Volume 1 Issue 1, August 2018, Page. 1-14
P A L R E V | J O U R N A L O F LAW
ISSN : 2622-8408 – E-ISSN 2622-8616

PAMULANG
L A W R E V I E W

KEBIJAKAN APLIKASI TINDAK PIDANA SIBER (*CYBER CRIME*) DI INDONESIA

Budi Kristian Bivanda Putra
Pascasarjana Doktor Ilmu Hukum, Universitas Islam Bandung
budi.bivanda@gmail.com

Abstract

The government initiated the birth of the Law on Information and electronic transactions in an effort to prevent the occurrence of ciber crimes. The percentage of cyber crimes in Indonesia is 32%. This figure is certainly not a small number and certainly can have a serious impact on the protection and welfare of the Indonesian people This research emphasizes first, how the cyber crime policy in Indonesia in mitigating the second, how cyber prevention efforts in the future. The research method in this research is normative juridical using primary and secondary data analyzed qualitatively. First, law enforcement in dealing with cyber crimes in Indonesia has not been optimally implemented. Factors that influence law enforcement against cyber crimes include legal factors, law enforcement factors, facilities and facilities in law enforcement and community factors Second, prevention of cyber crimes in the future can be done by increasing facilities, knowledge and specialization and training of law enforcement officers in the cyber field as well as efforts to secure information systems through collaboration with Internet Service Providers (ISP).

Keywords: *Policy, Criminal Act, Cyber*

Abstrak

Pemerintah menginisiasi lahirnya Undang-undang mengenai Informasi dan transaksi elektronik dalam upaya mencegah terjadinya tindak pidana siber. Adapun presentase kejahatan siber (*cyber crimes*) di Indonesia adalah sebesar 32%. Angka ini tentunya bukanlah angka yang kecil dan tentunya dapat berdampak serius terhadap perlindungan dan kesejahteraan masyarakat Indonesia. Penelitian ini menekankan pada pertama, bagaimana kebijakan tindak pidana siber di Indonesia di dalam menanggulanginya kedua, bagaimana upaya penanggulangan siber di masa yang akan datang. Metode penelitian dalam penelitian ini yuridis normatif menggunakan data primer dan sekunder di analisis secara kualitatif. Hasil penelitian ini menunjukan *Pertama*, Penegakan hukum dalam penanggulangan *cyber crimes* di Indonesia belum dilaksanakan secara optimal. Faktor-faktor yang mempengaruhi penegakan hukum terhadap *cyber crimes* meliputi faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas dalam penegakan hukum dan faktor masyarakat. Kedua, Penanggulangan *cyber crimes* kedepan dapat dilakukan dengan cara meningkatkan fasilitas, pengetahuan dan spesialisasi dan pelatihan-pelatihan terhadap aparat penegak hukum di bidang *cyber* serta upaya pengamanan sistem informasi melalui kerjasama dengan *Internet Service Provider* (ISP).

Kata kunci: Kebijakan, Tindak Pidana, Siber

PENDAHULUAN

Peradaban dunia pada masa kini dicirikan dengan fenomena kemajuan teknologi informasi dan komunikasi yang berlangsung hampir di semua bidang kehidupan manusia. Revolusi yang dihasilkan oleh teknologi informasi dan komunikasi biasanya dilihat dari sudut pandang penurunan jarak geografis, penghilangan batas-batas negara dan zona waktu serta peningkatan efisiensi dalam pengumpulan, penyebaran, analisis dan mungkin juga penggunaan data.

Disamping berbagai hal positif yang diapat diambil dari kemajuan teknologi informasi dan transaksi elektronik komunikasi, perkembangannya yang pesat dari perkembangan internet juga menimbulkan sisi gelap (sisi negatif) yakni dalam bentuk kejahatan dan pelanggaran. *Internet* membuat kejahatan yang semula bersifat konvensional dan langsung seperti pengancaman, pencurian, pencemaran nama baik, pornografi, perjudian, penipuan hingga tindak pidana terorisme kini melalui media *internet* beberapa jenis tindak pidana tersebut dapat dilakukan secara *on line* oleh individu maupun kelompok dengan resiko tertangkap yang sangat kecil dengan akibat kerugian yang lebih besar baik untuk masyarakat maupun Negara (Petrus Reinhard Golose, 2006: 5).

Fenomena tindak pidana teknologi informasi merupakan bentuk kejahatan yang relatif baru apabila dibandingkan dengan bentuk-bentuk kejahatan lain yang sifatnya konvensional. Tindak pidana teknologi informasi muncul bersamaan dengan lahirnya revolusi teknologi informasi. Sebagaimana dikemukakan oleh Ronni R.Nitibaskara bahwa: "*Interaksi sosial yang meminimalisir kehadiran secara fisik, merupakan ciri lain revolusi teknologi informasi. Dengan interaksi*

semacam ini, penyimpangan hubungan sosial berupa kejahatan (crime) akan menyesuaikan bentuknya dengan karakter tersebut." (Tubagus Ronny Rahman Nitibaskara, 2001: 38.)

Penetrasi internet yang begitu besar apabila tidak dipergunakan dengan bijak maka akan melahirkan kejahatan di dunia maya atau yang diistilahkan dengan kejahatan siber atau *cyber crime* yang merupakan perkembangan lebih lanjut dari *computer crime*. Dunia maya (*cyberspace*) saat ini ternyata rentan terhadap perilaku kriminal. Sebagai contoh adalah praktik-praktik implantasi virus yang mencederai komputer di seluruh dunia, bank dan lembaga keuangan telah kehilangan uang dalam jumlah besar. Negara maju seperti Amerika Serikat dan Inggris dan beberapa negara lainnya mengungkapkan bahwa data tentang keamanan nasional telah dibobol dan di *download* oleh orang-orang yang tidak berkepentingan. Tindak pidanalain juga dapat dilakukan melalui media internet seperti pornografi anak, penyerangan terhadap *privacy* seseorang, perdagangan barang ilegal, atau hadirnya situs-situs yang meresahkan masyarakat. Contoh lain, bagi mereka yang senang akan perjudian dapat melakukannya dari rumah atau di kantor hanya dengan mengakses situs www.indobetonline.com atau dapat juga www.tebaknomor.com dan banyak lagi situs sejenis yang menyediakan fasilitas tersebut dan memanfaatkan fasilitas *internet bangking* untuk pembayarannya tanpa harus bertemu secara fisik.

