangkapan tidak selalu dilaksanakan pada hari kerja, melainkan bisa juga dilaksanakan pada hari libur. Terlebih lagi jika upaya paksa itu dilakukan di tempat terpencil yang sulit jalur transportasi dan komunikasinya. (Wawancara dengan I Ketut Budi Hendrawan tanggal 1 Maret 2010).

Hambatan karena tidak keluarnya penetapan upaya paksa ini pernah dialami AKBP Parmin ketika menyidik sebuah kasus perjudian *online*. Karena tidak berhasil mendapatkan penetapan penahanan dari ketua pengadilan tepat pada waktunya, ia harus melepaskan tersangka dalam kasus itu (Wawancara tanggal 13 April 2010). Oleh karena itu, penyidik lebih memilih menggunakan pasal-pasal KUHP apabila penyidik tidak cukup waktu meminta penetapan Ketua Pengadilan negeri atas penangkapan dan penahanan tersangka. Penyidik baru akan memilih menggunakan UU ITE apabila penyidik telah memiliki keyakinan kuat akan keluarnya penetapan Ketua Pengadilan Negeri terhadap upaya paksa yang dilakukannya (Wawancara dengan I Ketut Budi Hendrawan tanggal 1 Maret 2010, Wawancara dengan Parmin tanggal 13 April 2010). Preferensi ini juga tercermin dari data penanganan kasus *internet fraud* oleh Unit V/ IT & Cyber crime tahun 2008 dan 2009. Pada tahun 2008, dari empat kasus yang ditangani seluruhnya dikenakan pasal 378 KUHP. Sementara itu, dari sebelas kasus yang ditangani dalam 2009, hanya tiga yang dikenakan pasal undang-undang ITE. Observasi yang saya lakukan juga menguatkan temuan ini. Saya menemukan penyidik menerapkan pasal 378 KUHP terhadap kasus yang baru ditangani. Ketika saya mengkonfirmasikannya dengan si penyidik. Ia menyatakan tidak mudah untuk menerapkan Undang-Undang ITE karena adanya

aturan pasal 43 undang-undang itu (Wawancara dengan Sonar Sandina Mayasir tanggal 26 April 2010).

2.5 Penentuan Locus Delicti dan Yurisdiksi

Dalam masalah yurisdiksi, Undang-Undang ITE secara jelas menyebutkan yurisdiksinya meliputi setiap oang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ITE, 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. Sementara itu, jika mengacu pada KUHP, yurisdiksi harus didasarkan kepada asas-asas yang tercantum dalam pasal 2 sampai dengan pasal 5 KUHP.

Penyidik berkeyakinan yurisdiksi Indonesia bisa diterapkan terhadap kasus www.henbing.com dengan mengacu kepada asas teritorialitas. Keyakinan ini tercermin dalam wawancara tanggal 25 Januari 2010 dan wawancara tanggal 2 Februari 2010 dengan I Ketut Budi Hendrawan. Menurutnya, meskipun korban berkewarganegaraan Thailand dan mengakses situs dari Hongkong, tersangka Ronal mengupload situs yang digunakannya untuk menipu di wilayah Indonesia. Oleh karena itu berdasarkan prinsip teritorialitas, para tersangka dapat diadili dengan hukum Indonesia.

> Keyakinan penyidik ini erat dengan penentuan locus delicti perbuatan Ronal:
>
> "Locus delictinya bisa di Indonesia, karena di situ kan tempat dia melakukan penipuan, dia juga ditangkap di Indonesia, barang bukti kejahatan ditemukan di Jakarta, rekening tersangka juga berada di Jakarta" (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2002)

Keyakinan serupa juga dimiliki oleh penuntut umum. Terhadap Ronal, Raharjo menyatakan bahwa ia menerapkan teori perbuatan dalam menentukan locus delicti. Menurutnya, rumah Ronal adalah locus delicti karena di rumahnya inilah ia

menawarkan jetski kepada korban Di rumahnya pula lah ia melakukan komunikasi yang intens dengan sehingga korban mau mengirimkan sejumlah uang kepadanya (Wawancara dengan Raharjo Budi Kisnanto tanggal 5 Februari 2010).

Namun, teori berbeda diterapkan pada penentuan locus delicti bagi tersangka Devvy. Menurut Raharjo, dalam sebuah tindakan penyertaan yang didakwakan terhadap Ronal dan Devvy, kedua orang ini tidak perlu melakukan tindakan yang sama, melainkan cukup melakukan suatu rangkaian kegiatan dari beberapa orang yang memungkinkan terjadinya suatu kejahatan (Wawancara tanggal 15 Maret 2010) Devvy memang mendesain dan membuat website www.henbing.com di Denpasar, tetapi website itu digunakan oleh Ronal untuk menipu di Tangerang. Oleh karena itu berdasarkan teori akibat, rumah Ronal juga merupakan locus delicti perbuatan Devvy.

Agak sedikit berbeda, Raharjo Budi Kisnanto memberikan alternatif penggunaan asas nasionalitas aktif untuk menjerat para pelaku *fraud*. Ia berpendapat bahwa asas yang paling mudah diterapkan untuk mendakwa Ronal adalah asas nasionalitas aktif. Selama pelaku berkewarganegaraan Indonesia, ia dapat dituntut di muka pengadilan Indonesia, sebagaimana yang dikatakannya:

> "...nah kan begini kan ada beberapa asas dalam KUHP. Ada asas nasional, teritorialitas, universal, nah, itu kan begini, kita pake asas-asas yang ada dalam KUHP kita. Sehingga kok termasuk kewenangan mengadili. Di situ , kan kalo menentukan locus delicti kan ada beberapa teori locus delicti kan, ada, ada teori perbuatan, teori perencanaan, teori akibat. Tinggal mana yang kita pakai. Paling-paling kan nanti kalo di pengadilan kan dieksepsi penasehat hukum, karena kejadian di luar negeri, sehingga tidak bisa disidangkan di Indonesia. Nah mereka lupa asas nasional aktif, meskipun kejahatan terhadap orang, transaksinya di luar negeri dengan cara mentransfer duit ke Indonesia tapi dia kan melakukan perbuatnnya di sini.....kita pake teori yang lebih umum, kita, jaksa penuntut umum kan yang penting bagaimana supaya terdakwa bisa dituntut dan dibuktikan.....yang penting orang itu

warganegara Indonesia melakukan kejahatan, meskipun kejadiannya di luar negeri" (Wawancara tanggal 5 Februari 2010).

Penentuan locus delicti ini tentunya berpengaruh terhadap kewenangan Pengadilan Negeri Tangerang mengadili perkara ini. Jaksa meyakini bahwa Pengadilan Negeri Tangerang berhak mengadili perkara ini berdasarkan pasal 84 KUHAP (Wawancara dengan Raharjo Budi Kisnanto tanggal 5 Februari 2010 dan tanggal 15 Maret 2010).

Keyakinan bahwa perkara Ronal dan Devvy bisa diadili oleh Pengadilan Tangerang juga ditunjukkan oleh pernyataan Ismail, hakim ketua dalam persidangan perkara ini:

> ".....berwenangnya Pengadilan Negeri Tangerang memeriksa, mengadili perkara itu karena terdakwa bertempat tinggal di sini, itu satu, kemudian sebagian saksi-saksi juga ada di sini dan terdakwanya di tahan di sini kan. (Wawancara tanggal 16 Februari 2010).

Keyakinan hakim ini pada dasarnya merupakan penerapan ketentuan pasal 84 ayat (2) KUHAP yang berbunyi 'Pengadilan negeri yang di dalam daerah hukumnya terdakwa bertempat tinggal, berdiam terakhir, di tempat dia diketemukan, atau ditahan, hanya berwenang mengadili perkara tersebut, apabila tempat kediaman sebagian besar saksi yang dipanggil lebih dekat pada tempat pengadilan negeri itu daripada tempat kedudukan pengadilan negeri yang di dalam daerahnya itu tindak pidana dilakukan". Oleh karena itu, perkara kedua terdakwa masuk dalam kewenangan mengadili Pengadilan Negeri Tangerang.

2.6 Kendala dalam Penegakan Hukum

Selain permasalahan yang berkaitan dengan perundang-undangan, penyidik mengungkapkan adanya beberapa kendala teknis yang ditemui dalam penegakan hukum terhadap *internet fraud*. Kendala yang pertama berkaitan dengan anonimitas pelaku. Sebenarnya, ada beberapa hal yang dapat menjadi petunjuk identitas pelaku, yaitu alamat dan nomor telepon di situs, alamat pendaftaran di rumah hosting telepon,

dan nomor rekening bank. Namun, sudah barang tentu untuk menutupi jejak, baik alamat dalam situs maupun alamat yang diajukan untuk pendaftaran hosting bersifat fiktif. Namun, tidak demikian halnya dengan nomor telepon dan nomor rekening bank. Kedua nomor ini eksis dan digunakan oleh si pelaku. Rekening bank merupakan bagian yang sangat penting dalam sebuah kejahatan *internet fraud* karena diperlukan untuk menerima uang kiriman dari korbannya. Secara normatif, pembukaan rekening ini seharusnya diawali dengan pemberian data yang benar dari calon pembuka rekening dan oleh karena itu, dapat menjadi petunjuk berharga untuk pencarian pelaku. Sesuai pasal 42 Undang-Undang Perbankan, dalam rangka memperoleh keterangan mengenai simpanan tersangka, diperlukan izin Pimpinan Bank Indonesia, dengan berdasarkan permintaan tertulis dari Kapolri. Prosedur ini memakan waktu hingga kurang lebih 30 hari. Selain itu, hasil yang diperoleh biasanya tidak maksimal, karena lagi-lagi si pelaku menggunakan identitas dan alamat fiktif dalam pembukaan rekening (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2010).

Sementara itu, nomor telepon digunakan tidak hanya sebagai media komunikasi antara sebagai alat pelaku untuk meyakinkan calon korbannya. Dengan keberadaan nomor telepon yang bisa dihubungi, calon korban merasa sedang bertransaksi dengan pengusaha yang bonafide, meskipun setelah uang dikirim, nomor itu tidak dapat dihubungi lagi. Hampir serupa dengan permintaan keterangan mengenai rekening bank, permintaan keterangan kepada operator telepon juga membutuhkan waktu yang cukup panjang., Hal ini tentu menghambat jalannya pengungkapan kasus (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2010).

Kesulitan juga terjadi ketika penyidik membutuhkan informasi komunikasi pelaku yang terdapat dalam logfiles yang dimiliki rumah hosting. Penyimpanan logfiles sangat bergantung kepada kapasitas server. Pada umumnya kapasitas server rumah hosting di Indonesia belum begitu besar. Akibatnya, logfiles yang dibutuhkan penyidik sudah dihapus oleh server karena server tidak lagi mampu menampungnya.

Kehilangan "jejak" ini tentu menjadi kendala dalam pengungkapan kasus *cyber crime* (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2010).

Kesulitan selanjutnya berhubungan dengan pelaporan kasus. Dalam kasus *internet fraud* dengan korban berdomisili di luar negeri, korban hanya melaporkan kasusnya kepada kepolisian setempat atau perwakilan RI di negaranya. Padahal, untuk terpenuhinya persyaratan penegakan hukum lebih lanjut, diperlukan adanya laporan polisi dan berita acara pemeriksaan. Diperlukan biaya yang sangat besar jika harus pergi ke tempat korban untuk mendapatkan dua dokumen tadi. Apalagi jika kerugian tidak terlalu besar, pemeriksaan korban di luar negeri tentu tidak efisien. (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2010).

Ketut Budi juga memberikan contoh lain tidak berjalannya penegakan hukum terhadap *internet fraud* tanpa adanya laporan resmi. Dari hasil penyelidikan dan penyidikan kasus www.henbing.com, diketahui bahwa ada pelaku lain yang tinggal serumah dengan Ronal. Namun, karena tidak ada korban yang mau melapor, penyidik tidak dapat melakukan tindakan hukum terhadapnya. Kejadian serupa juga terjadi dalam kasus yang melibatkan pelaku seorang siswa sebuah sekolah aviasi. Dalam kasus ini ada korban yang mau menceritakan kasusnya dan bahkan memberikan petunjuk identitas pelaku. Namun, ia tidak mau membuat laporan resmi. Akibatnya tidak ada penegakan hukum terhadap kejahatan yang ia lakukan (Wawancara tanggal 1 Maret 2010).

Ketika ditanya kemungkinan penggunaan laporan polisi model A dimana penyidik membuat laporan polisi sendiri setelah menerima laporan dugaan adanya kejahatan dari korban, Ketut Budi menyatakan bahwa hal itu pernah dilakukan, namun, sekarang tidak lagi dengan alasan kebijakan pimpinan (Wawancara tanggal 1 Maret 2010). Sementara itu terhadap pelaporan *online* sebagaimana saran hasil penelitian Andi Mochammad Dicky, Kombes Pol Petrus Golose menolaknya dengan dasar prinsip kehati-hatian. Menurutnya kita tidak bisa mengetahui apakah laporan itu benar, baik identitas pelapor maupun isi laporannya itu (Wawancara tanggal 12 Februari 2010).

Kesulitan selanjutnya adalah jumlah petugas yang tidak sebanding dengan jumlah kasus yang sebenarnya. Setiap saat, Unit Cyber Crime mendapatkan laporan, tetapi tidak semua bisa dilanjutkan ke tingkat penyelidikan karena kurangnya personel. Selain itu, dari observasi peneliti selama penelitian, unit ini tidak pernah lengkap. Hal ini disebabkan karena para petugas ini harus mengikuti berbagai kegiatan di luar kantor, baik itu yang berhubungan dengan *cyber crime* itu sendiri, seperti pelatihan, penyelidikan dan penyidikan atau hal-hal lain yang tidak berhubungan dengan kasus *cyber crime* seperti penanganan terorisme.

Sementara itu, dari penanganan kasus www.henbing,com, terlihat bahwa pengalaman para aparat penegak hukum menangani kasus *cyber crime* cukup beragam. Sebagai anggota unit khusus yang menangani masalah *cyber crime*, para penyidik telah berkali-kali menangani kasus *cyber crime* (Wawancara dengan I Ketut Budi Hendrawan tanggal 2 Februari 2010; Wawancara dengan Maryudi Salempang tanggal 1 April 2010). Para penyidik juga telah berulang kali mengikuti pelatihan dalam rangka peningkatan kemampuan penanganan kasus *cyber crime*. Hal ini berbeda dengan pengalaman para aparat penegak hukum yang lain. Dari dua jaksa penuntut umum dalam kasus ini, Raharjo Budi Kisnanto dan Faisal Adhi, Raharjo memiliki pengalaman yang lebih baik dibandingkan koleganya, Faisal. Selain menangani penuntutan Ronal dan Devvy, Raharjo telah melakukan penuntutan terhadap dua terdakwa lain, yaitu Toni Dewayanto dan Prita Mulyasari. Ia juga telah mengikuti beberapa kegiatan peningkatan kemampuan penanganan kasus *cyber crime*, baik berupa pelatihan maupun seminar (Wawancara tanggal 5 Februari 2010). Sementara itu, bagi Faisal Adhi, penuntutan kasus www.henbing.com adalah satu-satunya pengalamannya menangani kasus *cyber crime*. Ia sendiri belum pernah mengikuti kegiatan khusus dalam rangka peningkatan kemampuan penanganan kasus *cyber crime* (Wawancara tanggal 16 Februari 2010). Demikian pula halnya bagi Ismail, penanganan kasus www.henbing.com adalah satu-satunya pengalaman mengadili kasus yang berhubungan dengan *cyber crime* (Wawancara tanggal 17 Februari 2010).

