ISSN: NO. 0854-2031

EFEKTIVITAS PENERAPAN UNDANG – UNDANG ITE DALAM TINDAK PIDANA CYBER CRIME

Rini Retno Winarni *

ABSTRACT

Crime in cyberspace is a growing problem both in terms of modus operandi as well as variety of crimes. The enactment - Law Number 11 Year 2008 on Information and Electronic Transactions (UUITE) is expected to overarching legal issues, especially in the field of telematics, although we recognize that there are imperfections found in the law, therefore the need for revision of some articles. Rule of law can not be separated from law enforcement issues involving many parties. Therefore, the success of law enforcement is affected by things that in general there are several factors, namely the Act / regulations, factors law enforcement include those formed and those applying the law, a factor means or facilities to support law enforcement, community factors cultural factors as work, creativity and taste which is based on human initiative in social life. Accordingly, many factors that influence the effectiveness of a law lies in the professional and optimal role, powers and functions of law enforcement officials in their duties.

Keywords: Effectiveness, UUITE, Cyber Crime

ABSTRAK

Kejahatan di dunia maya merupakan persoalan yang berkembang baik dari sisi modus operandi maupun ragam kejahatannya. Lahirnya Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) diharapkan mampu memayungi persoalan hukum khususnya di bidang telematika, meskipun disadari bahwa masih terdapat ketidaksempurnaan yang ditemukan dalam UU tersebut, oleh karena itu perlu adanya revisi terhadap beberapa pasal. Berlakunya hukum tidak lepas dari permasalahan penegakan hukum yang melibatkan banyak pihak. Oleh karena itu, keberhasilan penegakan hukum dipengaruhi oleh hal-hal yang secara umum ada beberapa faktor, yaitu perangkat Undang-Undang / peraturan, faktor penegak hukumnya meliputi pihak yang membentuk maupun yang menerapkan hukum, faktor sarana atau fasilitas yang mendukung penegakan hukum, faktor masyarakat, faktor budaya sebagai hasil karya, cipta dan rasa yang didasarkan pada karsa manusia di dalam pergaulan hidup. Dengan demikian, faktor yang banyak mempengaruhi efektivitas suatu perundang-undangan terletak pada profesional dan optimalnya peran, wewenang dan fungsi dari para penegak hukum dalam menjalankan tugasnya.

Kata Kunci: Efektivitas, UU ITE, Cyber Crime

^{*} Rini Retno Winarni, Dosen Fakultas Hukum, Universitas 17 Agustus 1945 Semarang, email: riniretnowinarni@gmail.com

PENDAHULUAN

Negara yang sedang berkembang tentunya membawa dampak positif dan negatif seperti misalnya dengan ilmu pengetahuan dan teknologi yang saat ini berkembang dengan pesat yang tentunya membawa dampak pula terhadap tingkat peradaban manusia yang membawa perubahan suatu yang besar dalam membetuk pola dan perilaku masyarakat.

Di Negara Indonesia khususnya untuk menuju kemajuan pada ilmu pengetahuan dan teknologi antara lain pada bidang telekomunikasi, informasi, dan komputer sangat pesat. Perkembangnya. orang menyebutnya sebagai revolusi teknologi informasi

Pada tahun 1980-an sebetulnya istilahteknologi informasi sudah mulai dipergunakan secara luas. Teknologi ini merupakan pengembangan dari teknologi komputer yang dipadukan dengan teknologi telekomunikasi. Teknologi informasi sendiri diartikan sebagai suatu teknologi yang berhubungan dengan pengolahan data menjadi informasi dan proses penyaluran data / informasi tersebut dalam batas – batas ruang dan waktu. ¹

Kecenderungan terus berkembang nya teknologi tentunya membawa berbagai implikasi yang harus segera diantisipasi dan juga diwaspadai. Upaya itu sekarang telah melahirkan suatu produk hukum dalam bentuk Undang – Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik (UU ITE).Namun dengan lahirnya ÙU ITE belum semua permasalahan menyangkut masalah ITE dapat tertangani. Persoalan tersebut antara lain dikarenakan: pertama,dengan lahirnya Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik tidak semata – mata UU ini bisa diketahui oleh masyarakat pengguna teknologi