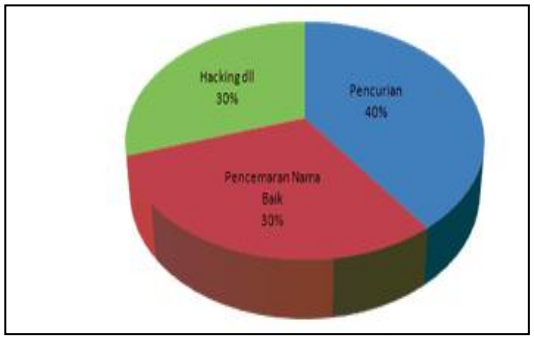
Selanjutnya, berdasarkan data Polri, kasus kejahatan dunia maya yang terjadi selama kurun waktu 4 (empat) tahun terakhir tercatat 48 (empat puluh delapan) kasus. Dari 48 (empat puluh delapan) kasus yang dilaporkan tersebut, 25 (dua puluh lima) kasus telah dinyatakan P-21.

oleh Jaksa Penuntut Umum. (Petrus Reinhard Golose, 2006: 6) Data Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, kasus kejahatan dunia maya selama kurun waktu 3 (tiga) tahun yang dilaporkan

sebanyak 37 (tiga puluh tujuh) kasus dan 14 (empat belas) kasus telah dinyatakan P-21 oleh Jaksa Penuntut Umum dan beberapa kasus telah mendapatkan vonis serta beberapa kasus dihentikan penyidikannya. Alasan dihentikannya penyidikan (SP-3) oleh penyidik dikarenakan tidak cukup bukti, dicabutnya pengaduan atas permintaan pelapor (kasus pencemaran nama baik), dan deportasi ke luar negeri (*handing over*). (Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, 2016)

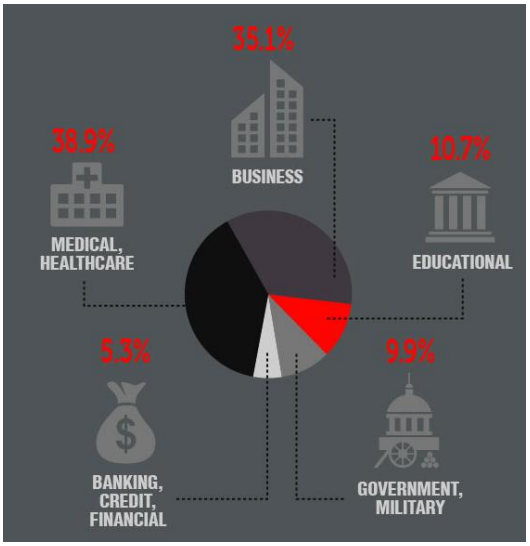
Dalam bentuk gambar, kejahatan siber dapat digambarkan dengan beberapa gambar sebagai berikut:

Gambar 1: Bentuk Kejahatan Siber (*Cyber Crimes*) di Indonesia.
(Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, 2016)



Dari gambar diatas, dapat dilihat bahwa bentuk tindak pidana siber yang marak terjadi di Indonesia adalah *Hacking* dan tindak pidana yang sejenisnya (30%), pencemaran nama baik (30%) dan pencurian (pencurian data atau pencurian informasi dan bentuk-bentuk pencurian lainnya) sebanyak 40%.

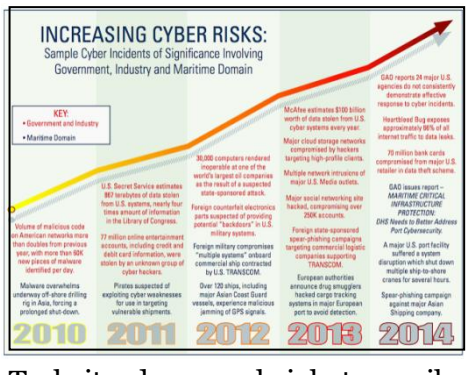
Gambar 2: Kejahatan Siber Pada Beberapa Industri.
(https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf)



Data diatas menunjukan bahwa institusi yang marak terserang kejahatan siber (*cyber crimes*) adalah sebagai berikut:

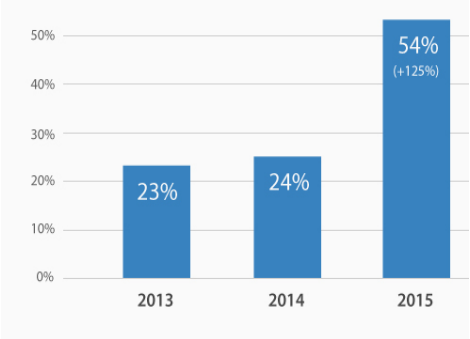
1. Institusi kesehatan: 38, 9%
2. Institusi Bisnis: 35,1%
3. Institusi Pendidikan: 10,7%
4. Institusi Militer: 9,9%
5. Institusi Perbankan dan Keuangan: 5,3%.

Gambar 3: Pertumbuhan Organisasi Kejahatan *Cyber*.
(https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf)



Terkait dengan kejahatan siber (*cyber crimes*) ini, data dari tahun 2010 sampai dengan tahun 2014 menunjukan bahwa kejahatan siber (*cyber crimes*) terus meningkat.