Selain itu, penegakan hukum terhadap *cyber crime* identik dengan penggunaan bukti digital. Pengumpulan bukti digital ini akan sangat bergantung kepada sarana *computer forensic* yang dimiliki oleh penegak hukum. Saat ini di Indonesia terdapat empat laboratorium *computer forensic* yang berlokasi di Polda Sumatra Utara, Polda Jawa Timur, Polda Metro Jaya dan Unit V/ IT& Cyber Crime Bareskrim Polri. Jumlah ini dirasakan kurang optimal jika harus meliputi seluruh wilayah Indonesia. Belum lagi jika dihubungkan dengan proses pengolahan data digital itu sendiri. Suatu proses pengolahan data harus selesai secara sempurna dahulu barulah komputer yang digunakan untuk mengolah data, dapat digunakan lagi (Wawancara dengan Alexander Sabar tanggal 16 April 2010).

Selain itu, dalam penolahan bukti digital, bukan hanya *hardware* yang dibutuhkan. Pengolahan data juga memerlukan *software* yang digunakan sebagai *tools* dalam proses itu. *Tools* tadi dibeli dari perusahaan penyedia dan dapat diperbaharui selama lisensi kepemilikannya berlaku. Masalah akan timbul jika lisensinya mati, *tools* tadi tidak akan bisa lagi digunakan. Masalah semacam ini telah terjadi pada *software* pemroses data telepon seluler, sementara tidak pernah ada anggaran yang dialokasikan khusus untuk pembelian *tools* itu (Wawancara dengan Alexander Sabar tanggal 16 April 2010).

BAB 3

KERJASAMA INTERNASIONAL DALAM PENEGAKAN HUKUM

3.1 Permohonan Bantuan Penegakan Hukum terhadap Internet Fraud

Sesuai karakternya yang nampu melintas batas negara, kerjasama internasional merupakan sesuatu yang esensial dalam penanganan kasus *cyber crime*. Solusi domestik saja tidak cukup karena ruang siber tidak memiliki batas baik secara geografis maupun politis. Hampir semua sistem komputer dapat diakses secara mudah dan secara rahasia dari semua belahan dunia. (Audal, Lu dan Roman 2008, 271). Akibatnya, korban dan pelaku bisa jadi berlokasi di yurisdiksi negara yang berbeda. Perbedaan ini akan semakin rumit dengan adanya perbedaan konsepsi dan legislasi masing-masing negara terhadap *cyber crime*. Guna mereduksi akibat dari permasalahan ini, semua negara sepakat untuk melaksanakan kerjasama baik dengan memberdayakan bentuk-bentuk kerjasama dalam penegakan hukum terhadap kejahatan yang telah ada sebelumnya, maupun dengan menciptakan bentuk kerjasama yang baru dan spesifik mengenai *cyber crime.*

Penegakan hukum terhadap *internet fraud* yang dilakukan oleh Indonesia. pun tidak akan terlepas dari kerjasama internasional. Indonesia akan sangat mungkin harus berhubungan dengan negara lain karena keterlibatan warga negaranya, baik sebagai pelaku maupun sebagai korban. Dalam kasus warga negara Indonesia sebagai korban *fraud*, Indonesia akan meminta bantuan kepada negara tempat pelaku berdomisili untuk melakukan penindakan terhadap warganya itu. demikian pula sebaliknya, negara asal korban akan meminta bantuan Indonesia untuk melakukan penindakan terhadap warga negara Indonesia yang telah menipu warga negaranya. Sesuai asas resiprositas dalam hubungan internasional, apa yang dilakukan oleh Indonesia dalam menangani warga negara Indonesia yang diduga merugikan warga negara lain, akan berimplikasi terhadap apa yang akan diterima Indonesia ketika meminta bantuan serupa dari negara itu.

Secara ringkas, ada tiga jalur permohonan bantuan dalam penegakan hukum yaitu melalui (Wawancara dengan Dadang Sutrasno tanggal 25 Januari 2010) :

a. Jalur interpol, melalui Sekretariat Jenderal ICPO-Interpol atau dengan sarana I-24/7, surat dan faksimili.
b. Jalur Diplomatik, dengan alur
    1) NCB-Interpol Indonesia- KemkumHAM-Kemlu-Negara Tujuan
    2) NCB-Interpol Indonesia-Perwakilan Republik Indonesia di negara tujuan-Negara tujuan
    3) NCB-Interpol Indonesia-Perwakilan negara tujuan di Indonesia-Negara tujuan
c. Jalur informal antar aparat penegak hukum.

Melalui jalur kerjasama tadi, banyak keluhan yang diterima oleh polri melalui NCB-Interpol yang berkaitan dengan kasus-kasus penipuan melalui internet. Laporan yang diterima oleh NCB itu kemudian disalurkan kepada kesatuan-kesatuan yang berwenang naik itu ditingkat Mabes Polri mapun pada kepolisian daerah. (Wawancara dengan Dadang Sutrasno tanggal 25 Januari 2010). Setelah laporan itu ditindaklanjuti, Indonesia akan memberitahukan hasil penindakannya kepada negara peminta bantuan.

Salah satu bentuk permohonan bantuan yang berkaitan dengan kasus www.henbing.com adalah Berita Faksimil beromor RR-027/Athena/III/08 tanggal 14 Maret 2008 dari Kedutaan Besar Republik Indonesia di Athena. Surat itu berisikan enam pengaduan yang dibuat oleh para pengusaha Yunani yang mengaku menjadi korban penipuan yang dilakukan baik oleh beberapa perusahaan penyedia barang di Indonesia. Para pengusaha tadi menjadi korban penipuan setelah bertransaksi bisnis dengan perusahaan yang tertera dalam situs www.alibaba.com. Menurut mereka, para pelaku penipuan mewajibkan mereka untuk membayar uang muka melalui nomor rekening yang ditentukan dan berjanji akan segera mengirimkan barang sesegera mungkin setelah uang muka diterima. Pada kenyataannya, setelah uang muka dikirimkan, barang sama sekali tidak dikirimkan. Sementara itu, komunikasi dengan perusahaan penyedia barang terhenti karena tidak dapat lagi dihubungi baik melalui

telepon dan email, bahkan situs-situsnya tidak dapat diakses lagi. Salah seorang dari pelapor, Nanouris Bill memesan radio Raptor 90 Se RTF seharga US$ 460,- kepada CV Dua Arena Toys melalui order@henbing.com.

3.2 ICPO-Interpol

Bentuk kerjasama internasional dalam penegakan hukum yang paling populer adalah kerjasama yang dilaksanakan dalam kerangka organisasi International Criminal Police Organization (ICPO-Interpol). Saat ini, ICPO-Interpol tidak hanya merupakan organisasi kerjasama penegakan hukum terbesar di dunia, melainkan juga merupakan organsiasi terbesar kedua di dunia setelah Perserikatan Bangsa-Bangsa dengan 188 negara anggotanya. Organisasi yang bermarkas di Lyon, Perancis saat ini dipimpin oleh Commissioner of Police Khoo Bun Hui, mantan Kepala kepolisian Republik Singapura dengan Ronald Noble dari Amerika Serikat sebagai sekretaris jenderal. Organisasi ini dibentuk atas dasar pertimbangan akan pererkembangan kejahatan yang mampu melewati batas negara dimana seorang tersangka mampu melarikan diri ke luar wilayah negara tempat ia melakukan suatu kejahatan atau pengaruh kejahatan yang dilakukannya dapat dirasakan di luar negeri.. Tujuan utama organisasi ini adalah memastikan dan meningkatkan bantuan timbal balik antar institusi kepolisian dan berupaya untuk meningkatkan peran serta mereka dalam pencegahan dan penekanan angka kejahatan tanpa melakukan intervensi terhadap kegiatan-kegiatan militer, politik agama dan ras (Pasal 2 dan Pasal 3 Konstitusi ICPO-Interpol). Untuk mencapai tujuan itu, negara-negara anggota ICPO-Interpol dengan difasilitasi sekretariat jenderal melakukan kegiatan pertukarain informasi kejahatan, penyusunan database, permohonan bantuan penegakan hukum, asistensi dalam penanganan keadaan krisis, pelatihan-pelatihan serta berbagai kegiatan lainnya. Salah satu bentuk permohonan bantuan yang sangat terkenal dari ICPO-Interpol adalah penerbitan *Interpol Notices*, yang terdiri dari

a. *red notice,* untuk meminta bantuan pencarian buronan
b. *blue notice,* untuk meminta informasi

c. *green notice*, untuk memberi peringatan akan orang yang dicurigai
d. *yellow notice*, untuk meminta bantuan pencarian orang hilang
e. *black notice*, untuk memberitahukan penemuan mayat yang ditemukan tanpa identitas.

Sebagai organisasi penegakan hukum, ICPO-Interpol tentunya terus mengikuti trend perkembangan kejahatan. Salah satu upaya yang dilakukannya adalah menentukan enam area kejahatan sebagai prioritas, yaitu:

a. *Drugs and criminal organizations. Tacling the growing problem of drug sbuse and trafficking, ofeten linked to othe crimes.*
b. *Financial and high-tech crime. Combatting counterfeiting, payment card fraud, intelectual property and cyber-crime.*
c. *Fugitives. Tarcking fugitives, who threaten publuc safety and undermine criminal justice systems.*
d. *Public safety and terrorism. Countering terrorism, which theratens public safety aand world security*
e. *Trafficking in human beings. Fighting abuse and exploitation of people which breach human rights and destroy lives.*
f. *Corruption. Towards a corrpution-free world by promoting and defending integrity, justice and rule of law.*

Dalam area kejahatan *financial and high-tech crime* di atas kita menemukan *cyber crime* menjadi salah satu prioritas kerjasama penegakan hukum. Hal ini disebabkan teknologi yang digunakan dalam kejahatan ini memberi banyak kesempatan bagi para pelaku kejahatan untuk melakukan kejahatan finansial tradisional dalam kemasan yang baru. Oleh karena itu, berbagai kegiatan telah dilakukan untuk mengeliminasi atau minimal mereduksi kejahatan ini. Tidak hanya melalui pertukaran informasi dan pelatihan melainkan juga melalui Pertemuan Kelompok Kerja para para penegak hukum. Pertemuan ini tidak hanya sebagai ajang berbagi informasi secara atau peningkatan kemampuan para penegak hukum saja, melainkan juga sebagai sarana untuk merumuskan kerjasama ke depan sekaligus sebagai ajang temu muka secara langsung guna mempererat hubungan antar penegak

hukum. Kerjasama dan koneksi antar penegak hukum ini sangat penting mengingat karakteristik cyber-crime yang mampu melintasi batas negara.

Dalam aktivitas organisasi ICPO-Intepol, Indonesia diwakili oleh Polri. Hal ini erat kaitannya dengan status Polri sebagai pelaksana *National Central Bureau* (NCB) ICPO-Interpol di Indonesia. Sesuai pasal 32 Konsitusi Interpol, NCB yang dibentuk pada masing-masing negara untuk bertindak sebagai *permanent central point* di tingkat nasional guna menjamin hubungan dengan instansi pemerintah terkait di dalam negeri, NCB-NCB negara lain serta Sekretariat Jenderal ICPO-Interpol. Polri sendiri mendapatkan status sebagai NCB-Interpol Indonesia berdasarkan Surat Keputusan Perdana Menteri No 245/PM/1954 tanggal 5 Oktober 1954, pemerintah menunjuk Jawatan Kepolisian Negara sebagai NCB untuk mewakili pemerintah RI di dalam organisasi kepolisian kriminal internasional dan Kepala Kepolisian Negara sebagai kepalanya. Tugas NCB ini dirumuskan sebagai berikut:

a. tukar-menukar informasi kriminal dengan NCB negara lain
b. memberikan bantuan penyelidikan/penyidikan sesuai dengan permintaan dari dalam dan luar negeri.
c. melaksanakan international public service.
d. ikut aktif melaksanakan agenda kegiatan ICPO-Interpol

Dalam melaksanakan tugasnya memberikan bantuan dalam penegakan hukum NCB-Interpol Indonesia berperan sebagai fasilitator. NCB akan melakukan pendampingan baik kepada penyidik Polri yang membutuhkan bantuan dari kepolisian negara asing maupun sebaliknya. Asistensi semacam ini biasanya diberikkan bila hubungan Indonesia dengan kepolisian negara tujuan cukup erat. Adakalanya, meskipun hubungan dengan kepolisian negara itu cukup erat, prosedur yang berlaku di negara itu melarang pemberian bantuan secara langsung melainkan harus melalui prosedur resmi seperti ekstradisi maupun bantuan hukum timbal balik. Di sini peran NCB adalah memfasilitasi serta memberi asistensi pemenuhan syarat-syarat dan prosedur dalam ekstradisi dan bantuan hukum timbal balik. Demikian pula halnya ketika Indonesia dimintai bantuan yang serupa, NCB akan menyalurkan

permohonan bantuan yang diterima melalui Kementrian Hukum dan HAM kepada kesatuan kepolisian yang berkompeten.

Selain itu, sebagai *focal point* Interpol di Indonesia, NCB juga berkoordinasi dan beketjasama dengan para pemangku kepentingan dalam penegakan hukum lainnya, khususnya instansi-instansi yang juga memiliki kewenangan dalam penyidikan tindak pidana. Koordinasi ini diwadahi dalam sebuah tim yang disebut Tim Koordinasi Interpol. Tim ini pertama kali dibentuk berdasarkan Surat Keputusan Kapolri No.Pol : Skep/203/V/1992 tanggal 9 Mei 1992 dan diperbaharui dengan Surat Keputusan Kapolri No.Pol : Skep/628/XII/2007 tanggal 27 Desember 2007. Selain Polri, instansi lain yang ikut serta dalam tim ini adalah instansi yang juga memiliki kewenangan penegakan hukum seperti Bank Indonesia, TNI AL, Perum Peruri, KemHum dan HAM, Kemkeu, Kemlu, Kementrian Pemberdayaan Perempuan dan Perlindungan Anak, Kejagung, Badan POM, Kemkominfo, Kemdag, Kemnaker, Botasupal, Kemhub, BIN, PPATK dan KPK.

3.3 ASEANAPOL

Organisasi Aseanapol (Asean Chiefs Of Police Meeting) berawal dari Sidang Umum ICPO-Interpol ke-49 November 1980 di Manila, Filipina. Di sela-sela pertemuan itu, para kepala kepolisian wilayah Asia Tenggara mengadakan pertemuan informal tersendiri. Dalam pertemuan informal itu, terlontar gagasan untuk menyelenggarakan konferensi tahunan di antara negara-negara ASEAN. Gagasan ini disambut baik oleh para pimpinan kepolisian negara-negara ASEAN yang saat itu terdiri dari Indonesia, Malaysia, Filipina, Singapura dan Thailand.