Tetapi di dalam pelaksanaannya masih banyak ketentuan – ketentuan yang menyangkut tentang perbuatan jahat atau perbuatan yang dapat dihukum belum masuk dalam Undang - Undang ITE, seperti hal – hal yng diatur dalam buku 1 KUHP tidak ada dalam Undang – Undang ITE. Seperti kelalain atau khilaf, dimana lalai dan khilaf adalah kalimat yang sering dilakukan oleh manusia di dunia maya dan menimbulkan kerugian bagi dirinya sendiridan orang lain, diatur secara tersendiri dengan menggunakan pasal pasal tertentu. Namun di dunia maya (cyber space) kelalaian adalah tindakan fatal yang bisa menimbulkan kerugian yang tidak sedikit, bahkan bisa menghancurkansebuah negara sekalipun, Demikian juga terhadap pendistribusian informasi yang mengandung muatan mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yamg bermuatan penghinaan dan/atau pencemaran nama baik.Dengan demikian faktor yang banyak mempengaruhi efektivitas suatau perundang – undangan adalah profesional dan optimal pelaksanaan peran, wewenang dan fungsi dari para aparat penegak hukum,baik di dalam menjelaskan tugas yang dibebankan terhadap diri mereka ataupun dalam menegakkan perundang - undangan tersebut.

informasi dan praktisi hukum. Kedua, berbagai bentuk perkembangan teknologi yang menimbulkan penyelenggaraan dan jasa baru harus dapat diidentifikasikan dalam rangka antisipasi terhadap pemecahan berbagai persoalan teknis yang dianggap baru sehingga dapat dijadikan bahan untuk penyusunan berbagai peraturan pelaksanaan. Ketiga, pengayaan akan bidang – bidang hukum yang sifatnya sektotal (rejim hukum baru) akanmakin menambah semarak dinamika hukum akan menjadi bagian sistem hukum nasional.

¹ Richardus Eko Indrajit, 2000, *Sistem Informasi* dan *Teknologi Informasi*, ELex Media Komputindo, Jakarta: Gramedia.

Perumusan masalah

Berkaitan dengan latar belakang di atas, permasalahan yang akan dibahas dalam tulisan ini adalah : Evektivitas Penerapan Undang – Undang ITE dalam tindak pidana *cyber crime*.

Pembahasan

Pengertian Telematika

Istilah telematika berasal dari Perancis yang merupakan asal kata telematique yang menggambarkan berpadunya sistem jaringan komunikasi dan teknologi informasi². Sementara yang dimaksud dengan teknologi informasi hanyalah merujuk pada perkembangan perangkat—perangkat pengolah informasi, dalam perkembangan selanjutnya dalam praktik, istilah telematika (telecom munication and informatics) yang merupakan perpaduan antara komputer (computing) dan komunikasi (communication).

Oleh karena itu, istilah telematics juga dikenal sebagai the new hybrid technologi yang lahir akibat perkembangan teknologi digital telah mengakibatkan teknologi telekomunikasi dan informatika menjadi semakin terpadu atau populer dikenal dengan istilah konvergensi. Dalam perkembangan lebih lanjut,telematics tidak hanya melingkupi telekomunikasi dan informatika yang telah dikenal sebelumnya, akan tetapi media juga tidak menjadi bagian yang tak terpisahkan sebagai satu kesatuan konvergensi.

Pengertian cyber crime

Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut dengan *cyber crime*.³ Dari pengertian ini tampak bahwa

cyber crime mencakup smua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet. Dalam definisi ini tidak menyebut kan secara spesifik dari karakteristik cyber crime. Definisi ini mencakup segala kejahatan yang dalam modus operandinya menggunakan fasilitas internet.

Menurut Kepolisian Inggris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan / atau kriminil berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital⁴.