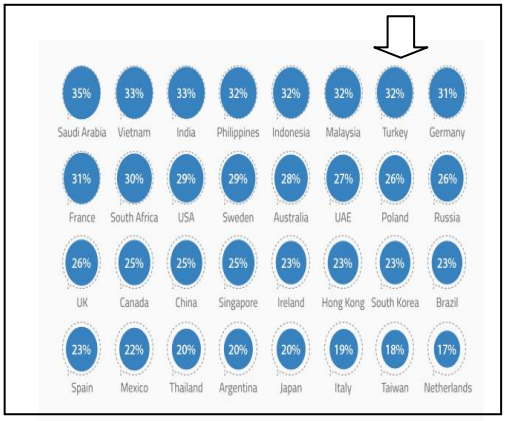
Gambar 4: Pertumbuhan Kejahatan Siber.
(http://www.euroforum.de/edpd/cyber-crime-darknet/)



Gambar di atas merupakan data dari tahun 2014-2015 yang menunjukan bahwa kejahatan siber (*cyber crimes*) mengalami peningkatan sebesar 125% dan terus meningkat dari tahun ke tahunnya.

Perlu pula disadari bahwa meningkatnya kejahatan siber (*cyber crimes*) di dunia telah membuat Indonesia masuk dalam salah satu Negara yang rawan dilakukannya tindak pidana atau kejahatan siber. Hal tersebut dapat digambarkan dengan gambar berikut ini:

Gambar 5: Posisi Indonesia Dibandingkan Dengan Negara-Negara Lain Terkait Dengan Kejahatan Siber (*Cyber Crimes*). (http://nasional.kompas.com/read/2015/05/12/06551741/Indonesia.Urutan.Kedua.Terbesar.Negara.Asal.Cyber)



Gambar di atas menunjukan bahwa Negara Indonesia menempati posisi ke 5 (lima) sebagai Negara yang marak dilakukannya kejahatan siber (*cyber crimes*) dibandingkan dengan Negara-negara lainnya di dunia. Terkait dengan kejahatan siber (*cyber crimes*), negara Indonesia berada dibawah Piliphina dan diatas Malaysia. Adapun presentase kejahatan siber (*cyber crimes*) di Indonesia adalah sebesar 32%. Angka ini tentunya bukanlah angka yang kecil dan tentunya dapat berdampak serius terhadap perlindungan dan kesejahteraan masyarakat Indonesia.

Dalam kenyataannya, penulis menemukan sebuah fakta bahwa meskipun telah ada berbagai peraturan perundang-undangan yang mengatur mengenai tindak pidana siber atau *cyber crime,* pelaku kejahatan tindak pidana siber atau *cyber crime* masih sulit untuk dijerat. Hal ini dikarenakan sifat dari kejahatan tersebut yang bersifat transnasional dan memiliki karakter-karakter tersendiri yang rumit. Untuk itu pada makalah ini, akan dibahas mengenai penegakan hukum atau kebijakan aplikasi terkait dengan penanggulangan tindak pidana siber atau *cyber crime* di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian yuridis normatif dan metode interpretasi. Jenis dan sumber data yang dipergunakan adalah data sekunder yang berupa bahan hukum primer, bahan hukum sekunder dan bahan hukum tertier. Data yang telah terkumpul akan dianalisis berdasarkan metode analisis secara kualitatif.

PERMASALAHAN

Berdasarkan beberapa hal tersebut di atas, makalah ini hendak membahas Pertama, bagaimana penegakan hukum (kebijakan aplikasi) dalam rangka menanggulangi kejahatan siber (*cybercrimes)* di Indonesia ? Kedua, Bagaimana upaya penanggulangan kejahatan siber di masa depan ?

PEMBAHASAN

Penegakan Hukum Kebijakan Aplikasi dalam Rangka Menanggulangi Kejahatan Siber (Cyber Crime) Di Indonesia

Perkembangan teknologi informasi di era globalisasi yang semakin berkembang serta diiringi dengan pembentukan hukum teknologi informasi dewasa ini hendaknya diikuti dengan langkah-langkah antisipatif oleh aparat penegak hukum untuk mencapai keseimbangan dan tata pergaulan di tengah-tengah kehidupan kelompok, golongan, ras dan suku, serta masyarakat, di dalam suatu negara maupaun dalam hubungan dengan pergaulan di kawasan regional dan internasional sehingga dapat menciptakan perlindungan yang baik dan kesejahteraan masyarakat Indonesia sebagaimana diamanatkan oleh alinea ke empat UUD 1945 sebagai tujuan nasional bangsa Indonesia sekaligus elemen dasar penyelenggaraan Negara hukum di Indonesia.

Berikut ini akan diuraikan faktor-faktor yang mempengaruhi penegakan hukum terhadap kejahatan siber (*ciber crimes)*. Faktor-faktor yang dimaksud yaitu sebagai berikut:

Penegakan hukum terhadap kejahatan siber sangat dipengaruhi oleh faktor hukum. Karena kejahatan siber berada pada anatomi kejahatan transnasional maka hukum yang digunakan adalah hukum nasional yang dalam pembahasan ini adalah hukum Indonesia. Namun sepanjang tidak diatur dalam hukum nasional maka yang dipergunakan adalah asas-asas, prinsip-prinsip dan kaidah hukum internasional.

Penanggulangan *cyber crime* oleh aparat penegak hukum sangat dipengaruhi oleh adanya peraturan perundang-undangan, terdapat beberapa perundang-undangan yang berkaitan dengan teknologi informasi khususnya kejahatan yang berkaitan dengan internet sebelum disahkannya UU ITE. Penegakkan hukum *cybercrime* sebelum disahkannya UU ITE dilakukan dengan menafsirkan *cyber crime* ke dalam perundang-undangan KUHP dan khususnya undang-undang yang terkait dengan perkembangan teknologi informasi *diantaranya*:

1. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi;
2. Undang-Undang No. 19 tahun 2002 sebagaimana telah diubah oleh Undang-Undang No. 28 Tahun 2014 tentang Hak Cipta;
3. Undang-Undang No 25 Tahun 2003 tentang Perubahan atas Undang-Undang No. 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang sebagaimana telah diganti dengan Undang-Undang No. 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang;
4. Undang-Undang No 15 Tahun 2003 tentang Pemberantasan Tindak Pidana Terorisme;
5. Dan lain sebagainya.