Atas inisiatif Letnan Jenderal Fidel V. Ramos dari Filipina, tanggal 20-24 Oktober, lima kepala kepolisian negara-negara ASEAN mengadakan pertemuan Aseanapol pertama. Dari Indonesia, hadir Letnan Jenderal Polisi Sabar yang mewakili Kapolri saat itu, Jenderal Polisi Awaludin Djamin. Sementara itu, dari Malaysia hadir Tan Sri Mohammad Hanief Bin Omar, sedangkan Singapura diwakili

oleh Komisaris Goh Yong Hong dan Thailand diwakili oleh Jenderal Polisi Surapon Chulabrahm.

Sebelum pembentukan Aseanapol, kerjasama Interpol antara negara-negara ASEAN sudah berjalan dengan baik. Namun, tampaknya kerjasama yang sudah ada belum efektif sehingga dibutuhkan suatu bentuk kerjasama regional. Para kepala kepolisian negara-negara ASEAN berpendapat, kerjasama tingkat Asia yang sudah ada saat itu terlalu luas. Selain itu karakteristik kejahatan di kawasan Asia Tenggara bersifat unik dan bisa jadi berbeda dengan kejahatan di wilayah lainnya. Oleh karena itu, mereka sepakat untuk untuk membentuk Aseanapol sebagai forum kerjasama dalam lingkup yang lebih sempit. Adapun tujuan Aseanaopol adalah

a. penanggulangan kejahatan internasional di kawasan ASEAN,
b. tukar menukar informasi kriminal secara cepat dan tepat,
c. *hot pursuit* terhadap penjahat yang melintas batas,
d. tukar menukar pesonel dalam rangka saling mengenal dan menimba pengalaman satu sama lain,
e. kerjasama di bidang pendidikan dan teknologi kepolisian.

Saat ini anggota Aseanapol berjumlah sepuluh negara sesuai dengan keanggotaan ASEAN. Berdasarkan urutan abjad dalam bahasa Inggris, negara-negara itu adalah Brunei Darussalam, Kamboja, Indonesia, Laos, Malaysia, Myanmar, Filipina, Singapura, Thailand dan Vietnam. Sekretariat Aseanapol sebagai pusat korrdinasi kerjasama ini didirikan pada tahun 2009 dan bertempat di Kuala Lumpur.

Aseanapol telah merumuskan 8 kejahatan yang menjadi prioritas kerjasamanya, yaiu

a. *terrorism*
b. *illicit drugs trafficking*,
c. *fraudulent travel documents*,
d. *human trafficking*,
e. *commercial crimes* (*bank offence and credit card frauds*),
f. *maritime frauds*,
g. *products counterfeiting*,

h. *cyber crime*.

3.4 AMMTC

Dalam pertemuan tingkat tinggi pada tahun 1997 di Manila, negara-negara ASEAN menyepakati deklarasi ASEAN tentang pemberantasan kejahatan transnasional. ASEAN menyetujui peningkatan kerjasama di antara negara-negara ASEAN melalui pembentukan forum khusus pembahasan kejahatan transnasional yang dinamakan ASEAN Ministerial Meeting on Transnational Meeting on Transnational Crime (AMMTC) yang bersidang setiap dua tahun. Sementara itu, di tingkat pejabat pelaksana di bawah AMMTC dibentuk forum Senior Official Meeting on Transnational Crime (SOMTC) yang mengadakan pertemuan rutin tiap tahun. Forum ASEAN ini difokuskan pada pertukaran informasi, pengalaman, bantuan teknis dan forum kerjasama diantara negara-negara anggota ASEAN. Secara rutin, forum dimanfaatkan pula untuk berdialog dengan negara mitra dialog seperti Cina, Korea, Jepang, Amerika Serikat, Australia,

Dalam deklarasi tahun ASEAN menyetujui enam jenis kejahatan transnasional yang menjadi prioritas kerjasama yaitu *terrorism, money laundering, drug trafficking, arms smuggling, sea piracy*, serta *trafficking in person (especially women and children.* Pada sidang AMMTC ke-3 di Singapura tahun 2001, kerjasama diperluas dengan memasukkan *cyber crime* dan *international economic crime* sebagai bagian dari ruang lingkup kerjasama AMMTC.

Salah satu bentuk nyata dari kerjasama AMMTC dalam penanganan *cyber crime* adalah penyelenggaraan *Workshop On Enhancing Cyber Crime Investigation Capacity Of Asean Law Enforcement Agencies* di Bandung tanggal 5-6 November 2009. Dalam lokakarya yang dilaksanakan atas kerjasama dengan pemerintah Republik Korea ini, para penegak hukum dari negara-negara ASEAN meningkatkan kemampuan penyidikan melalui tukar menukar pengalaman, keahlian dan pengetahuan dalam proses, cara, serta teknik-teknik penyidikan cyber crime.

3.5 Ekstradisi

Definisi ekstradisi menurut Undang-Undang nomor 1 tahun 1979 adalah penyerahan oleh suatu negara kepada negara yang meminta penyerahan seseorang yang disangka atau dipidana karena melakukan suatu kejahatan di luar wilayah negara yang menyerahkan dan di dalam yurisdiksi wilayah negara yang meminta penyerahan tersebut karena berwenang untuk mengadili dan memidananya.

Ekstradisi sendiri tunduk kepada beberapa azas yaitu:

a. Asas kejahatan rangkap, yaitu perbuatan yang dilakukan baik oleh negara peminta maupun oleh negara yang diminta dianggap sebagai kejahatan (Pasal 4)
b. Asas jika suatu kejahatan tertentu oleh negara yang diminta dianggap sebagai kejahatan politik, maka permintaan ekstradisi ditolak (pasal 5)
c. Asas bahwa negara yang diminta mempunyai hak untuk tidak menyerahkan warganegaranya sendiri (pasal 7)
d. Asas bahwa suatu kejahatan yang telah dilakukan seluruhnya atau sebagian di wilayah yang termasuk atau dianggap termasuk dalam yurisdiksi negara yang diminta, mp orang yang aka negara ini dapat menolak permintaan ekstradisi (pasal 8)
e. Asas bahwa suatu permintaan ekstradisi dapat ditolak jika pejabat yang berwenang dari negara yang diminta sedang mengadakan pemeriksaan terhadap orang yang bersangkutan mengenai kejahatan yang dimintakan penyerahannya (pasal 9)
f. Asas bahwa apabila terhadap suatu kejahatan tertentu, suatu keputusan yang telah mempunyai kekuatan pasti telah dijatuhkan oleh pengadilan yang berwenang dari negara yang diminta, permintaan ekstradisi ditolak (pasal 10)
g. Asas bahwa seseorang tidak diserahkan karena hak untuk menuntut atau hak untuk melaksanakan putusan pidana telah kadaluwarsa (pasal 12)

h. Asas bahwa seseorang yang diserahkan tidak akan dituntut, dipidana atau ditahan untuk kejahatan apa pun yang dilakukan sebelum yang bersangkutan diekstradisikan selain daripada untuk kejahaan untuk mana ia diserahkan, kecuali bila negara yang diminta untuk menyerahkan orang itu mnyetujuinya.

Saat ini Indonesia telah memiliki perjanjian ekstradisi dengan enam negara, yaitu

a. Malaysia, yang disahkan dengan undang-undang nomor 9 tahun 1974
b. Philipina, yang disahkan dengan undang-undang nomor 10 tahun 1976
c. Thailand, yang disahkan dengan undang-undang nomor 2 tahun 1978
d. Australia, yang disahkan dengan undang-undang nomor nomor 8 tahun 1994
e. Hong Kong, yang disahkan dengan undang-undang nomor 1 tahun 2001
f. Korea Selatan, yang disahkan dengan undang-undang nomor 42 tahun 2007

Dalam hal permintaan bantuan ekstradisi ada beberapa kasus yang menarik untuk dicermati. Salah satunya adalah kasus pembunuhan yang dilakukan oleh Harnoko Dewanto (Oki) . Pada tahun 1995, kepolisian Los Angeles (LAPD) menemukan mayat dua warga negara Indonesia dan seorang warga negara India. Penyidikan LAPD menghasilkan dugaan tersangka terhadap Harnoko Dewanto (Oki) yang pada saat itu telah kembali ke Indonesia. LAPD kemudian menginformasikan kasus ini kepada Polri dengan maksud meminta bantuan penangkapan dan penahanan tersangka serta ekstradisi Oki. Namun, Oki adalah warganegara indonesia. Oleh karena itu, pemerintah Republik Indonesia tidak memenuhi permintaaan itu. Pemerintah Republik Indonesia bahkan meminta LAPD untuk meminjamkan barang bukti. Akhirnya, dengan kerjasama yang baik antara kedua institusi kepolisian, LAPD bersedia menyerahkan barang bukti kepada Polri yang kemudian berhasil mengajukannya ke meja persidangan. Ada dua hal yang menarik di sini. Yang pertama adalah berlakunya asas ekstradisi tidak menyerahkan warga negaranya kepada negara lain. Hal kedua yang lebih menarik adalah berlakunya asas

f. melaksanakan permintaan penggeledahan dan penyitaan;
g. perampasan hasil tindak pidana;
h. memperoleh kembali sanksi denda berupa uang sehubungan dengan tindak pidana;
i. melarang transaksi kekayaan, membekukan aset yang dapat dilepaskan atau disita, atau yang mungkin diperlukan untuk memenuhi sanksi denda yang dikenakan, sehubungan dengan tindak pidana;
j. mencari kekayaan yang dapat dilepaskan, atau yang mungkin diperlukan untuk memenuhi sanksi denda yang dikenakan, sehubungan dengan tindak pidana; dan/atau
k. bantuan lain yang sesuai dengan Undang-Undang no 1 tahun 2006.

Saat ini Indonesia telah memiliki kerjasama bantuan timbal balik dalam maslah pidana dengan lima negara, yaitu

a. Amerika Serikat,
b. Australia,
c. China,
d. Korea Selatan,
e. Hongkong

3.7 Konvensi-Konvensi Internasional

Saat ini terdapat beberapa konvensi internasional yang mengatur *cyber crime*. Meskipun dalam konvensi-konvensi itu, Indonesia tidak selalu menjadi negara pihak, aturan-aturan dalam konvensi dapat dijadikan acuan bagi Indonesia dalam melaksanakan penindakan terhadap *cyber crime*. Di antara konvensi-konvensi itu terdapat dua konvensi yang paling sering dijadikan pedoman dalam penindakan terhadap *cyber crime* yaitu Convention on Cyber Crime dan United Nation Convention Against Transnational Organized Crime

nasionalitas aktif kepada warganegara Indonesia meskipun ia melakukan perbuatan kejahatannya di luar negeri.

Kasus lainnya adalah kasus pembunuhan di Pantai Gading. Kasus pembunuhan ini terjadi pembunuhan yang terjadi di atas kapal berbendera Honduras yang sedang berlabuh di Afika Barat. Baik pelaku dan korban adalah awak kapal itu yang berkewarganegaraan Indonesia. Oleh kapten kapal, tersangka, korban dan barang bukti diserahkan kepada Pemerintah Pantai Gading sebagai penguasa terdekat. Pemerintah Indonesia selanjutnya meminta agar tersangka diekstradisi ke Indonesia. Meskipun sempat terhambat, tersangka dapat diserahkan kepada Pemerintah Indonesia. Sayangnya, barang bukti tidak diserahkan, sehingga penegakan hukum terhadap kasus itu harus dihentikan. Dari kasus ini ada dua hal yang patut menjadi catatan. Selain berlakunya asas nasionalitas aktif, kita dapat menemukan kendala penegakan hukum apabila barang bukti yang berada di luar negeri tidak diserahkan kepada Pemerintah Indonesia.

3.6 Bantuan Timbal Balik dalam Perkara Pidana

Bentuk kerjasama yang dapat digunakan untuk meminta bantuan penyerahan barang bukti adalah melalui bantuan timbal balik dalam masalah pidana atau yang lebih dikenal sebagai *mutual legal assistance*. Undang-undang nomor 1 tahun 2006 telah mengatur ruang lingkup bantuan itu meliputi permintaan bantuan berkenaan dengan penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan sesuai dengan ketentuan peraturan perundang-undangan Negara Diminta.

Bantuan itu dapat berupa:

a. mengidentifikasi dan mencari orang;
b. mendapatkan pernyataan atau bentuk lainnya;
c. menunjukkan dokumen atau bentuk lainnya;
d. mengupayakan kehadiran orang untuk memberikan keterangan atau membantu penyidikan;
e. menyampaikan surat;

3.7.1 Convention on Cyber Crime

Pada 23 November 2001 di Budapest, Hongaria, 30 negara Eropa sepakat untuk menandatangani Convention on Cybercrime. Konvensi ini merupakan kerjasama multilateral yang diadakan guna menanggulangi penyebaran aktivitas kriminal melalui internet dan jaringan komputer lainnya. Melalui kerjasama ini diharapkan dapat menggugah masyarakat internasional untuk ikut berpartisipasi dalam penanggulangan kejahatan berteknologi tinggi. Meskipun konvensi ini digagas oleh Uni Eropa, tidak tertutup kemungkinan bagi negara di luar Eropa untuk turut serta menadi negara pihak.

Dalam konvensi ini, negara-negara pihak setuju untuk mengdopsi ke dalam perundang-undangan nasionalnya, aturan-aturan tentang kejahatan terhadap kerahasiaan, integritas dan ketersedian data dan sistem komputer, kejahatan yang berhubungan dengan komputer, kejahatan yang berhubungan dengan konten, serta kejahatan yang berhubungan dengan hak cipta. Rumusan inilah yang diadopsi oleh Undang-Undang ITE dalam mendefinisikan kejahatan yang berhubungan dengan informasi dan transaksi elektronik.

Mengenai yurisdiksi, konvensi ini mengamanatkan para negara pihak untuk menerapkan yurisdiksi terhadap kejahatan-kejahatan yang disebutkan sebelumnya, ketika kejahatan itu dilakukan

a. Dalam teritorinya
b. Dalam perjalanan di atas kapal laut berbendera negara pihak
c. Dalam perjalanan di atas pesawat terbang yang didaftarkan di bawah perundang-undangan negara pihak
d. Oleh salah seorang warga negaranya, jika kejahatan itu dapat dipidana berdasarkan hukum pidana di tempat ia melakukan kejahatan atau jika kejahatan itu dilakukan di luar yurisdiksi teritorial negara manapun.

3.7.2 United Nation Convention Against Transnational Organized Crime

PBB telah mensahkan United Nation Convention Against Transnational Organized Crime (UNCATOC) atau yang dikenal dengan sebutan Palermo Convention pada *plenary meeting* ke-62 tanggal 15 November 2000. Konvensi ini memiliki empat (4) protokol yaitu

a. United Nations Convention against Transnational Organized Crime,
b. Protocol against the Smuggling of Migrants by Land Air and Sea, supplementing the United Nations Convention against Transnational Organized Crime,
c. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime,
d. Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing United Nations Convention against Transnational Organized Crime.