Sebelum Kita memberikan penjabaran atau pemahaman lebih lanjut tentang apa itu *cyber crime*, baiklah kita samakan dulu persepsi tentang Kejahatan Telematika dengan Kejahatan Komputer (*Computer Crimes*) atau Kejahatan Siber (*Cyber Crime*) apakah merupakan jenis kejahatan yang sama.

Pada dasarnya cyber crime merupakan kegiatan yang memanfaatkan komputer sebagai sarana atau media yang didukung oleh sistem telekomunikasi, baik menggunakan telepon atau wireles system yang menggunakan antena khusus yang nirkabel. Hal inilah yang disebut "telematika" yaitu konvergensi antar teknologi telekomunikasi, media dan informatika yang semula masing-masing berkembang secara terpisah.

Hal ini dapat dilihat pada pandangan Indra Safitri yang mengemuka kan bahwa kejahatan dunia maya adalah jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas suatu memiliki karakteristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan kepada tingkat keamanan yang fungsi dan kredibilitas dari sebuah informasi yang

² Edmon makarim,2004,Kompilasi Hukum Telematika, Jakarta: Rajar Grafindo Persada.hal
3

³ Ari Juliano Gema, 2000, Cyber Crime: Sebuah Fenomena di Dunia Maya, diakses pada www.theceli.com

⁴ Ade Maman Suherman, 2002. Kejahatan Internet Cybercrime. http://myeptik-nolnol.blogspot.co.id/2015/04/kejahatan-internet-cybercrime_21.html

disampaikan dan diakses oleh pelanggar internet⁵.

Cyber crime dipandang sebagai dunia komunikasi yang berbasis komputer, dalam kehidupan manusia yang dalam bahasa sehari-hari disebut "Internet" yaitu jaringan komputer yang menghubungkan antar negara antar benua yang berbasis protokol transmission control protocal / internet protokol. Cyber Space (Internet) telah mengubah jarak dan waktu menjadi tidak terbatas. Internet digambarkan sebagai kumpulan jaringan komputer yang terdiri dari sejumlah jaringan yang lebih kecil yang mempunyai sistem jaringan yang berbeda-beda⁶.

Beberapa Bentuk Cyber Crime

Ada beberapa bentuk *cyber crime* yang berhubungan erat dengan penggunaan teknologi yang berbasis komputer dan jaringan telekomunikasi, antara lain:

1. Unauthorized Access to Computer System and Service, yaitu kejahatan yang dilakukan ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa pengetahuan dari pemilik sistem jaringan komputer yang dimasukinnya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia. Namun begitu, ada juga yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus suatu sistem yang memiliki tingkat proteksi tinggi. Kejahatan ini semakin marak dengan berkembangnya teknologi internet.

Beberapa contoh yang berhubungan dengan hal tersebut, antara lain:

- 5 Indra Safitri, 1999, *Tindak Pidana di dunia cyber, Insiler, Legal, Journal From Indonesia Capital and Insvesment Market,* diakses http.businness for funecity.com
- 6 Kenny Wiston, 2002, The Internet: Issue of Jurisdictio and Controversies Surrounding Domain Names, Bandung: Citra Aditya, Hlm vii

- a. Pada tahun 1999, ketika masalah Timur Timor sedang hangat-hangatnya dibicarakan di level internasional, beberapa *website* milik pemerintah Republik Indonesia dirusak oleh *hacker*.
- b. Pada tahun 2000, *hacker* berhasil menembus masuk ke dalam *data base* sebuah perusahaan Amerika Serikat yang bergerak di bidang *e-commerce* yang memiliki tingkat kerahasiaan yang tinggi.
- c. Pada Tahun 2004, situs Komisi Pemeilihan Umum (KPU) dibobol *hacker* yang notabene memiliki tingkat keamanan yang sangat tinggi.
- 2. Illegal Contents, yaitu kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis, dan dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya adalah:
- a. Pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain.
- b. Pemuatan hal-hal yang berhubungan dengan pornografi.
- c. Pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propanganda untuk melawan pemerintah yang sah, dan sebagainya.
- 3. Data Forgery, yaitu kejahatan dengan memalsukan data pada dokumendokumen penting yang tersimpan sebagai scriptless document melalui internet. Kejahatan ini biasanya ditujukan pada dokumen-dokumen ecommerce dengan membuat seolaholah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku.
- 4. Cyber Espionage, yaitu kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer (computer network system) pihak sasaran. Kejahatan ini biasanya ditujukan