Dalam perkembangan terkini, dalam rangka mengatur *cyber space* dan kejahatan siber (*ciber crimes)* telah terbit Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik sebagai payung hukum. UU ITE ini diharapkan sebagai kekuatan pengendali dan penegak ketertiban bagi kegiatan pemanfaatan teknologi informasi tidak hanya terbatas pada kegiatan internet, tetapi semua kegiatan yang memanfaatkan perangkat komputer, dan instrumen elektronik lainnya.

Undang-undang ini telah memenuhi syarat keberlakuan hukum baik secara yuridis, sosiologis dan filosofis. Secara filosofis, lahirnya Undang-undang Nomor 11 Tahun 2008 Tentang Informasi

dan Transaksi Eleketronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik didasarkan amanat yang terkandung pada Pasal 28F Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 yang menyatakan "Setiap orang berhak untuk berkomunikasi dan memperoleh informasi dengan baik untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia. Secara yuridis, undang-undang ini telah mengatur mengenai segala sesuatu yang berkaitan dengan kegiatan internet, perangkat komputer, dan instrumen elektronik lainnya serta dibentuk oleh lembaga yang berwenang yakni Dewan Perwakilan Rakyat selaku legislator.

Secara sosiologis, masyarakat memang memerlukan Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik untuk mengatur berbagai aktivitas yang mereka lakukan selama berinteraksi di *cyber space*. Dinamika globalisasi informasi telah menuntut adanya suatu aturan untuk melindungi kepentingan para *netter* dalam mengakses pelbagai informasi. Pengaturan dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik ini sejalan dengan agama, nilai-nilai maupun kaidah moral yang diterima secara universal sehingga keberadaan *cyber law* (termasuk instrumen hukum internasional yang mengaturnya) diakui, diterima dan dilaksanakan oleh *information society*.

Dalam praktik penegakan hukum terhadap apapun bentuk kejahatan-kejahatan transnasional salah satunya kejahatan siber (*cyber crimes*), faktor hukum yang utama yang seringkali menjadi kendala penegakan hukum dalam praktik adalah masalah yurisdiksi. Masalah keraguan penentuan yurisdiksi dalam *cyber space* pun justru diakui oleh pakar hukum itu sendiri. Tien S. Saefullah yang menyatakan bahwa yurisdiksi suatu negara yang diakui hukum internasional dalam pengertian kovensional, didasarkan pada batas-batas geografis dan waktu sementara komunikasi dan informasi multimedia bersifat internasional, multi yurisdiksi dan tanpa batas-batas geografis sehingga sampai saat ini belum dapat dipastikan bagaimana yurisdiksi suatu negara dapat diberlakukan terhadap komunikasi multimedia dewasa ini sebagai salah satu pemanfaatan teknologi informasi. (Dikdik M. Arief Mansur dan Elisatris Gultom, 2005: 34)

Penentuan yurisdiksi merupakan suatu diskursus yang sangat penting dalam rangka penegakan *cyber law* apalagi dalam konsteks penegakan hukum terhadap kejahatan transnasional. Permasalahan mengenai yurisdiksi diatur dalam Pasal 2 Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik menyebutkan 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. Selanjutnya, dalam Pasal 1 angka 21 yang menyatakan bahwa "orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum."

Dalam penjelasan Pasal 2 disebutkan Undang-Undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/ atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan Teknologi Informasi untuk Informasi Elektronik dan Transaksi Elektronik dapat bersifat lintas teritorial atau universal. Yang dimaksud dengan "merugikan kepentingan Indonesia adalah 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.

"Darrel Menthe menyatakan bahwa yurisdiksi di *cyber space* membutuhkan prinsip-prinsip yang jelas yang berakar dari hukum internasional. Hanya melalui prinsip-prinsip yurisdiksi dalam hukum internasional ini, negara-negara dapat dihimbau untuk mengadopsi pemecahan yang sama terhadap pertanyaan mengenai yurisdiksi internet. (Dikdik M. Arief Mansur dan Elisatris Gultom, 2007: 38) Pendapat Menthe ini dapat ditafsirkan bahwa dengan diakuinya prinsip-prinsip yurisdiksi yang berlaku dalam hukum internasional dalam kegiatan *cyber space* oleh setiap negara, maka akan mudah bagi negara-negara untuk mengadakan kerjasama dalam rangka harmonisasi ketentuan-ketentuan pidana untuk menanggulangi *cyber crime*. Pada hakikatnya untuk menentukan yurisdiksi manakah yang dapat diterapkan dalam kegiatan *cyberspace*, termasuk di dalamnya *cyber crime*, tidak perlu dicari yurisdiksi tertentu yang lain dari pada yang lain (yurisdiksi dengan karakteristik khusus), karena sebenarnya prinsip-prinsip dalam hukum internasional sudah memadai untuk dipergunakan. (Dikdik M. Arief Mansur dan Elisatris Gultom, 2007: 38)

"Penentuan yurisdiksi *cyber crimes* dapat ditelaah dari asas-asas hukum internasional. Ada dua pandangan dari negara yakni perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang terjadi di dalam wilayah negara, baik dilakukan oleh warga negaranya sendiri maupun oleh orang asing (asas teritorial). Kedua, perundang-undangan hukum pidana berlaku bagi semua perbuatan pidana yang dilakukan oleh warga negara, dimana saja, juga di lua wilayah negara (asas personal). Juga dinamakan prinsip nasionalitas yang aktif. Lebih lanjut dikatakan bahwa dasar lain yang masuk akal bahwa hukum pidana di luar negara adalah asas melindungi kepentingan. Ini dapat dibedakan antara melindungi kepentingan nasional (prinsip nasional pasif) dan melindungi kepentingan internasional (prinsip universal). (Moeljatno, 1985: 38-40)"