Konvensi ini berhubungan erat dengan konsep *transnational crime* sebagai tindak pidana atau kejahatan yang melintasi batas negara. Konsep ini diperkenalkan pertama kali secara internasional pada era tahun 1990-an dalam pertemuan Perserikatan Bangsa-Bangsa (PBB) yang membahas pencegahan kejahatan. Pada tahun 1995, PBB mengidentifikasi 18 jenis kejahatan transnasional yaitu *money laundering, terrorism, theft of art and cultural objects, theft of intellectual property, illicit arms trafficking, aircraft hijacking, sea piracy, insurance fraud, computer crime, environmental crime, trafficking in persons, trade in human body parts, illicit drug trafficking, fraudulent bankruptcy, infiltration of legal business, corruption and bribery of public or party officials.*

BAB 4
PEMBAHASAN

4.1 Penerapan Pasal Terhadap Pelaku *Internet Fraud*

Kejahatan *internet* fraud yang dialami korban Chumpon telah sempurna saat ia mengirimkan uang kepada tersangka. Oleh karena itu, "tempus delicti" kasus ini adalah saat ia mengirimkan uang kepada tersangka dalam bulan November 2007. Kepastian akan "tempus delicti" menurut Profesor Van Bemmelen sangat penting, antara lain akan berkenaan dengan pasal 1 ayat (1) dan (2) KUHP (Lamintang 1997, 227) yang berbunyi

> (1) Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan perundang-undangan pidana yang telah ada
>
> (2) Bilamana ada perubahan dalam perundang-undangan sesudah perbuatan dilakukan, maka terhadap terdakwa diterapkan ketentuan yang paling menguntungkannya

Dari pasal 1 ayat (1) KUHP ini terdapat dua asas penting dari hukum pidana. Asas itu adalah sanksi pidana hanya dapat ditentukan dengan undang-undang serta ketentuan bahwa sanksi pidana tidak boleh berlaku surut (Prodjodikoro 1989, 39). Tetapi, ketentuan yang dimuat dalam pasal 1 ayat (2) KUHP, pada dasarnya merupakan penyimpangan dari larangan berlaku surut apabila terjadi perubahan perundang-undangan. Terhadap terdakwa diterapkan ancaman yang lebih menguntungkan dirinya meskipun aturan itu ada setelah perbuatannya.

Pada saat penegakan hukum kasus www.henbing.com dimulai, memang telah ada peraturan perundang-undangan baru yang memberikan ancaman pidana terhadap jenis perbuatan para pelaku. Peraturan baru memang termuat dalam sebuah hukum yang bersifat administratif, namun dengan adanya ancaman pidana dalam perundang-undangan itu, telah terjadi sebuah perubahan perundang-undangan. Pasal 378 KUHP mengatur ancaman pidana kepada pelaku penipuan dengan pidana penjara maksimal

empat tahun, sedangkan pasal 28 ayat (1) jo pasal 45 ayat (2) Undang-Undang ITE sebagai pasal yang dapat dikenakan terhadap plekau *internet fraud* mengatur ancaman pidana penjara maksimal enam tahun dan/atau denda maksimal Rp 1.000.000.000,-. Jika kita bandingkan kedua ancaman pidana ini, tentu kita setuju bahwa ancaman pidana pasal 378 KUHP lebih rendah dibandingkan dengan pasal 28 ayat (1) jo pasal 45 ayat (2) Undang-Undang ITE. Atas dasar pemikiran ini, kita dapat meyakini bahwa penerapan pasal 378 KUHP tentu akan lebih menguntungkan bagi para terdakwa. Oleh karena itu dengan merujuk pada ketentuan pasal 1 ayat (2) KUHP, penerapan pasal 378 KUHP terhadap para terdakwa adalah langkah yang seharusnya diambil oleh para penegak hukum.

Tidak hanya terhadap kasus-kasus yang terjadi sebelum lahirnya Undang-Undang ITE saja pasal 378 KUHP dapat diterapkan. Penerapan pasal 378 KUHP terhadap kasus yang terjadi pasca pengesahan Undang-Undang ITE juga dimungkinkan. Untuk meyakininya, ada baiknya kita kembali kepada rumusan pasal yang mengatur masalah *internet fraud* , baik dalam KUHP maupun Undang-Undang ITE.. Pasal 378 KUHP berbunyi "Barang siapa dengan maksud hendak menguntungkan diri sendiri atau orang lain dengan melawan hak, baik dengan memakai nama palsu atau keadaan palsu, baik dengan akal dan tipu muslihat maupun dengan karangan perkataan-perkataan bohong, membujuk orang supaya memberikan sesuatu barang, membuat utang atau menghapus piutang, di hukum karena penipuan, dengan hukuman selama-lamanya empat tahun". Sementara itu, pasal 28 ayat (1) Undang-Undang ITE berbunyi 'Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik".

Apabila kita mencermati rumusan kedua pasal ini, kita akan menemukan adanya perbedaan unsur-unsur di dalamnya. Oleh karena itu, kita harus meyakini bahwa kedua pasal tadi sesungguhnya delik yang berbeda meskipun dapat diterapkan untuk memidana satu perbuatan yang sama. Sebaliknya, jika kita menyamakannya, tentu akan bertentangan dengan azas *lex certa* dimana ketentuan perturan-perundang-undangan tidak dapat diartikan lain. Implikasinya, penegak hukum bisa saja tidak

menerapkan pasal 28 ayat (1) Undang-Undang ITE sebagai *lex posterior* dan tetap menggunakan Pasal 378 KUHP, atau dapat pula memasukkan keduanya dalam dakwaan berlapis.[2]

Sebenarnya, apabila kita mencermati modus pelaku, masih ada perundang-undangan lain yang dapat digunakan sebagai alternatif pemidanaan oleh para penegak hukum. Ketika pelaku telah menerima uang sebagai pembayaran barang yang dipesan korban sebagai konsumennya tetapi tidak mengirimkan barang yang dipesan maka ia dapat dikenakan aturan pasal 16 huruf a Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Pasal ini berbunyi "Pelaku usaha dalam menawarkan barang dan/atau jasa melalui pesanan dilarang untuk : tidak menepati pesanan dan/atau kesepakatan waktu penyelesaian sesuai dengan yang dijanjikan." Hanya saja dengan ancaman pidana penjaranya lebih rendah, baik dibandingkan dengan pasal 378 KUHP maupun dengan 28 ayat (1) Undang-Undang ITE, yaitu penjara paling lama 2 (dua) tahun atau pidana denda paling banyak Rp 500.000.000,00 (lima ratus juta rupiah). Oleh karena itu, meskipun unsur-unsur dalam pasal ini relatif lebih mudah dibuktikan oleh para penegak hukum, saya

---

[2] Walaupun pasal 28 ayat (1) Undang-Undang ITE merupakan *lex posterior* terhadap pasal 378 KUHP, tidak semua pasal pidana dalam Undang-Undang merupakan *lex posterior* terhadap pasal-pasal dalam KUHP. Keadaan berbeda terjadi dalam hubungan antara pasal 27 ayat (3) Undang-Undang ITE dengan Pasal 310 KUHP. Rumusan pasal 27 ayat (3) Undang-Undang ITE berbunyi "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik". Dalam rumusan pasal ini terdapat unsur penghinaan dan/atau pencemaran nama baik, padahal tidak terdapat rumusan khusus mengenai kedua hal ini dalam Undang-Undang ITE. Rumusan kedua hal ini hanya dapat kita temukan dalam pasal 310 KUHP yang berbunyi:

(1) Barang siapa sengaja menyerang kehormatan atau nama baik seseorang dengan menuduhkan sesuatu hal, yang maksudnya terang supaya hal itu diketahui umum, diancam karena pencemaran dengan pidana penjara paling lama sembilan bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(2) Jika hal itu dilakukan dengan tulisan atau gambaran yang disiarkan, dipertunjukkan atau ditempelkan di muka umum, maka diancam karena pencemaran tertulis dengan pidana penjara paling lama satu tahun empat bulan atau pidana denda paling banyak empat ribu lima ratus rupiah.

(3) Tidak merupakan pencemaran atau pencemaran tertulis, jika perbuatan jelas dilakukan demi kepentingan umum atau karena terpaksa untuk membela diri.

Oleh karena itu, pasal 27 ayat (3) Undang-Undang ITE merupakan *lex specialis* dan sudah seharusnya penegak hukum menerapkan pasal itu pada kasus pencemaran nama baik dan/atau penghinaan di internet.

menyarankan untuk tidak menerapkannya sendirian. Pasal ini lebih tepat digunakan dalam dakwaan alternatif atau berlapis bersama-sama dengan 378 KUHP dan/atau 28 ayat (1) Undang-Undang ITE.

Selanjutnya, penerapan KUHP semata seperti yang terjadi dalam kasus www.henbing.com akan berimplikasi pada timbulnya kesulitan yang akan dihadapi oleh para penegak hukum. Barda Nawawi Arief menyebutkan sedikitnya ada tiga kesulitan yang akan dihadapi oleh penegakan hukum terhadap *cyber crime*. Kesulitan-kesulitan itu adalah (2006, 79)

a. *Cyber crime* berada di lingkungan elektronik dan dunia maya yang sulit didentifikasikan secara pasti sedangkan asas legalitas konvensional dari perbuatan riel dan kepastian hukum.
b. *Cyber crime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah sedangkan asas legalitas konvensional bertolak dari sumber hukum formal atau undang-undang yang statis.
c. *Cyber crime* melampaui batas-batas negara, sedangkan perundang-undangan suatu negara pada umumnya hanya berlaku di wilayah teritorialnya sendiri.

Dua kesulitan pertama dibahas dalam sub bab ini, sementara kesulitan yang ketiga akan dibahas dalam sub bab berikutnya.

Untuk mengatasi kesulitan akan asas legalitas, penegak hukum harus mencocokkan perbuatan riel yang dilakukan oleh para terdakwa dengan unsur-unsur yang terdapat dalam pasal 378 KUHP. Pada titik ini, penegak hukum harus melakukan penemuan hukum sebagai proses konkretisasi dan individualisasi peraturan hukum yang bersifat umum terhadap perbuatan para pelaku. Pada analisa yuridis yang dilakukan oleh penyidik serta dakwaan penuntut umum, kita menemukan mereka menempatkan website www.henbing.com sebagai sarana pelaku untuk menarik hati korban untuk mau membeli barang yang ditawarkan. Hal ini tentu tidak berbeda dengan bentuk-bentuk reklame yang sering kita jumpai dalam kehidupan sehari-hari. Yang berbeda, hanyalah tempat dimana reklame itu dipasang. Jika biasanya reklame kita temukan di jalan atau di media massa, reklame kali ini

berada di suatu sistem yang bernama internet. Sementara itu, para penegak hukum tidak memiliki kesulitan untuk membuktkan bahwa para pelaku telah melakukan akal muslihat atau berkata bohong untuk membujuk korban menyerahkan barang untuk keuntungan para pelaku seperti yang termuat dalam pasal 378 KUHP. Oleh karena itu, kita dapat meyakini bahwa para penegak hukum telah melakukan penemuan hukum dengan melakukan sebuah interpretasi ekstensif.

Interpretasi ekstensif ini juga memudahkan pelaksanaan tugas hakim. Dengan meletakkannya sebagai kasus penipuan biasa, hakim akan terhindar dari kesulitan memenuhi ketentuan pasal 16 ayat (1) undang-undang kekuasaan kehakiman dimana pengadilan tidak boleh menolak untuk memeriksa, mengadili, dan memutus suatu perkara yang diajukan dengan dalih bahwa hukum tidak ada atau kurang jelas,melainkan wajib untuk memeriksa dan mengadilinya. Putusan dalam perkara ini pun lebih mudah untuk dijatuhkan mengingat yurisprudensi yang menyangkut kejahatan penipuan sangat berlimpah.

Sebagaimana pernyataan Barda Nawawi Arief di atas, hal yang sedikit memberatkan dalam penegakan hukum terhadap kasus www.henbing.com adalah masalah acara pidananya. Penuntut menghadirkan laptop terdakwa dan berupaya untuk memperlihatkan situs yang digunakan oleh terdakwa dalam menjalankan aksinya. Bagaimana jika ternyata situs itu tidak bisa diakses lagi? Tentunya hal ini dapat berpengaruh terhadap alat bukti petunjuk yang sangat berguna untuk pembuktian kejahatan para terdakwa. Untungnya, dalam kasus www.henbing.com, para terdakwa mengakui perbuatan mereka, sehingga ketentuan pasal 183 yang mewajibkan minimal dua alat bukti untuk menjatuhkan putusan dapat terpenuhi.

Meskipun demikian, ada satu hal yang perlu kita catat dalam pemberian keterangan oleh terdakwa. Kita menemukan para penegak hukum melakukan pemisahan perkara (*splitsing*) terhadap para pelaku. Pemisahan maupun penggabungan perkara pada dasarnya merupakan kewenangan penuntut umum. Kewenangan ini diatur dengan rambu-rambu pasal 141 dan 142 KUHAP. Pasal 141 KUHAP berbunyi "Penuntut umum dapat melakukan penggabungan perkara dan

membuatnya dalam satu surat dakwaan, apabila pada waktu yang sama atau hampir bersamaan ia menerima beberapa berkas perkara dalam hal:

a. beberapa tindak pidana yang dilakukan oleh seorang yang sama dan kepentingan pemeriksaan tidak menjadikan halangan terhadap penggabungannya;
b. beberapa tindak pidana yang bersangkut-paut satu dengan yang lain;
c. beberapa tindak pidana yang tidak bersangkut-paut satu dengan yang lain, akan tetapi yang satu dengan yang lain itu ada hubungannya, yang dalam hal ini penggabungan tersebut perlu bagi kepentingan pemeriksaan."

Pasal 142 KUHAP berbunyi " Dalam hal penuntut umum menerima satu berkas perkara yang memuat beberapa tindak pidana yang dilakukan oleh beberapa orang tersangka yang tidak termasuk dalam ketentuan pasal 141, penuntut umum dapat melakukan penuntutan terhadap masing-masing terdakwa secara terpisah.

(1) Penuntut umum melimpahkan perkara ke pengadilan negeri dengan permintaan agar segera mengadili perkara tersebut disertai dengan surat dakwaan.
(2) Penuntut umum membuat surat dakwaan yang diberi tanggal dan ditandatangani serta berisi:
    a. nama lengkap, tempat lahir, umur atau tanggal lahir, jenis kelamin, kebangsaan, tempat tinggal, agama dan pekerjaan tersangka;
    b. uraian secara cermat, jelas dan lengkap mengenai tindak pidana yang didakwakan dengan menyebutkan waktu dan termpat tindak pidana itu dilakukan.
(3) Surat dakwaan yang tidak memenuhi ketentuan sebagaimana dimaksud dalam ayat (2) huruf b batal demi hukum.

Pemisahan perkara ini digunakan oleh penuntut umum sebagai strategi untuk membuktikan dakwaannya sepanjang tidak bertentangan dengan ketentuan pasal 141 dan 142 KUHAP dapat dibenarkan. Hanya saja pada praktiknya menimbulkan kehadiran saksi mahkota (*kroon getuide)* dimana para terdakwa bersaksi satu sama lain. Hal ini tidak bisa dilepaskan dari keterbatasan alat bukti berdasarkan KUHAP

yang dapat diajukan oleh para penegak hukum untuk dapat memperoleh keyakinan hakim di persidangan.