- terhadap saingan bisnis yang dokumen ataupun data-data pentingnya tersimpan dalam suatu sistem komputerisasi.
- 5. Cyber Sabotase and Extortion, yaitu kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang tersambung dengan internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku. Dalam beberapa kasus setelah hal tersebut terjadi, maka pelaku kejahatan tersebut menawarkan diri kepada korban untuk memperbaiki data, program komputer atau sistem jaringan komputer yang telah disabotase, tentunya dengan bayaran tertentu.
- 6. Offence Against Intellectual Property, yaitu kekayaan yang ditujukan terhadap hak kekayaan intelektual yang dimiliki seseorang di internet. Sebagai contoh adalah peniruan tampilan web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan rahasia dagang orang lain, dan sebagainya.
- 7. Infringements of Privacy, kejahatan yang ditujukan terhadap informasi seseorang yang merupakan hal yang sangat pribadi dan rahasia. Kejahatan ini biasanya ditujukan terhadap keterangan pribadi seseorang yang tersimpan pada formulir data pribadi yang tersimpan secara komputerisasi, yang apabila diketahui oleh orang lain, maka dapat merugikan orang secara material maupun imaterial, seperti nomor kartu kredit, nomor PIN ATM, keterangan tentang cacat atau penyakit tersembunyi, dan sebagainya.⁷

Di dalam meyikapi kejahatan dunia

maya harus ada kerjasama yang harmonis antara pemerintah, penegak hukum, ataupun masyarakat, karena selama ini kasus-kasus *cyber crime* yang terjadi di masyarakat bisa terungkap kalau memang ada laporan dari masyarakat dalam hal ini "korban".

Hukum dibutuhkan oleh masyarakat untuk menjadi lawan utama dari kejahatan atau hukum menjadi senjata istimewa guna menghadapi kejahatan yang sedang dan telah berkembang di tengah masyarakat. Senjata ini harus benar-benar berfungsi, sebab jika gagal mengfungsikan dirinya dalam menanggulangi atau memerangi kejahatan, maka citranya akan jatuh bukan lagi menjadi norma suci, melainkan menjadi norma yang impotensi.

Peranan pemerintah dalam UU No 11 Tahun 2008

1. Peran Pemerintah dan Peran Masyarakat Pengertian Peran Pemerintah dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam Pasal 40 adalah (i) pemerintah memfasilitasi pemanfaatan teknologi informasi dan transaksi elektronik; (ii) melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalah gunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum, sesuai dengan peraturan perundangundangan; (iii) Pemerintah menetapkan instansi atau institusi yang memiliki data elektronik strategis yang wajib dilindungi; (iv) Instansi atau institusi sebagaimana dimaksud pada butir (iii) harus membuat dokumen elektronik dan rekam cadang elektroniknya setelah menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data; (v) Instansi atau institusi lain selain diatur pada butir (iv) membuat dokumen elektronik dari rekam cadang elektroniknya sesuai dengan keperluan

⁷ Maskun, 2013, *Kejahatan Siber (Cyber Crime)*, Jakarta: Kencana, hlm 51-54

dengan perlindungan data yang dimilikinya 2. PeranMasyarakat

Peran masyarakat diatur dalam Pasal 41 Undang- Undang Nomor 11 Tahun 2008, yang dimaksud peran masyarakat dalam hal ini adalah: (i) masyarakat dapat berperan meningkatkan pemanfaatan teknologi informasi melalui penggunaan dan penyelenggaraan sistem elektronik dan transaksi elektronik sesuai dengan undangundang ini. Peran masyarakat sebagaimana dimaksud pada butir (i) dapat diselenggara kan melalui lembaga yang dibentuk oleh masyarakat yaitu lembaga yang bergerak di bidang teknologi informasi dan transaksi elektronik (iii) Lembaga sebagaimana dimaksud pada butir (ii) dapat memiliki fungsi konsultasi dan mediasi.