Dalam substansi hukum di Amerika terdapat beberapa teori yang berkaitan dengan yurisdiksi di *cyber space* yakni: (Tien S. Saefullah, 2002: 102-103)

a. *The theory of the uploader and the downloader* (teori tentang mengunggah dan mengunduh). *Uploader* (pengunggah) adalah pihak yang memasukkan informasi elektronik ke dalam *cyber space* sedangkan *downloader* (pengunduh) adalah pihak yang mengakses informasi. Pada

umumnya, yurisdiksi mengenai perbuatan-perbuatan perdata dan tindak pidana tidak ada kesulitan. Suatu negara dapat melarang dalam wilayahnya kegiatan *uploading* dan *downloading* yang diperkirakan dapat bertentangan dengan kepentingan negaranya. Misalnya, suatu negara dapat melarang setiap orang untuk *uploading* kegiatan perjudian dalam wilayah negaranya dan melarang setiap orang dalam wilayahnya untuk *downloading* kegiatan perjudian.

b. *The theory of the law of the server* (teori hukum pusat penyedia). Pendekatan lain yang dapat digunakan adalah memperlakukan *server* dimana *webpages* secara fisik berlokasi, yaitu dimana mereka dicatat sebagai data elektronik. Menurut teori ini sebuah *webpages* yang berlokasi di *server* pada Standford University tunduk pada hukum California. Namun teori ini akan sulit dipergunakan apabila *uploader* berada dalam yurisdiksi asing.
c. *The theory of International Space* (teori ruang internasional). Menurut teori ini, *cyber space* adalah lingkungan hukum yang terpisah dengan hukum konvensional dimana setiap negara memiliki kedaulatan yang sama. Dalam kaitan dengan teori ini Menthe mengusulkan agar *cyber space* menjadi *fourth space*. Yang menjadi dasar analogi tidak terletak pada kesatuan fisik, melainkan pada sifat internasional yakni *sovereignless quality* (kualitas kedaulatan). Semua kegiatan dalam *cyber space* dianalogikan dengan kegiatan ruang angkasa. Semua kegiatan ini diatur secara bersama-sama.

Menurut Barda Nawawi Arief, membicarakan masalah yurisdiksi *cyber* pada hakikatnya berkaitan dengan masalah kekuasaan atau kewenangan, yaitu siapa yang berkuasa atau siapa yang berwenang mengatur dunia internet. Merujuk pada pendapat David R. Jhonson dan Davis G. Post, Barda Nawawi Arief menuliskan mengenai empat model yang saling bersaing yaitu: (Barda Nawawi Arief, 2006: 29-30.)

a. Pelaksanaan kontrol yang dilakukan oleh badan-badan pengadilan yang saat ini ada (*the existing judicial forums*).
b. Penguasa nasional melakukan kesepakatan internasional mengenai *the governance of cyber space*.
c. Pembentukan suatu organisasi internasional baru (*a New International Organization*) yang secara khusus menangani masalah-masalah di dunia internet.
d. Pemerintah atau pengaturan sendiri (*self governance*) oleh para pengguna internet.

Dari keempat model yang dikemukakannya itu, Johnson dan Post mendukung model ke-4 (*selfgovernance*) dengan alasan bahwa penerapan prinsip-prinsip tradisional dari *Due Process and Personal Jurisdiction* (proses dan yurisdiksi pribadi) tidak sesuai dan akan mengacaukan apabila diterapkan di dunia *cyber space*. *Cyber space* menurut mereka harus diperlakukan secara terpisah dari dunia nyata dengan menerapkan hukum yang berbeda untuk *cyber space* (*cyber space should be treated as a separate space from the real world by applying distinct law to cyber space*). (Barda Nawawi Arief, 2006: 30.)

Pandangan Johnson dan Post ini ternyata banyak mendapat kritikan dari para pakar hukum seperti Lawrence Lessig, Christoper Doran, Masaki Hamano termasuk juga Barda Nawawi Arief. Barda

Nawawi Arief sependapat dengan apa yang disampaikan oleh Masaki Hamano bahwa sistem hukum dan yurisdiksi nasional atau teritorial memang memiliki keterbatasan, namun tidak berarti di ruang *cyber* dibiarkan bebas tanpa hukum. *Cyber space* juga merupakan bagian atau perluasan dari lingkungan hidup (*life environment*) yang perlu dipelihara dan dijaga kualitasnya. Jadi merupakan kepentingan hukum yang harus dilindungi. (Barda Nawawi Arief, 2006: 31-32.) Apalagi keberadaan kejahatan siber atau *cyber crimes* yang berada pada anatomi kejahatan transnasional, dimana dalam teori hukum ditentukan bahwa yurisdiksi yang berlaku pada kejahatan transnasional adalah yurisdiksi teritorial. Hal ini juga didukung dengan *au dedere au punere* yang menyatakan bahwa *locus delicti*lah yang menjadi titik penentu dari yurisdiksi yang berlaku atas kejahatan yang dilakukan. Sehingga yurisdiksi yang berlaku bagi *cyber crimes* adalah yurisdiksi teritorial.

Salah satu elemen penggerak substansi hukum adalah struktur hukum. Agar hukum dirasakan manfaatnya, maka dibutuhkan jasa pelaku hukum yang kreatif menerjemahkan hukum itu dalam fora kepentingan-kepentingan sosial yang memang harus dilayaninya. (Bernard L. Tanya, Yoan N. Simanjuntak dan markus Yage, 2010: 213) Adapun struktur hukum yang dimaksud untuk menerjemahkan hukum adalah penegak hukum.

Penegak hukum atau orang yang bertugas menerapkan hukum mencakup ruang lingkup yang sangat luas. Sebab, menyangkut petugas pada strata atas, menengah dan bawah. Artinya di dalam melaksanakan tugas penerapan hukum, petugas seyogianya harus memiliki suatu pedoman salah satunya peraturan tertulis tertentu yang mencakup ruang lingkup tugasnya. (H. Zainuddin Ali, 2010: 9) Penegak hukum mencakup komponen sistem peradilan pidana yang terdiri dari Polisi, Jaksa, Hakim, Advokat dan Lembaga Pemasyarakatan. Di dalam penegakan hukum, H. Zainuddin Ali mengestimasi kemungkinan-kemungkinan yang dapat dihadapi petugas penegak hukum dalam melaksanakan tugas penegakan hukum: (H. Zainuddin Ali, 2010: 95.)

a. Sampai sejauh mana petugas terikat dengan peraturan yang ada.
b. Sampai batas-batas mana petugas berkenan memberikan kebijakan.
c. Teladan macam apakah yang sebaiknya diberikan oleh petugas kepada masyarakat.
d. Sampai sejauh manakah derajat sinkronisasi penugasan yang diberikan kepada para petugas sehingga memberikan batas-batas yang tepat pada wewenangnya.