Secara lengkap pasal 183 KUHAP berbunyi "Hakim tidak boleh menjatuhkan pidana kepada seseorang kecuali apabila dengan sekurang-kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi". Rumusan pasal ini menunjukkan bahwa KUHAP menganut *negatief wetelijk stelsel* atau sistem pembuktian yang negatif (Hamzah 2008, 256). Menurut Simmons, pemidanaan didasarkan kepada pembuktian yang berganda, yaitu pada peraturan undang-undang dan pada keyakinan hakim dan menurut undang-undang, dasar keyakinan tiu bersumberkan pada peraturan undang-undang (Hamzah 2008, 256). Oleh karena itu, hakim berkewajiban untuk secara mengkonstruksi keyakinannya berdasarkan alat bukti yang sah sesuai pasal 184 KUHAP yaitu keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Sesuai urutannya, keterangan saksi merupakan alat bukti yang paling utama. Sementara itu, alat bukti keterangan terdakwa merupakan konsep alat bukti baru yang menggantikan konsep alat bukti konservatif berupa pengakuan terdakwa sebagaimana yang diatur dalam ketentuan Pasal 295 *Het Herziene Inlandsch Reglement* (HIR). Hal itu sesuai dengan dianutnya prinsip akusator oleh KUHAP.

Istilah saksi mahkota sendiri tidak disebutkan secara tegas dalam KUHAP. Pengaturan mengenai saksi mahkota hanya diatur dalam ketentuan pasal 168 huruf (c) KUHAP yang pada pokoknya menjelaskan bahwa pihak yang bersama-sama sebagai terdakwa tidak dapat didengar keterangannya dan dapat mengundurkan diri sebagai saksi. Dalam perkembangan berikutnya, Mahkamah Agung melalui yurisprudensi nomor 1986 K/Pid/1989 tanggal 21 Maret 1990 tidak melarang jaksa penuntut umum untuk mengajukan saksi mahkota di persidangan dengan syarat bahwa saksi ini dalam kedudukannya sebagai terdakwa tidak termasuk dalam satu berkas perkara dengan terdakwa yang diberikan kesaksian. Selain itu, dalam yurisprudensi itu telah diberikan suatu definisi tentang saksi mahkota sebagai teman terdakwa yang melakukan tindak pidana bersama-sama dan diajukan sebagai saksi untuk membuktikan dakwaan penuntut umum, yang perkara diantaranya dipisah karena

kurangnya alat bukti. Tetapi, kemudian Mahkamah Agung memiliki pendapat terbaru tentang penggunaan saksi mahkota dalam suatu perkara pidana karena dianggap bertentangan dengan hukum acara pidana yang menjunjung tinggi hak asasi manusia. Hal itu dijelaskan dalam Yurisprudensi Mahkamah Agung Republik Indonesia Nomor 1174 K/Pid/1994 tanggal 3 Mei 1995, Yurisprudensi Mahkamah Agung Republik Indonesia Nomor 1952 K/Pid/1994 tanggal 29 April 1995, Yurisprudensi Mahkamah Agung Republik Indonesia Nomor 1590 K/Pid/1995 tanggal 3 Mei 1995 dan Yurisprudensi Mahkamah Agung Republik Indonesia Nomor 1592 K/Pid/1995 tanggal 3 Mei 1995.

Pengajuan saksi mahkota juga dikritik oleh Andi Hamzah. Menurutnya terjadi penyalahartian akan saksi mahkota di Indonesia. Seakan-akan para terdakwa dalam hal ikut serta (*medeplegen*), perkaranya dipisah dan secara bergantian menjadi saksi (2008, 271). Pada dasarnya, saksi mahkota adalah terdakwa dan sebagai terdakwa dan ia memiliki hak absolut untuk diam atau bahkan hak absolut untuk memberikan jawaban yang bersifat ingkar atau berbohong. Hal itu erat hubungannya dengan tidak adanya kewajiban bagi terdakwa untuk mengucapkan sumpah dalam memberikan keterangannya. Selain itu, menurut ketentuan Pasal 66 KUHAP dijelaskan bahwa terdakwa tidak memiliki beban pembuktian dimana beban pembuktian untuk membuktikan kesalahan terdakwa terletak pada pihak jaksa penuntut umum. Sebaliknya ketika seorang terdakwa diajukan sebagai seorang saksi, ia akan terikat sumpah dalam memberikan keterangannya. Adanya kewajiban untuk bersumpah ini, menyebabkan ia tidak bisa mengoptimalkan hak ingkar yang ia miliki karena akan menghadapi ancaman dakwaan sumpah palsu sesuai pasal 242 KUHP. Akibatnya, ia tidak bisa lagi memberikan keterangan secara bebas dan mengakibatkan dirinya mendakwa diri sendiri (*self incrimination*) (Hamzah 2008, 271). Oleh karena itu, pengajuan saksi mahkota sebagaimana yang dilakukan oleh penegak hukum dalam kasus www.henbing.com harus dihindari karena bertentangan dan melanggar kaidah

hak asasi manusia sebagaimana diatur dalam KUHAP maupun instrumen hak asasi manusia internasional.[3]

Apabila penegak hukum memang mengalami kesulitan untuk mendapatkan alat bukti sebanyak-banyaknya di persidangan, seperti minimnya saksi misalnya. Hal itu harus dilengkapi dengan pencarian alat bukti yang lain. Merujuk kepada kasus www. henbing.com, alat bukti yang lain itu belum dapat dioptimalkan penggunaannya. Permasalahanya adalah belum digunakannya *digital evidence* dalam penegakan hukum kasus itu. *Digital evidence* sendiri bukanlah hal yang baru, tetapi memang baru diakui dalam beberapa perundang-undangan saja seperti undang-undang terorisme, undang-undang pencucian uang dan undang-undang tindak pidana korupsi. Sebenarnya pasal 5 ayat(1) dan (2) Undang-Undang ITE yang sudah disahkan saat penegakan hukum berlangsung dapat diterapkan untuk mempermudah acara pidana kasus itu. Pasal itu berbunyi

(1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

(2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Dengan rumusan pasal di atas, semua informasi dan dokumen elektronik yang didapat dalam penegakan hukum adalah alat bukti yang sah. Artinya, penegakan hukum di luar Undang-Undang ITE pun dapat menggunakan informasi dan dokumen elektronik dan/atau hasil cetaknya sebagai alat bukti yang sah. Pasal ini merupakan jembatan yang menghubungkan Undang-Undang ITE dengan peraturan pidana lainnya. Hanya saja kita patut mencermati klasifikasi informasi dan dokumen elektronik sebagai alat bukti. Pasal 44 Undang-Undang ITE memang mendudukannya sebagai alat bukti yang khusus, namun, perlu diingat bahwa kedudukan itu hanyalah dalam konteks

[3] Salah satu konvensi internasional yang berkaitan dengan saksi mahkota adadalah International Covenant on Civil and Political Right yang dalam pasal 14 ayat (3) huruf g- nya berbunyi " In the dtermination of any criminal charge against him, everyone shall be entitled to the foloowing minimum guarantees, in full equality: (g) not to be compelled to testify against himself or to confess guilty.

penyidikan, penuntutan dan pemeriksaan di sidang pengadilan menurut ketentuan Undang-Undang ITE. Sementara itu untuk penegakan hukum peraturan perundang-undangan yang lain, informasi dan dokumen elektronik merupakan perluasan dari alat bukti yang tercantum dalam pasal 184 KUHAP.

Di sisi lain, penerapan Undang-Undang ITE bukannya tanpa masalah. Masalah utama adalah adanya perbedaan penafsiran terhadap undang-undang ini dan aturan-aturan di dalamnya. Hal ini tentu tidak terlepas dari keberadaan Undang-Undang ITE sebagai undang-undang yang belum lama diberlakukan. Walaupun demikian, sudah seharusnya berdasarkan asas *ius curia novit*, penegak hukum mengetahui dan memahami isi peraturan sebuah perundang-undangan. Jika terjadi perbedaan penafsiran, maka sebaiknya, diadakan sebuah forum untuk menyamakan pandangan mengenai Undang-Undang ITE yang tidak hanya dihadiri oleh para penegak hukum melainkan juga dihadiri oleh para pembuat undang-undang sebagai nara sumber.

Sementara itu, untuk memahami pernyataan para penyidik yang menyatakan adanya kesulitan dalam memenuhi aturan pasal 43 ayat (6) Undang-Undang ITE, sebaiknya kita melihat kembali rumusan pasal itu. Bunyi pasal itu adalah "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". Dengan rumusan pasal ini, dalam melakukan penangkapan atau penahanan, penyidik harus pertama-tama menghubungi penuntut umum terlebih dahulu, kemudian penuntut umum yang memintakan penetapan kepada ketua pengadilan negeri. Hal ini memang memberatkan, karena ada prosedur di tiga instansi yang berbeda yang harus dipenuhi dalam waktu satu kali dua puluh empat jam. Sebagai ilustrasi, seorang penyidik yang akan melakukan penangkapan terhadap tersangka pelaku *cyber crime* membutuhkan penetapan ketua pengadilan negeri sebagai dasar sahnya penankapan yang dia lakukan. Hal pertama yang harus dia lakukan adalah mendapatkan surat pemberitahuan yang ditandatangani kepala kesatuannya untuk dikirimkan kepada kejaksaan setempat. Setelah surat pemberitahuan diterima, kepala kejaksaan menunjuk jaksa yang bertanggung jawab.

Selanjutnya jaksa yang ditunjuk akan mengusahakan surat permohonan penetapan yang ditandatangani kepala kejaksaan untuk dikirimkan kepada ketua pengadilan negeri. Setelah diterima dan dipelajari oleh ketua pengadilan negeri, barulah surat penetapan itu dapat diterbitkan. Ada beberapa titik kelemahan dalam prosedur semacam ini. Yang pertama, kita sudah mafhum bahwa dalam penebitan surat dinas di masing-masing instansi memiliki prosedur yang bahkan bisa memakan waktu hampir satu hari lamanya. Selain itu, bagaimana seandainya penangkapan itu dilaksanakan penyidik pada hari di luar hari kerja kejaksaan dan pengadilan? Sudah barang tentu penetapan dari ketua pengadilan negeri tidak akan berhasil diperoleh penyidik, bahkan oleh penyidik di kota besar sekalipun.

Namun, di sisi lain, preferensi penyidik untuk memilih menggunakan KUHP dibandingkan Undang-Undang ITE untuk menghindari kesulitan yang timbul dari pasal 43 ayat (6) bisa menimbulkan preseden yang kurang baik bagi penegakan hukum Undang-Undang ITE sendiri. Undang-undang ITE sebagai suatu *lex posterior* seharusnya memudahkan para penegak hukum untuk melakukan penindakan terhadap para pelaku kejahatan, tetapi pada praktiknya dianggap memberatkan penegak hukum itu sendiri. Oleh karena itu, perlu diadakan amandemen terhadap Undang-Undang ITE, khususnya terhadap pasal 43 Undang-Undang ITE.

4.2 Penentuan Yurisdiksi

Dalam menentukan yurisdiksi, yang pertama kali harus kita lakukan adalah menentukan *locus delicti* dari suatu kejahatan. Dalam kasus ini, kita menemukan bahwa keempat teori *locus delicti* dapat dipergunakan dalam menentukan *locus delictie*, yaitu

a. *de leer van de lichamlijke daad* atau ajaran mengenai tindakan secara pribadi atau ajaran tindakan badaniah atau ajaran perbuatan., dimana locus delictie adalah tempat dimana seorang pelaku telah melakukan sendiri perbuatannya yang terlarang atau tempat di mana disyaratkan bahwa pelaku itu melakukan perbuatannya secara pribadi;

b. *de leer van heet instrument* atau ajaran mengenai alat, dimana locus delicti adalah terutama tempat seorang pelaku itu telah melakukan sendiri perbuatannya yang terlarang oleh undang-undang, akan tetapi apabila untuk melakukan perbuatannya itu si pelaku telah menggunakan sebuah alat, maka tempat di mana alat itu bekerja harus juga dipandang sebagai tempat dilakukannya tindak pidana yang bersangkutan ;

c. *de leer van het gevolg* atau ajaran tentang akibat, dimana locus delicti adalah tempat dimana suatu tindak pidana itu telah menimbulkan akibat, baik itu merupakan suatu akibat yang telah ditimbulkan secara langsung oleh sesuatu tindak pidana maupun suatu akibat yang timbulnya itu merupakan syarat untuk selesainya suatu tindak pidana;

d. *de leer van de meervoudige plaats* atau ajaran gabungan tindak pidana, dimana locus delicti adalah semua tempat, baik tempat dimana seorang pelaku telah melakukan sendiri perbuatannya yang dilarang undang-undang maupun tempat dimana alat yang dipergunakannya itu telah menimbulkan akibat, yaitu apabila tindak pidana yang telah dilakukannya itu meliputi beberapa peristiwa yang telah terjadi di beberapa tempat.

Dengan berdasar kepada ajaran tentang perbuatan, maka *locus delicti* kasus Ronal adalah di rumahnya yang terletak di Giri Loka III Blok Z I Nomor 17 BSD City Tangerang. Hal ini disebabkan karena di rumahnya itulah dia melakukan upaya-upaya untuk menarik calon korbannya. Sementara itu, dengan ajaran tentang akibat, Bangkok sebagai tempat Chumpon mengirimkan uangnya dapat juga dijadikan sebagai *locus delicti*. Namun, di sini, para penegak hukum sepakat untuk menerapkan ajaran tentang perbuatan terhadap Ronal sehingga *locus delicti*nya adalah rumahnya.

Penentuan *locus delicti* dengan berdasarkan ajaran tentang teori perbuatan ini juga tercermin dalam putusan pengadilan terhadap kasus-kasus *cyber crime berikut*:

a. Putusan Pengadilan Negeri Sleman Nomor 94/Pid. B/2002/PN.SLM atas terdakwa Petrus Pangkur alias Bony Diobok-obok.

b. Putusan Pengadilan Negeri Jakarta Selatan Nomor 2098/Pid. B/2005/PN.JS atas terdakwa Emilia Karolina .

Perkara Petrus Pangkur adalah perkara cyber crime pertama yang diajukan ke peradilan pidana di Indonesia. Petrus Pangkur didakwa karena ia melakukan pemesanan barang melalui sebuah situs perbelanjaan online yang ada di Amerika Serikat dengan menggunakan kartu kredit yang diperoleh dalam chatting. *Locus delicti* kejahatan Petrus Pangkur adalah warung internet "Naganet" yang beralamat Jl Pringgodani Nomor 66 Depok Sleman yang ditentukan berdasarkan ajaran tentang perbuatan.

Perkara Emilia Karolina adalah pengancaman melalui email yang dikirimkan dari warung internet sporta@net, Kebayoran Baru kepada ke alamat email milik Kathryn Hopkins seorang guru di Falls Church City Public School, Virginia, Amerika Serikat. Akibat kiriman email itu, terjadi ketakutan yang luar biasa di sekolah tempat Hopkins mengajar hingga sekolah dikosongkan dan berada dalam pengawasan polisi. Meskipun, terjadi akibat yang sangat besar di Falls Church City, Emilia tetap diadili di Pengadilan Negeri Jakarta Selatan. Hal ini sejalan dengan pendapat hakim pada perkara itu yang menyatakan bahwa perbuatan kejahatan dilakukan di wilayah hukum Pengadilan Negeri Jakarta Selatan.

Dengan menentukan *locus delicti* kejahatan Ronal di rumahnya yang terletak di Tangerang, maka kita dapat menentukan yurisdiksi yang berlaku terhadapnya. Jika rumah Ronal adalah tempat ia melakukan kejahatan, maka berdasarkan prinsip teritorialitas yang ditegaskan dalam pasal 2 KUHP, ketentuan hukum pidana Indonesia berlaku kepadanya.

Lain halnya dengan penentuan *locus delictie* Devvy. Jika berdasar kepada ajaran tentang perbuatan, *locus delicti*nya adalah rumahnya yang berada di Denpasar. Tetapi, perbuatannya itu berakibat Ronal dapat melakukan kejahatan di rumahnya. Oleh karena itu berdasarkan ajaran tentang akibat, rumah Ronal juga merupakan *locus delicti* perbuatannya. Dengan menetapkan rumah Ronal sebagai *locus delicti* maka berdasarkan prinsip teritorialitas, yurisdiksi Indonesia dapat diberlakukan terhadap Devvy.

Setelah kita dapat meyakini bahwa terhadap kedua pelaku dapat dikenakan yurisdiksi Indonesia, tugas kita adalah menentukan pengadilan negeri yang memiliki kewenangan untuk mengadili. Kewenangan mengadili ini diatur dalam pasal 84 KUHAP yang berbunyi

(1) Pengadilan negeri berwenang mengadili segala perkara mengenai tindak pidana yang dilakukan di daerahnya.

(2) Pengadilan negeri yang di dalam daerah hukumnya terdakwa bertempat tinggal, berdiam terakhir, di tempat dia diketemukan, atau ditahan, hanya berwenang mengadili perkara tersebut, apabila tempat kediaman sebagian besar saksi yang dipanggil lebih dekat pada tempat pengadilan negeri itu daripada tempat kedudukan pengadilan negeri yang di dalam daerahnya itu tindak pidana dilakukan.

(3) Apabila seorang terdakwa melakukan beberapa tindak pidana dalam daerah hukum pelbagai pengadilan negeri, maka tiap pengadilan negeri itu masing-masing berwenang mengadili perkara pidana itu.

(4) Terhadap beberapa perkara pidana yang satu sama lain ada sangkut pautnya dan dilakukan oleh seorang dalam daerah hukum pelbagai pengadilan negeri, diadili oleh masing-masingpengadilan negeri dengan ketentuan dibuka kemungkinan penggabungan perkara tersebut.

Ronal melakukan perbuatannya rumah tempat tinggalnya di Tangerang, maka berdasarkan ketentuan pasal 84 ayat (1) dan (2), Pengadilan Negeri Tangerang memiliki kewenangan mengadili terhadapnya. Sementara itu, Devvy ditahan di Tangerang, sedangkan saksi-saksi dalam kasusnya lebih dekat ke Tangerang dibandingkan ke Denpasar, tempatnya membuat desain www.henbing.com. oleh karenanya berdasarkan pasal 84 ayat (2), Pengadilan Negeri Tangerang memiliki kewenangan mengadili terhadapnya.

Selanjutnya, kita harus berhati-hati dalam menerapkan asas nasionalitas aktif sebagai alternatif dalam penentuan yurisdiksi. Untuk lebih jelasnya, mari kita kembali lihat rumusan pasal 5 KUHP. Pasal ini berbunyi

(1) Ketentuan-ketentuan hukum pidana Indonesia berlaku bagi warga negara Indonesia bersalah melakukan ;

Kesatu: salah satu dari kejahatan-kejahatan yang termuat dalam titel 1 dan 2 Buku II dan dalam pasal-pasal 160,161, 240, 279, 450, dan 451

Kedua: suatu tindak pidana yang menurut hukum pidana Indonesia masuk golongan "kejahatan" dan yang menurut hukum pidana dari negara tempat pidana itu dilakukan, diancam pula hukuman pidana.

(2) Penuntutan kejahatan-kejahatan tersebut dalam sub-bab kedua juga dapat diberlakukan apabila si tersangka baru setelah melakukan tindak pidana menjadi warga negara Indonesia.

Dari rumusan pasal 5 KUHP di atas, sepertinya tidak tepat bagi kita untuk menerapkan asas nasionalitas aktif bagi para pelaku kejahatan *internet fraud*. Penyebabnya, para pelaku itu melakukan kejahatannya tidak berada di luar negeri, melainkan di wilayah Indonesia. Tidak hanya itu, seandainya pelaku berkewarganegaraan Indonesia melakukan kejahatan *internet fraud* di luar negeri, asas nasionalitas aktif pun tidak bisa diberlakukan seandainya tidak memenuhi asas *double criminality* yang dipersyaratkan oleh pasal 5 ayat (2) ke-2 KUHP.

Walaupun demikian, hal itu tidak berarti nasionalitas sama sekali tidak bisa diterapkan dalam kasus *internet fraud*. Menurut Menthe dalam teori *international space*-nya, nasionalitas dari pelaku bisa digunakan sebagai dasar penentuan yurisdiksi bagi sebuah kejahatan *cyber crime*. Teori ini diajukan Menthe untuk menjawab yurisdiksi internet. Ruang siber diperlakukan sama dengan antartika, laut lepas dan ruang angkasa dimana tidak ada negara yang memiliki yurisdiksi berdasarkan teritorial. Dalam wilayah yang bersifat *sovereignless* tadi, penentuan yurisdiksi terhadap suatu tindak pidana akan bergantung pada nasionalitas si pelaku. Teori ini diadopsi oleh Konvensi Negara-Negara Eropa tentang Cyber crime dalam penentuan yurisdiksi pelaku *cyber crime*.

Dengan merujuk kepada teori *international space* ini, kita tidak lagi mempersoalkan dimana Ronal ataupun Devvy melakukan *upload* www.henbing.com. Meskipun seandainya kegiatan itu dilakukan di luar wilayah

Indonesia, dengan melakukan pendekatan berdasarkan teori *international space*, kewarganegaraan keduanya sudah bisa menjadi dasar berlakunya yurisdiksi terhadap mereka. Demikian pula halnya dengan keberadaan server www.henbing.com yang berlokasi di luar Indonesia. Jika kita berpegang pada ajaran mengenai alat dalam penentuan *locus delicti*, lokasi server juga merupakan *locus delicti*. Oleh karena itu berdasarkan azas teritorialitas, negara tempat lokasi server juga memiliki yurisdiksi atas perkara www.henbing.com. Namun, dengan melakukan pendekatan ruang siber sebagai wilayah yang *sovereignless*, kewarganegaraan pelaku adalah dasar utama penentuan yurisdiksi kasus www.henbing.com

Pertanyaan mengenai penerapan teori *international space* akan timbul seandainya negara korban tidak mengenal *double criminality system*. Apakah teori ini dapat diterapkan dalam keadaan demikian? Untuk menjawabnya, saya akan merujuk pada prinsip-prinsip yurisdiksi yang dikenal hukum pidana kita. Saya berpendapat bahwa ada dua prinsip dalam hukum pidana kita yang erat hubungannya dengan teori ini, yaitu prinsip nasionalitas aktif dan prinsip universalitas. Kedua prinsip ini harus dielaborasi guna penerapan teori *international space* tadi. Seperti sudah disebut sebelumnya prinsip nasionalitas aktif sangat berperan dalam penentuan yurisdiksi berdasarkan teori *international space*. Ketika berhadapan dengan negara yang tidak mengenal *double criminality system*, di sini para penegak hukum dapat menerapkan prinsip universalitas. Prinsip ini memandang pada suatu tata hukum internasional dimana terlibat kepentingan bersama dari semua negara di dunia. Maka, bila asa suatu tindak pidana yang merugikan kepentingan bersama dari semua negara itu, adalah layak, bahwa tindak pidana itu dapat dituntut dan dihukum oleh pengadilan setiap negara, dengan tidak memedulikan siapa yang melakukan dan dimana ia melakukan (Projodikoro 1989, 53). Meskipun negara asal korban tidak mengklasifikasikan *internet fraud* sebagai kejahatan, pada dasarnya telah terjadi kerugian bagi warganegaranya. Penedekatan serupa bisa kita temukan pada pasal 448 KUHP yang berbunyi "Seorang penumpang kapal Indonesia yang merampas kekuasaan atas kapal secara melawan hukum, diancam dengan pidana penjara paling lama tujuh tahun." Dalam pasal ini sama sekali tidak disebutkan ketentuan bendera kapal. Artinya di

wilayah perairan mana saja dan bendera negara mana saja pasal itu dapat diterapkan kepada warganegara Indonesia. Oleh karena itu, elaborasi prinsip universalitas ini memungkinkan teori *international space* untuk diterapkan untuk kasus *internet fraud* dimana negara korban tidak menganut *double criminality system.*

Lalu, bagaimana seandainya Thailand ingin melakukan peradilan pidana terhadap Ronal dan Devvy. Hal itu dimungkinkan jika Thailand juga menganut asas nasionalitas pasif sebagai dasar penentuan yurisdiksinya. Namun, hal ini tidak mudah untuk terealisasi mengingat baik Ronal maupun Devvy berada di Indonesia. Berdasarkan pasal 7 Undang-Undang Ekstradisi, Indonesia memiliki hak untuk tidak menyerahkan warganegaranya, dalam kasus ini, Ronal dan Devvy kepada negara lain.

Dari uraian di atas, kita dapat menarik benang merah tentang bagaimana para penegak hukum menentukan yurisdiksi dalam kasus yang diteliti. Mereka, pada dasarnya, memilih untuk menerapkan prinsip teritorialitas dalam penegakan hukum terhadap kasus penipuan internet dengan korban berdomisili di luar negeri. Meskipun demikian, kita harus ingat bahwa kasus ini terjadi sebelum pengesahan Undang-Undang ITE. Dalam penegakan hukum yang didasarkan pada Undang-Undang ITE, yurisdiksi yang berlaku adalah sesuai dengan aturan pasal 2 undang-undang itu 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". Yurisdiksi ini bahkan lebih luas jika kita bandingkan dengan yurisdiksi yang diatur dalam Convention on Cyber Crime. Dalam konvensi itu, negara-negara pihak seharusnya mengatur yurisdiksi yang meliputi teritorinya, kapal laut berbendera negara pihak, pesawat terbang yang didaftarkan di bawah perundang-undangan negara pihak atau warga negaranya, jika kejahatan itu dapat dipidana berdasarkan hukum pidana di tempat ia melakukan kejahatan atau jika kejahatan itu dilakukan di luar yurisdiksi teritorial negara manapun. Jika kita perhatikan yurisdiksi menurut konvensi ini hanyalah berdasarkan asas teritorialitas, asas nasionalitas aktif dengan penambahan teori *International Space* milik Darrel

Menthe. Sebaliknya Undang-Undang ITE memiliki penekanan pada rumusan kepentingan Indonesia. Siapa saja, dimanapun dapat ditindak berdasarkan undang-undang ITE selama dianggap dapat merugikan kepentingan Indonesia yang meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia. Oleh karena itu, seharusnya yurisdiksi bukan lagi menjadi masalah dalam penegakan hukum terhadap kasus-kasus *internet fraud* di masa yang akan datang.

4.3 Kendala dalam Penegakan Hukum

Ketika kita berbicara mengenai kendala dalam penegakan hukum terhadap kejahatan internet fraud dengan korban berdomisili di luar negeri, kita tidak bisa melepaskan diri dari faktor-faktor yang mempengaruhi penegakan hukum itu. Seperti disampaikan oleh Soerjono Soekanto, faktor-faktor itu bersifat netral. Jika faktor-faktor itu berfungsi dengan baik, penegakan hukum akan berjalan dengan baik. Sebaliknya, faktor-faktor itu bisa menjadi hambatan jika ternyata ada penyimpangan dalam faktor-faktor tadi. Dalam pembahasan berikut saya mencoba menganalisa kendala-kendala yang dihadapi dalam penegakan hukum berdasarkan lima faktor yang diidentifikasi oleh Soerjono Soekanto itu.

4.3.1 Faktor Hukum

Dari uraian sebelumnya, kita telah menyinggung adanya hambatan yang disebabkan oleh peraturan perundang-undangan. Hambatan yang disebabkan oleh peraturan perundang-undangan ini dapat kita klasifikasikan ke dalam dua kelompok berdasarkan waktu, sebelum dan sesudah diadakannya Undang-Undang ITE.

Sebelum adanya Undang-Undang ITE, penegakan hukum dilaksanakan dengan berdasarkan ketentuan-ketentuan yang ada dalam KUHP dan KUHAP. Dalam

KUHP sendiri tidak ada aturan yang secara jelas mengatur mengenai dunia siber. Para penegak hukum harus melakukan penafsiran terhadap pasal 378 KUHP yang mengatur pidana terhadap kejahatan penipuan. Namun, penafsiran itu tidak sampai menjadi "penemuan hukum" karena rumusan pasal 378 masih relevan dengan kejahatan pelaku dan tidak menghambat para penegak hukum dalam melaksanakan tugasnya.

Hambatan paling besar yang ditemui pada masa pra-Undang-Undang ITE adalah masalah pembuktian. KUHAP belum mengatur kedudukan informasi dan dokumen elektronik sebagai alat bukti yang sah. Tentu saja, penerapan KUHAP semata ini akan menyulitkan para penegak hukum. Karena sebagai kejahatan yang menggunakan teknologi informasi, barang bukti yang tersedia akan berbentuk informasi dan dokumen elektronik. Atau, betapa tidak mudah dan tidak praktisnya harus membawa semua sistem ke persidangan. Apalagi jika ternyata dokumen atau informasi yang dimaksud tidak dapat ditampilkan dengan baik di muka persidangan. Tetapi, setelah disahkannya Undang-Undang ITE, terdapat pengakuan informasi dan dokumen elektronik sebagai alat bukti yang sah. Pengakuan ini tidak terbatas dalam penegakan hukum berdasarkan Undang-Undang ITE saja, melainkan untuk semua penegakan hukum yang di dalamnya terdapat keterlibatan informasi dan dokumen elektronik.

Disahkannya Undang-Undang ITE tidak serta merta berarti semua penegakan hukum terhadap *internet fraud* menggunakan undang-undang ini. Ada kecenderungan peferensi penyidik untuk tetap menggunakan pasal 378 KUHP dibandingkan pasal-pasal dalam Undang-Undang ITE jika dirasakan tidak mampu memperoleh penetapan penangkapan ataupun penahanan dari Ketua Pengadilan Negeri. Padahal, situasi dalam penegakan hukum berkembang sangat dinamis. Bisa jadi tersangka ditangkap tanpa ada perencanaan sebelumnya, pada kasus tertangkap tangan misalnya. Meskipun Undang-Undang ITE tidak mengatur masalah tertangkap tangan, pasal 42 undang-undang ini menyatakan bahwa penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ITE, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ITE.

Oleh karena itu, seharusnya pada kasus tertangkap tangan, semua aturan dikembalikan kepada KUHAP.

Bagaimanapun juga penggunaan pasal 378 KUHP adalah preseden yang kurang baik. Memang, tingkat kemungkinan keberhasilan penegakan hukum akan lebih besar. Tetapi, hal itu akan memberikan anggapan bahwa pasal-pasal pidana dalam Undang-Undang ITE tidak dapat dioperasionalisasikan. Selain itu, ancaman dalam Undang-Undang ITE lebih berat dibandingkan KUHP, sehingga penerapannya tentu dapat memberikan efek jera yang lebih besar. Oleh karena itu, jika penyebab penyidik enggan menggunakan Undang-Undang ITE disebabkan aturan pasal 43 ayat (6) Undang-Undang ITE, seperti sudah saya kemukakan sebelumnya, aturan pasal ini harus ditinjau ulang.