"Berpijak pada estimasi yang disampaikan oleh H. Zainuddin Ali tersebut, maka dapat dianalisis mengenai kendala yang dihadapi penegak hukum dalam menanggulangi *cyber crimes* ini. Penegak hukum dalam menegakkan hukum seringkali masih menggunakan ketentuan dalam KUHP padahal sudah ada Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (pada kasus *carding*). Hal ini membuat terdakwa dengan mudah lepas dari jeratan hukum karena unsur-unsur pasal yang didakwakan tidak dapat dibuktikan. Kesalahan dalam menggunakan undang-undang memang sudah seringkali terlihat dalam kasus-kasus yang ditangani oleh penegak hukum dalam kasus kejahatan siber.

Ketidakcermatan penegak hukum ini disebabkan karena latar belakang pendidikan hukum yang belum memadai. Seorang penyidik tidak semuanya berpendidikan sarjana hukum, sehingga

wajar jika ia tidak mengerti kapan saat ia menggunakan suatu undang-undang atau pasal tertentu dalam kasus yang tengah dihadapinya. Ketidakcermatan penyidik ini juga didukung dengan sifat lemahnya mekanisme kontrol dari penuntut umum yang sesungguhnya mempunyai hak untuk mengembalikan berkas penyidikan saat prapenuntutan. Sehingga ketika terdakwa diadili maka unsur-unsur yang didakwakan tidak dapat dibuktikan.

Salah satu indikator dari kepatuhan hukum adalah teladan yang diberikan oleh penegak hukum kepada masyarakat. Namun penegak hukum seringkali melakukan perbuatan-perbuatan yang jauh dari keteladanan. Agak sulit bagi penegak hukum untuk menindak pelaku *cyber crimes* sementara ia sendiri justru menjadi pelaku atau bahkan pihak yang meindungi *cyber crimes* ini. Dalam kondisi seperti ini maka konsistensi hukum tidak mungkin ditegakkan. Kecanggihan perkembangan teknologi selain memberi manfaat bagi kesejahteraan masyarakat, juga telah terbukti merupakan prakondisi bagi peningkatan modus operandi kejahatan yang berkembang di masyarakat. Dalam kenyataannya secara tatanan praktis acapkali kecepatan pertumbuhan teknologi yang meningkatkan kecanggihan modus operandi kejahatan belum dapat diikuti dengan memadai pihak kepolisian. (Romli Atmasasmita, 2007: 118) Tidak semua kepolisian di daerah yang memiliki unit *cyber* padahal kejahatan ini berkembang sedemikian luas.

Kemampuan dari penegak hukum dalam menjaring pelaku pun masih diragukan karena mengungkap kejahatan di dunia maya memang memerlukan penguasaan teknologi yang bukan hanya sekadar untuk menggunakan dan mengetik atau mengoperasikan internet. Pakar teknologi informasi, Onno W. Purbo mengatakan bahwa untuk mengungkap *cyber crime* diperlukan penguasaan kemampuan teknologi yang tinggi. Untuk mendeteksinya, digunakan kategori ilmu forensik dalam dunia *hacker*.

Kemampuan berbahasa asing bagi polisi dan aparat penegak hukum lain pun masih perlu ditingkatkan jika ingin bekerjasama dengan penegak hukum di negara lain. Penguasaan bahasa asing ini hanyalah merupakan langkah awal dari terjalinnya kerjasama internasional yang baik, sebab hal yang paling penting adalah penentuan bahasa hukum yang digunakan untuk merumuskan tindak pidana. Apalagi jika terdapat perbedaan definisi mengenai *cyber crimes*.

Selanjutnya, respon penegak hukum terhadap laporan masyarakat masih sangat rendah. Penegak hukum seringkali mengatakan tidak ada kejahatan yang dimaksud tanpa menyelediki lebih lanjut. Birokrasi dalam penegakan hukum yang terlalu berbelit-belit selama ini justru menjadi hambatan bagi penegak hukum untuk menanggulangi kejahatan siber. Laporan pun sering ditanggapi dengan sikap yang tidak simpatik. Sikap-sikap birokratis dan anti kritik ini menjadikan penegak hukum sebagai bagian yang terpisah dari masyarakat. Dalam kondisi seperti ini, tidak mungkin ada kerjasama antara penegak hukum dan masyarakat dalam proses penegakan hukum.

Berdasarkan penjelasan diatas, dapat dilihat bahwa penegak hukum di Indonesia mengalami kesulitan dalam menghadapi merebaknya *cyber crimes*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukum yang memahami seluk-beluk teknologi informasi (internet), disamping itu aparat penegak hukum di daerah pun belum siap dalam mengantisipasi maraknya kejahatan ini karena masih banyak aparat penegak hukum yang gagap teknologi “gaptek” hal ini disebabkan oleh masih banyaknya institusi-institusi penegak hukum di daerah yang belum didukung dengan jaringan internet.

Upaya Penanggulangan Kejahatan Siber di Indonesia di masa depan

Belum optimalnya penegakan hukum terhadap *cyber crimes* disebabkan karena sarana dan fasilitas penegakan hukum yang belum memadai. Penegakan hukum terhadap *cyber crimes* mutlak memerlukan alat sebab karakteristik dari kejahatan ini adalah dilakukan dengan alat baik yang berwujud maupun yang tidak berwujud. Penentuan waktu dan tempat terjadinya *cyber crimes* ditentukan saat kapan alat itu bekerja efektif, oleh sebab itu analisis telematika sangat diperlukan dalam mengungkap kejahatan ini. Untuk menelusi, mendeteksi dan menanggulangi kejahatan ini Onno W. Purbo menjelaskan bahwa caranya sangat tergantung aplikasi dan topologi jaringan yang dipakai. Sebagian aplikasinya ada di *gnacktrack* dan *backtrack*. Hal ini menggambarkan bahwa sarana dan fasilitas yang memadai menjadi hal yang penting dalam proses penegakan hukum. Tanpa adanya sarana atau fasilitas tertentu, maka tidak mungkin penegakan hukum akan berlangsung dengan lancar. Sarana atau fasilitas tersebut antara lain, mencakup tenaga manusia yang berpendidikan dan trampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya. Kalau hal-hal itu tidak terpenuhi, maka mustahil penegakan hukum akan mencapai tujuannya.