4.3.2 Faktor Penegak Hukum

Faktor penegak hukum adalah faktor yang paling utama dalam sebuah penegakan hukum. hal itu disebabkan undang-undang disusun oleh penegak hukum, penerapannya dilakukan oleh penegak hukum dan penegak hukum dianggap sebagai golongan panutan hukum oleh masyarakat luas (Soekanto 2010, 69). Namun, dalam kasus yang kita dalami, kita menemukan bahwa kwantitas dan kwalitas penegak hukum menjadi hambatan dalam penegakan hukum. Jumlah penyidik dirasakan belum mampu menangani semua dugaan kasus *internet fraud*. Di sisi lain, kesempatan jaksa atau hakim menangani kasus cyber crime sangat sedikit. Hal ini bisa terlihat dari pengakuan Jaksa Penuntut Umum Faisal Adi dan Hakim Ismail bahwa penanganan kasus www.henbing.com adalah satu-satunya kejahatan cyber crime yang mereka tangani. Kenyataan ini tentu akan menjadi kendala besar mengingat faktor penegak hukum adalah titik sentral dalam penegakan hukum.

Jika kita berbicara mengenai kurangnya jumlah penegak hukum, maka penambahan personel merupakan jawabannya. Tetapi, penambahan ini bisa jadi sia-sia bila tidak diiringi kemampuan yang memadai. Dari uraian sebelumnya kita mengetahui akan minimnya "persentuhan" para penegak hukum selain polisi dengan

cyber crime. Hal itu tentu sedikit banyak berpengaruh terhadap kemampuan mereka dalam menangani kasus-kasus *cyber crime*. Oleh karena itu, peningkatan "persentuhan" para penegak hukum dengan *cyber crime* adalah suatu keharusan. Ada dua cara yang dapat ditempuh untuk menciptakan kondisi itu. Pertama, melalui forum pendidikan pelatihan bagi para penegak hukum mengenai penanganan kasus-kasus *cyber crime*. Melalui forum semacam ini, dapat dihasilkan sebanyak-banyaknya penegak hukum yang menguasai taktik dan teknik penanganan *cyber crime*. Dengan penguasaan taktik dan teknik itu, mereka akan siap untuk menangani kasus *cyber crime* dalam perjalanan tugas mereka.

Alternatif yang kedua adalah pembentukan unit atau penunjukan orang secara khusus untuk menangani *cyber crime*. Pengalaman kepolisian menerapkan spesialisasi telah menghasilkan penegak hukum yang memang menguasai bidangnya. Meskipun terdapat perbedaan struktur dan cara kerja, kebijakan pembentukan unit atau penunjukan petugas khusus sudah seharusnya dipertimbangkan oleh kejaksaan dan pengadilan. Unit atau petugas khusus ini ditunjuk dari petugas-petugas yang memiliki pengalaman menangani *cyber crime* atau pernah mengikuti pelatihan mengenai penanganan *cyber crime*. Selanjutnya, mereka lah yang menangani kasus-kasus *cyber crime* yang diajukan kepada instansi mereka. pengalaman yang mereka peroleh dalam penanganan kasus tentu akan berpengaruh positif bagi mereka dalam menangani kasus-kasus serupa di masa datang.

4.3.3 Faktor Sarana Atau Fasilitas Yang Mendukung Penegakan Hukum

Dalam kasus yang kita dalami, kita dapat melihat kekurangan sarana dan fasilitas yang berhubungan dengan pengolahan bukti digital. Jumlah laboratorium *computer forensic* yang saat ini dimiliki oleh kepolisian tidak sebanding dengan luas wilayah Indonesia serta kasus yang harus ditangani. Hal ini diperburuk dengan tidak adanya alokasi anggaran khusus bagi pemeliharaan dan peningkatan kemampuan alat-alat *computer forensic* yang digunakan dalam pemrosesan data digital.

Meskipun faktor sarana bukan merupakan faktor utama dalam penegakan hukum. Kekurangan dalam faktor ini tentu akan mebuat penegakan hukum berjalan pincang. Dalam rangka menanganinya, Soerjono Soekanto dan Purbacaraka menawarkan jalan pikiran sebagai berikut (Soekanto 2010, 44)

a. yang tidak ada, diadakan baru,
b. yang rusak atau salah, diperbaiki atau dibetulkan
c. yang kurang, ditambah
d. yang macet, dilancarkan
e. yang mundur atau merosot, dimajukan atau ditingkatkan

Beikutnya tentu timbul pertanyaan bagaimana untuk mencapainya jika dana masih menjadi persoalan utama. Di sini peran manajerial pada institusi penegakan hukum sangat penting. Seperti pada kepolisian sesuai dengan konteks pembicaraan kita kali ini. Seharusnya pejabat yang menangani perencanaan strategis dapat membuat skala prioritas danmendahulukan penyediaan alat-alat modal ini dibandingkan pengeluaran lain yang sesungguhnya bisa dikurangi atau dihemat pembiayaannya. Jika memang tidak ada anggaran yang bisa dilakokasikan, maka sudah seharusnya manajer mencari dukungan dari pihak ketiga, baik dari dalam maupun luar Indonesia.

4.3.4 Faktor Masyarakat

Dari faktor masyarakat, ada dua hal yang mengemuka, yaitu anonimitas pelaku, serta keengganan melapor . Anonimitas sendiri merupakan hal yang wajar bagi setiap pelaku kejahatan. Logikanya, tidak ada pelaku yang ingin tertangkap. Dalam contoh Ronal misalnya. Ia memiliki beberapa identitas palsu dan rekening bank yang dibuka berdasarkan identitas palsu yang ia ajukan. Yang perlu diperhatikan di sini adalah betapa mudahnya Ronal mendapatkan dokumen yang mendukung identitas palsunya itu. Hal ini tentu tidak terjadi jika Indonesia memiliki sistem adminstrasi kependudukan yang baik.

Sementara itu, keberadaan rekening yang digunakan tersangka untuk menerima uang dari korban seharusnya dapat menjadi petunjuk yang sangat berharga dalam pelacakan tersangka. Namun, tentu saja, pihak bank tidak dapat membuka identitas pemilik rekening begitu saja, karena akan melanggar aturan rahasia perbankan. Untuk membuka identitas pemilik rekening, harus melewati prosedur permintaan resmi. Alur prosedur itu adalah penyidik-atasan penyidik-Kapolri-Gubernur Bank Indonesia-bank yang bersangkutan. Panjangnya prosedur ini tidak hanya menghambat penyidikan, namun juga dapat mendorong terjadinya pelanggaran yang berkaitan dengan rahasia perbankan itu sendiri. Dengan alasan untuk mempersingkat waktu, penyidik bisa saja menghubungi kenalannya di bank bersangkutan dan mendapatkan informasi yang diperlukan dari kenalannya itu. Tetapi perlu diingat pengungkapan identitas pemilik rekening tanpa ijin Gubernur Bank Indonesia adalah kejahatan dan hal ini bisa digunakan oleh tersangka untuk menggugurkan proses hukum yang sedang dihadapinya. Oleh karena itu perlu dirumuskan lagi suatu bentuk prosedur yang lebih singkat, namun tetap tidak melanggar aturan undang-undang perbankan.

Selanjutnya, sesuai pendapat Jewkes yang telah dikutip sebelumnya, tidak dilaporkannya suatu kejahatan merupakan salah satu hambatan dalam penegakan hukum. Beberapa contoh yang diberikan penyidik juga memperlihatkan hal yang sama. KUHAP mengatur ketentuan tentang laporan ini dalam pasal 106 dan pasal 108 ayat (1) sampai dengan ayat (6). Pasal 106 berisikan kewjiban penyidik untuk segera melakukan tindakan penyidikan setelah mengetahui, menerima laporan atau pengaduan tentang suatu peristiwa yang diduga tindak pidana. Sementara itu pasal 108 berbunyi :

(1) setiap orang yang mengalami, melihat, menyaksikan dan atau menjadi korban peristiwa yang merupakan tindak pidana berhak untuk mengajukan laporan atau pengaduan kepada penyelidik dan atau penyidik baik lisan maupun tertulis

(2) setiap orang yang mengetahui permufakatan jahat untuk melakukan tindak pidana terhadap ketentraman dan ketentraman umum atau terhadap jiwa

atau terhadap hak milik wajib seketika itu juga melaporkan hal tersebut kepadapenyelidik atau penyidik.

(3) setiap pegawai negeri dalam rangka melaksanakan tugasnya yang mengetahui tentang terjadinya tindak pidana wajib segera melaporkan hal itu kepada penyelidik atau penyidik

(4) laporan atau pengaduan yang diajukan secara tertulis harus ditandatangani oleh pelapor atau pengadu

(5) laporan atau pengaduan yang diajukan secara lisan harus dicatat oleh penyidik dan ditandatangani oleh pelapor atau pengadu dan penyidik

(6) setelah menerima laporan atau pengaduan, penyelidik atau penyidik harus memberikan surat tanda penerimaan laporan atau pengaduan yang bersangkutan.

Rumusan pasal di atas tentu memberikan rambu-rambu yang sangat jelas bagi definisi laporan itu sendiri. Konsekwensinya jika seseorang korban enggan melapor, maka tidak akan ada laporan yang berarti tidak ada penegakan hukum terhadapnya. Namun, dalam beberapa kasus, si korban meskipun enggan melapor langsung ke kepolisian Indonessia, ia mau membuat sebuah laporan tertulis. Penggunaan laporan tertulis ini yang seharusnya bisa dioperasikan sebagai penafsiran pasal 108 ayat (4). Sementara itu, demi memenuhi prinsip kehati-hatian, laporan tertulis itu diautentikasi oleh perwakilan Republik Indonesia di negara korban berada. Mengingat kejadian ini bisa terjadi tidak hanya dalam kejahatan *cyber crime* saja, melainkan juga kejahatan lintas negara lainnya, sudah seharusnya masalah pelaporan ini menjadi masalah khusus yang harus dibahas dalam perumusan hukum acara pidana yang baru. Masalah berikutnya bisa jadi pemeriksaan saksi korban yang tidak bersedia datang ke Indonesia. Dalam hal meminta keterangan saksi, kita memang bisa menggunakan kerjasama bantuan hukum timbal balik. Tetapi perlu diingat, tidak semua negara memiliki perjanjian kerjasama bantuan timbal balik dalam masalah hukum pidana dengan Indonesia. Selain itu, prosedur yang harus dilalui dalam permohonan bantuan timbal balik cukup panjang dan keputusan akhir akan sangat bergantung kepada situasi hubungan diplomatik dengan negara yang diminta. Akhirnya hal ini akan

menyita waktu dan memberi suasana ketidakpastian dalam penegakan hukum. Alternatif lain adalah pemberdayaan atase kepolisian atau staf teknis kepolisian di perwakilan-perwakilan RI di luar negeri untuk memeriksa saksi. Pemberdayaan mereka tentu akan menghemat waktu dan biaya, mengingat mereka berada dekat dengan korban dan lebih memahami situasi yang dihadapi korban. Sayangnya, tidak di semua perwakilan RI ditempatkan Atase Kepolisian atau Staf Teknis Kepolisian.

Dengan adanya kesulitan yang berhubungan dengan pelaporan dan pemeriksaan saksi di atas, saya ingin menghidupkan kembali wacana penggunaan pelaporan dan pemeriksaan saksi secara online. Apabila hal ini direalisasikan tentu akan banyak sumber daya yang bisa dihemat dalam proses penegakan hukum. Ada keraguan memang mengenai keamanan dan kehati-hatian. Tetapi, kita harus memiliki keyakinan bahwa pada suatu saat akan ada jaringan yang aman untuk digunakan oleh penegak hukum dalam menerima pelaporan dan pemeriksaan saksi secara online.[4]

Lalu bagaimana dengan legalitasnya? Pada dasarnya setiap dokumen elektronik merupakan alat bukti yang sah, walaupun dokumen yang terkait dengan penegakan hukum tentu terikat dengan ketentuan pasal 5 ayat (4) Undang-Undang ITE dimana ketentuan tadi tidak berlaku bagi surat-surat yang menurut undang-undang harus dalam bentuk tertulis. KUHAP memang mempersyaratkan dokumen dalam acara pidana secara tertulis. Tetapi kita harus ingat bahwa KUHAP ada sebelum penggunaan teknologi informasi secara masif. Mengingat saat ini kita sedang berupaya merevisi KUHAP, ada baiknya kita memasukkan aturan penggunaan dokumen elektronik khusunya dalam penerimaan laporan dan pemeriksaan saksi sebagai langkah antisipatif terhadap tantangan penggunaaan teknologi informasi yang lebih besar di masa yang akan datang.

[4] Salah satu bentuk pengamanan yang sederhana adalah penggunaan tanda tangan elektronik sebagaimana yang diatur dalam KUHAP, tetapi saya yakin kita perlu bentuk-bentuk pengamanan yang lebih kompleks daripada sekadar tanda tangan elektronik yang bisa dicuri. Di sini penegak hukum bisa berkolaborasi dengan ilmuwan teknologi informasi untuk membentuk sebuah *network* yang aman. Kemungkinan untuk dirusak atau disusupi memang besar, tetapi dengan perencanaan yang matang dan pemeliharaan yang dilakukan secara tepat, saya merasa kemungkinan untuk menciptkan jaringan yang realatif aman tetap ada.

4.3.5 Faktor Kebudayaan

Faktor kebudayaan dibedakan dengan faktor masyarakat, karena dalam pembahasannya diketengahkan masalah sistem nilai-nilai yang menjadi inti dari kebudayaan spiritual atau non materiel. Sebagai suatu sistem, hukum menurut Friedman mencakup struktur, substansi dan kebudayaan. Struktur mencakup wadah ataupun bentuk dari sistem itu yang mencakup tatanan lembaga-lembaga formal. Substansi mencakup isi norma-norma hukum beserta perumusannya maupun acara untuk menegakkannya yang berlaku bagi pelaksana hukum, maupun pencari keadilan. Kebudayaan (sistem) hukum pada dasarnya mencakup nilai-nilai yang mendasari hukum yang berlaku, nilai-nilai yang merupakan konsepsi-konsepsi abstrak mengenai apa yang dianggap baik dan apa yang dianggap buruk. Nilai-nilai inilah yang mejadi pokok pembicaraan dalam faktor kebudayaan (Soekanto 2010, 60).

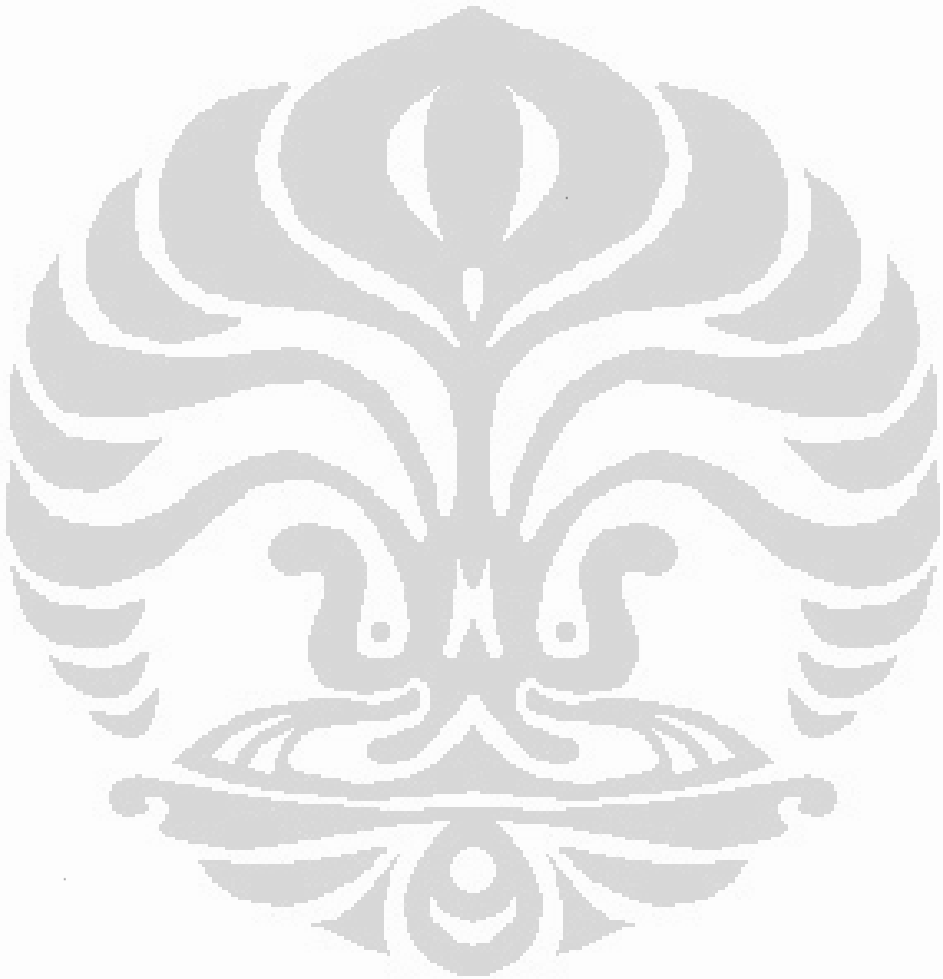
Sebagai sebuah sistem, dalam dunia siber juga memiliki etika yang mengatur nilai-nilai yang baik dan yang buruk. Berbeda dengan perundang-undangan yang memiliki sanksi tegas, etika ini hanya mengatur tentang apa yang boleh dan apa yang tidak boleh dilakukan oleh pengguna internet. Contohnya, nilai-nilai etis yang didefinisikan oleh the Computer Ethics Institue pada tahun 1992. Etika itu terdiri dari beberapa hal yang harus dijauhi oleh para pengguna internet, yaitu

a. tidak boleh menggunakan komputer untuk menyakiti orang lain
b. tidak boleh mengganggu perkerjaan orang lain
c. tidak boleh memata-matai file komputer milik orang lain
d. tidak boleh menggunakan komputer untuk mencuri
e. tidak boleh menggunakan komputer untuk membuat kesaksian palsu
f. tidak boleh menyalin atau menggunakan *software* yang tidak dibayar
g. tidak boleh menggunakan komputer orang lain tanpa otorisasi dari orang itu
h. tidak boleh mengakui hasil kerja intelektual orang lain
i. harus memikirkan konsekwensi sosial dari program atau sistem yang dibuat

j. harus menghormati orang lain

Nilai-nilai semacam ini juga bisa kita temukan dalam Undang-Undang ITE. Undang-undang itu telah mengatur asas-asas pemanfaatan teknologi informasi dan transaksi elektronik. Asas-asas itu ialah kepastian hukum, manfaat, kehati-hatian, iktikad baik, dan kebebasan memilih teknologi atau netral teknologi.

Dengan melihat banyaknya laporan mengenai kasus penipuan yang diterima kepolisian. Kita dapat meyakini bahwa etika di atas belum seperuhnya dilaksanakan oleh mereka yang terlibat dalam sebuah kasus *internet fraud*. Tidak hanya para pelaku, melainkan juga para korban yang tidak mengindahkan kehati-hatian dan kepastian hukum sebagai panduan bagi mereka untuk mencegah mereka menjadi korban sebuah kejahatan *cyber crime*. Oleh karena itu, sosialisasi etika ini sangat mendesak untuk dilakukan terhadap para pengguna internet. Sosialisasi ini akan lebih efektif jika diiringi dengan penegakan hukum. Efek jera yang disebabkan oleh penegakan hukum tentu akan mempertegas hal-hal yang diharuskan dan hal-hal yang dilarang dalam berinternet.



BAB 5
PENUTUP

5.1 Kesimpulan

Dari uraian sebelumnya, ada beberapa kesimpulan yang dapat kita tarik. Kesimpulan itu adalah

a. Dengan metode penafsiran ekstensif, Pasal 378 KUHP dapat diterapkan untuk melakukan penindakan terhadap kejahatan *internet fraud*. Namun, pengunaan pasal ini seharusnya tidak dilakukan lagi dengan keberadaan Undang-Undang ITE agar tidak bertentangan dengan azas *lex posterior derogat legi priori*.
b. Pada praktiknya, prosedur pasal 43 ayat (6) Undang-Undang ITE sulit untuk dipenuhi sehingga menghambat penegakan hukum dengan menerapkan pasal-pasal pidana dalam Undang-Undang ITE terhadap kasus *internet fraud* maupun kasus-kasus *cyber crime* lainnya.
c. Dalam kasus yang diteliti, para penegak hukum menggunakan prinsip teritorialitas dalam menentukan yurisdiksi dalam penegakan hukum terhadap kasus *internet fraud*. Namun, dengan dinerlakukannya pasal
d. Terdapat beberapa kendala yang dihadapi dalam penegakan hukum terhadap kejahatan *internet fraud*, yaitu
    1) adanya penafsiran yang berbeda dari para penegak hukum mengenai ketentuan-ketentuan Undang-Undang ITE,
    2) keterbatasan kemampuan penegak hukum akibat kurangnya pengalaman dalam menangani kasus *cyber crime*,.
    3) kurangnya sarana dan fasilitas yang berhubungan dengan pengolahan bukti digital,
    4) adanya anonimitas pelaku,

5) adanya keengganan korban untuk membuat laporan resmi atas kasus *internet fraud* yang dialaminya serta kesulitan pengumpulan keterangan saksi.

5.2 Saran

Mengacu pada kesimpulan di atas ada beberapa saran yang saya ajukan untuk memperlancar penegakan hukum terhadap kejahatan *internet fraud* dengan korban berdomisili di luar negeri. Saran-saran itu adalah

a. Diadakannya amandeman terhadap Undang-Undang ITE khususnya pasal-pasal yang menjadi hambatan seperti pasal 43 ayat (6) .
b. Peningkatan frekwensi dan intensitas pelatihan bagi para penegak hukum tentang penegakan hukum terhadap kejahatan *internet fraud.* Selain itu bagi jaksa dan hakim diadakan juga spesialiasi pelaksana penegakan hukum terhadap *cyber crime* sebagaimana yang diterapkan di kepolisian
c. Perumusan yang lebih luas tentang laporan dalam rancangan Undang-undang hukum acara pidana yang baru, khususnya dalam penerimaan laporan dan pemeriksaan saksi secara *online.*

DAFTAR PUSTAKA

Arief, Barda Nawawi. 2006. *Tindak Pidana Mayantara. Erkembangan kajian Cyber Crime di Indonesia.* Jakarta : Raja Grafindo Persada.

Audal, Joseph, Quincy Lu dan Peter Roman. 2008. Computer Crimes. Dalam *The American Criminal Law Review;* Spring 2008; 45, 2. Halaman 233-274.

Clifford, Ralph D. 2001. Dalam *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime.* Ed Tim Newburn. Cet ke-2. Durham: Carolina Academic Press.

Gading, Andi Mochamad D.P. 2004. Pelayanan Korban *Carding* oleh Unit V Infotek Direktorat II Ekonomi Bareskrim Polri. Skripsi, Perguruan Tinggi Ilmu Kepolsisian.

Golose, Petrus R. 2008. Manajemen Penyidikan Tindak Pidana Hacking.Studi Kasus : Penyidikan Tindak Pidana Hacking wbsite Partai Golkar oleh Unit V/IT & Cybercrime Bareskrim Polri. Disertasi, Universitas Indonesia.

Halstead, Karen D. 2008. A Management Construct in Investigating Cybercrime. Disertasi, The University of Tulsa.

Hamzah, Andi. 2008. *Hukum Acara Pidana di Indonesia.* Ed ke-2. Jakarta: Sinar Grafika.

Hikmiyati, Anisah. 2006. Penentuan Locus Delictie Dalam Cyber Crime Sebagai Usaha pembaharuan Hukum Pidana Nasional. Tesis, Universitas Indonesia.

Jewkes, Yvonne. 2003. Policing Cybercrime. Dalam *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime.* Ed Tim Newburn. Cet ke-2. Durham: Carolina Academic Press.

Lamintang, PAF. 1997. *Dasar-dasar Hukum Pidana Indonesia.* Bandung: PT Citra Aditya Bakti.

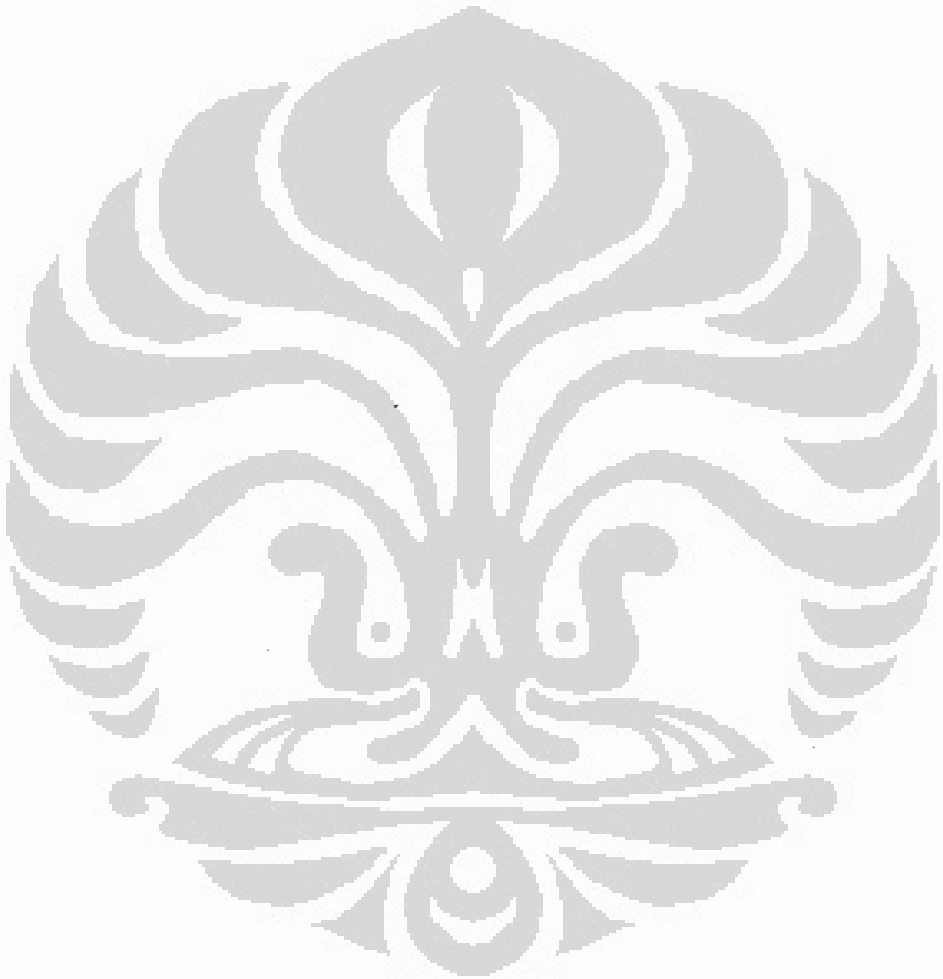
Mansur, Dikdik M.A. dan Elisatris Gultom. 2005. *Cyber Law Aspek Hukum Teknologi Informasi.* Bandung: PT Refika Aditama

Mertokusumo, Sudikno. 2002. *Meegenal Hukum (Suatu Pengantar).* Yogyakarta: Liberty Yogyakarta.

Nugroho, Hafid Ginanjar . 2006. Penentuan Locus Delictie Dalam Kejahatan Mayantara (Cyber Crime) : Studi Terhadap Bekerjanya Aparat Di Wilayah Hukum Pengadilan Negeri Sleman Yogyakarta. Skripsi, Universitas Sebelas Maret Surakarta.

Projodikoro, Wirjono. 1989. *Asas-Asas Hukum Pidana Indonesia.* Bandung : PT Eresco.

Rahardjo, Satjipto. 2006. *Ilmu Hukum.* Cet ke-6. Bandung: PT Citra Aditya Bakti.



Ramli, Ahmad. 2007. *Menuju Kepastian Hukum di Bidang Informasi dan Transaksi Elektronik.* Jakarta: Departemen Komunikasi dan Informatika Republik Indonesia.

Soekanto, Soerdjono. 2006. *Pengantar Penelitian Hukum* . Cetakan ke-3. Jakarta : UI Press.

Soekanto, Soerdjono. 2010. *FaktorFaktor yang Mempengaruhi Penegakan Hukum* . Cetakan ke-9. Jakarta : Rajawali.

Thomas, Douglas dan Brian D. Loader. Introduction-Cybercrime: Law Enforcement, Security and Surveilance in the Information Age. Dalam *Cybercrime: Law Enforcement, Security and Surveilance in the Information Age.* Ed. Douglas Thomas dan Brian D. Loader. London: Routledge.

Wagner, Cynthia G. 2009. Internet Fraud on the Rise. *The Futurist.* Juli-Agustus. 15.

Walker, Neil. 2003. The Pattern of Transnational Policing. Dalam *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime.* Ed. Tim Newburn. Cet ke-2. Durham: Carolina Academic Press.

Yar, Majid. 2006. *Cybercrime and Society.* London: Sage publication.

Wawancara

Wawancara dengan AKBP Dadang Sutrasno tanggal 25 Januari 2010

Wawancara dengan Kompol I Ketut Budi Hendrawan tanggal 25 Januari 2010

Wawancara dengan Kompol I Ketut Budi Hendrawan tanggal 2 Februari 2010

Wawancara dengan Kompol I Ketut Budi Hendrawan tanggal 1 April 2010

Wawancara dengan Kompol I Ketut Budi Hendrawan tanggal 13 April 2010

Wawancara dengan Kombes Pol Petrus Golose tanggal 12 Februari 2010

Wawancara dengan Raharjo Budi Kisnanto tanggal 5 Februari 2010

Wawancara dengan Raharjo Budi Kisnanto tanggal 15 Maret 2010

Wawancara dengan Raharjo Budi Kisnanto tanggal 1 April 2010

Wawancara dengan Faisal Adhi tanggal 16 Februari 2010

Wawancara dengan Ismail tanggal 17 Februari 2010

Wawancara dengan Iptu Maryudhi Salempang tanggal 1 April 2010

Wawancara dengan AKBP Parmin tanggal 13 April 2010

Wawancara dengan AKP Sonar Sandina Mayasir tanggal 26 April 2010