Untuk meningkatkan upaya penanggulangan kejahatan siber atau *cyber crimes* yang semakin meningkat Polri dalam hal ini Bareskrim Mabes Polri telah berupaya melakukan sosialisasi mengenai kejahatan *cyber* dan cara penanganannya kepada satuan di kewilayahan (Polda). Sosialisasi tersebut dilakukan dengan cara melakukan pelatihan (pendidikan kejuruan) dan peningkatan kemampuan penyidikan anggota Polri dengan mengirimkan personel-nya ke berbagai macam kursus yang berkaitan dengan *cyber crimes*. Pengiriman personel Polri tidak hanya terbatas dilakukan dalam lingkup nasional tetapi juga dikirim untuk mengikuti kursus di negara-negara maju agar dapat diterapkan dan diaplikasikan di Indonesia.

Pelatihan, kursus dan ceramah kepada aparat penegak hukum lain (misalnya Jaksa dan Hakim) mengenai *cyber crimes* juga hendaknya dilaksanakan, dikarenakan Jaksa dan Hakim belum memiliki satuan unit khusus yang menangani kejahatan dunia maya sehingga diperlukan sosialisasi terutama setelah disahkannya UU ITE agar memiliki kesamaan persepsi dan pengertian yang sama dalam melakukan penanganan terhadap kejahatan siber. Jaksa dan Hakim *cyber* sangat dibutuhkan seiring dengan perkembangan tindak pidana teknologi yang semakin banyak terjadi di masyarakat yang akibatnya dapat dirasakan di satu daerah, di luar daerah perbuatan yang dilakukan bahkan di luar negeri. Kurangnya sarana dan prasarana dalam penegakan hukum *cyber crimes*, sangat berpengaruh terhadap kinerja aparat penegak hukum dalam menghadapi *high-tech crimes*.

Pencegahan dan penanggulangan terhadap *cyber crimes* membutuhkan pendekatan *penal* dan *non penal* yang integral dan membutuhkan keterpaduan. Membicarakan masyarakat adalah suatu keharusan atau kewajiban yang melekat pada perbincangan mengenai hukum. Hukum dan masyarakatnya merupakan dua sisi dari satu mata uang. Maka tanpa perbincangan mengenai masyarakat terlebih dahulu, sesungguhnya berbicara tentang hukum yang kosong. (Satjipto Rahardjo, 2009: 9)

Satjipto Rahardjo menyimpulkan bahwa “setiap anggota masyarakat sebagai pemegang peranan ditentukan tingkah lakunya oleh pola-pola peraturan yang diharapkan daripadanya baik oleh norma-norma hukum maupun oleh kekuatan-

kekuatan di luar hukum." (Satjipto Rahardjo, 2009: 27) Penegakan hukum berasal dari masyarakat dan bertujuan untuk mencapai kedamaian di dalam masyarakat. Oleh karena itu, dipandang dari sudut tertentu, maka masyarakat dapat mempengaruhi penegakan hukum tersebut. (Soerjono Soekanto, 2005: 45.) Pengaruh masyarakat dalam penegakan hukum ini ditelaah dari kesadaran hukum yang menjadi indikator dari derajat kepatuhan hukum.

Kesadaran hukum masyarakat sangat diperlukan dalam berteknologi dan rendahnya kesadaran hukum para *netter* menjadikan penegakan hukum terhadap *cyber crimes* tidak berjalan optimal. Tidak adanya kesadaran hukum para *netter* ini terlihat pada pemanfaatan sarana internet untuk melakukan berbagai jenis tindak pidana salah satunya memperjualbelikan layanan seks dan berbagai jenis tindak pidana lainnya.

Kesadaran hukum dari para korban untuk melaporkan kejahatan yang dialaminya masih sangat sedikit. Berdasarkan laporan *Symantec* bertajuk *Norton Cybercrime Report*, hampir satu dari dua (45 persen) korban kejahatan siber (*cyber crimes*) tidak pernah menyelesaikan secara tuntas kejahatan *cyber* yang mereka alami. Padahal, sebanyak 86 persen pengguna yang disurvei mengaku pernah menjadi korban pelaku kejahatan tindak pindana *cyber*. (http://teknologi.vivanews.com/news/read/180241-45--korban-cybercrime-tak-melapor) Korban dari kasus eksploitasi seksual pun jarang ada yang melaporkan, hal ini disebabkan karena korban malu apabila ada orang yang mengetahui kejadian yang dialaminya.

Kurangnya kesadaran hukum masyarakat berimplikasi dan pemahaman serta ketidaktaatan mereka terhadap hukum. Dikdik M. Arief Mansur dan Elisatris Gultom merumuskan beberapa alasan maka sampai saat ini kesadaran hukum masyarakat Indonesia masih sangat kurang, yakni: Sampai saat ini, kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cyber crime* masih dirasakan kurang. Hal ini disebabkan antara lain oleh kurangnya pemahaman dan pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan *cyber crime*. *Lack of information* ini menyebabkan upaya penanggulangan *cyber crime* mengalami kendala, dalam hal ini kendala yang berkenaan dengan penaatan hukum dan proses pengawasan (*controlling*) masyarakat terhadap setiap aktivitas ang diduga berkaitan dengan *cyber crime*. Dengan demikian, kiranya tepatlah jika dikatakan bahwa penegakan hukum yang optimal memerlukan kesadaran hukum dan kesadaran moral dari masyarakat.

PENUTUP

Simpulan

Pertama, Penegakan hukum dalam penanggulangan *cyber crimes* di Indonesia belum dilaksanakan secara optimal. Faktor-faktor yang akan mempengaruhi penegakan hukum terhadap *cyber crimes* meliputi faktor hukum, faktor penegak hukum, faktor sarana dan fasilitas dalam penegakan hukum dan faktor masyarakat. Dari keempat faktor tersebut, maka faktor yang paling berpengaruh pada lemahnya penegakan hukum yang ada terhadap penanggulangan *cyber crimes* dalam anatomi kejahatan transnasional adalah faktor hukum (substansi hukum) yang banyak mengandung kelemahan dan faktor penegak hukum. Yurisdiksi *cyber crimes* juga sangat berpengaruh dalam penegakan hukum, mengingat jarak, biaya dan kedaulatan masing-masing negara. Oleh karena itu dibutuhkan kerjasama Internasional baik secara *mutual assistance*, perjanjian ekstradisi dan kesepakatan atau kerjasama dengan negara-negara lain terkait kejahatan siber atau *cyber crimes* dalam upaya penegakan

hukum dalam menanggulangi tindak pidana teknologi informasi.

Kedua, Penanggulangan *cyber crimes* dapat dilakukan dengan cara meningkatkan fasilitas, pengetahuan dan spesialisasi dan pelatihan-pelatihan terhadap aparat penegak hukum di bidang *cyber* serta upaya pengamanan sistem informasi melalui kerjasama dengan *Internet Service Provider* (ISP) sebagai penyedia layanan internet serta perlunya perhatian pertanggungjawaban *provider*, melakukan pengamanan *software* jaringan komputer (dengan cara mengatur akses (*access control*), *firewall* , *Intruder Detection System* (IDS) dan melakukan b*ack-up* rutin), Pengamanan *hardware* (dengan cara penguncian komputer atau penggunaan *dial back),* pengamanan personalia (yang mencakup seleksi operator dari sisi intelektual dan moral, membuat perjanjian atau MoU antara operator dengan manajemen atau MoU diantara penegak hukum yang berkaitan dengan kejahatan siber (*cyber crimes*) ini dan lain sebagainya).

Saran

Pertama, Bagi para penegak hukum, dalam rangka penanggulangan *cyber crimes* di Indonesia para penegak hukum perlu mengadakan perjanjian dan/atau kerjasama dengan para penegak hukum di negara lain. hukum, melaksanakan perjanjian internasional dengan efektif, kerjasama antara penegak hukum serta peningkatan kualitas dan kuantitas sarana dan prasana dalam penegakan hukum dan dapat dibentuk nota kesepahaman atau MoU diantara penegak hukum yang mengatur mengenai teknis pelaksanaan penyidikan dan penuntutan terkait dengan kejahatan siber (*cyber crimes*).

Kedua, pemerintah, meningkatkan komitmen strategi/prioritas nasional perlu dilakukan misalnya dengan membentuk *cyber task force* dari lingkup pusat hingga ke daerah. Dengan demikian, ada satuan tugas khusus yang menangani kasus-kasus *cybercrime* seperti layaknya kasus korupsi, terorisme, narkoba dan sebagainya. Mengingat terkait yurisdiksi *cybercrime* bersifat *transnational,* penanggulangan tindak pidana ini dapat memanfaatkan internet (melalui *e-mail* atau *messanger*) dan *digital signature* sebagai sarana pemeriksaan sehingga dapat menghemat waktu, biaya dan jarak serta perlu dilakukan peningkatan komitmen moral dalam penegakan hukum terhadap kejahatan transnasional dengan cara melakukan sosialisasi dan pelatihan-pelatihan.

DAFTAR PUSTAKA

Arief, Barda Nawawi. “Tindak Pidana Mayantara (Perkembangan Kajian Cybercrime Di Indonesia)”. PT. Raja Grafindo Persada. Jakarta. 2006.

Ali, H. Zainuddin. “Filsafat Hukum”. Sinar Grafika. Jakarta. 2010.

Atmasasmita, Romli. Teori dan Kapita Selekta Krimonologi”. Refika Aditama. Bandung. 2007.

Direktorat II Ekonomi dan Khusus Unit V IT & *Cybercrime* Bareskrim Mabes Polri, pada Tahun 2016.

Moeljatno, “Azas-azas Hukum Pidana. Bina aksara. Jakarta. 1985.

Mansur, Dikdik M. Arief dan Elisatris Gultom, “Cyber Law: Aspek Hukum Teknologi Informasi”. Refika Aditama. Bandung. 2005.

Nitibaskara, Tubagus Ronny Rahman. “Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi”. Peradaban. Jakarta. 2001.

Rahardjo, Satjipto. “Hukum dan Perilaku Hidup yang Baik adalah Dasar Hukum yang Baik”. Kompas. Jakarta. 2009.

Soekanto, Soerjono. “Faktor-Faktor Yang Mempengaruhi Penegakan Hukum”, PT. Raja Grafindo Persada. Jakarta. 2005.

Saefullah, Tien S. “Jurisdiksi sebagai Upaya Penegakan Hukum dalam Kegiatan Cyberspace, artikel dalam Cyberlaw: Suatu Pengantar”. Pusat Studi *Cyberlaw* Fakultas Hukum UNPAD. ELIPS. 2002.

Yoan N, Bernard L. Tanya. Simanjuntak dan markus Yage, “Teori Hukum strategi Tertib Manusia Lintas Ruang dan Generasi”, Genta Publishing. Yogyakarta. 2010.

_____, “Urgensi Perlindungan Korban Kejahatan Antara Norma dan Realita”. RajaGrafindo Persada. Jakarta. 2007.

Golose, Petrus Reinhard. Perkembangan Cybercrime dan Upaya Penanganannya di Indonesia Oleh Polri, Makalah pada Seminar Nasional tentang “Penanganan Masalah Cybercrime di Indonesia dan Pengembangan Kebijakan Nasional yang Menyeluruh Terpadu”, diselenggarakan oleh Deplu. BI, dan DEPKOMINFO, Jakarta. 10 Agustus 2006.