3. Pengertian Penegakan Hukum

Penegakan hukum mencakup lembaga-lembaga yang menerapkan (misalnya pengadilan, kejaksaan, kepolisi an), pejabat-pejabat yang memegang peran sebagai pelaksanaan atau penegak hukum (misalnya para hakim, jaksa, polisi) dan segi-segi administratif (misalnya proses peradilan, pengusutan, penahanan dan seterusnya).8 Menurut Jimly Asshidiqie: 9 penegakan hukum dalam arti luas mencakup kegiatan untuk melaksanakan dan menerapkan hukum serta melakukan tindakan hukum terhadap setiap penyelenggara atau penyimpangan hukum yang dilakukan oleh subjek hukum, baik melalui prosedur pengadilan ataupun melalui prosedur arbitrase dan mekanisme penyelesaian sengketa lainnya (alternative disputes nor conflict resolution). Bahkan dalam pengertian yang lebih luas lagi, kegiatan penegakan hukum mencakup pula segala sesuatu aktivitas yang dimaksudkan agar hukum sebagai perangkat kaidah normatif yang mengatur dan pengikat para subjek hukum dalam segala aspek Selanjutnya dikatakan bahwa dalam arti sempit, penegakan hukum itu menyangkut kegiatan peradilan terhadap setiap pelanggaran atau penyimpangan terhadap peraturan perundang-undangan, khususnya, yang lebih sempit lagi melalui proses peradilan pidana yang melibatkan peran aparat kepolisian, kejaksaan, advokat atau pengacara dan badan-badan peradilan.

Dalam kaitannya dengan tindak pidana informasi transaksi elektronik, penegakan hukumnya tidak dapat dilepaskan dari peranan dan komitmen para penegak hukumnya, yaitu: penyidik, penuntut umum, dan hakim. Penegak hukum harus mampu mengakomodasi harapan masyarakat akan rasa keadilan, bukan pembalasan dendam terhadap individu warga negara. Implementasi undang- undang ini khususnya dalam penegakan hukum, membutuhkan partisipasi masyarakat untuk membuat laporan atau pengaduan.

Untuk itu undang-undang akan efektif bilamana dapat memberikan motivasi kepada masyarakat untuk dapat menggunakan kewajibannya melaporkan adanya kejahatan tersebut sehingga penegak hukum, seperti polisi, jaksa, dan hakim dapat menindaklanjuti laporan atau pengaduan masyarakat itu untuk menjaga kewibawaan aparat penegak hukum itu agar tidak dituduh telah menyelewengkan perkara.

Cyber Crime dan Penegakan Hukum

Di dalam kejahatan cyber crime, kita tahu banyak cara hacker melakukan kejahatan atau aksinya melalui ranah internet, misal Microsoft dan Google serta berbagai website besar dunia hampir pernah di-hack oleh para hacker. Dunia hacker dan administrator website bagaikan pencuri dan saudagar, pencuri selalu mencari celah

kehidupan bermasyarakat dan bernegara benar-benar ditaati dan sungguh-sungguh dijalankan sebagaimana mestinya.

⁸ Jimly Assidiqie, 2006, Sekretaris Konstitusi dan Konstitusi Analisme, Jakarta: Sekretaris Jenderal dan Kepaniteraan Mahkamah Konstitusi RI, halm: 385

⁹ Ibid,., hlm 386

untuk dapat menjahati saudagar, bagaimana pun caranya. Sedikit berbeda dengan dunia "nyata", dalam dunia maya (internet) para pencuri tidak usah terburu-buru, bisa duduk santai sambil minum kopi, tidak perlu takut "ketangkap basah" sedang mencuri, bisa menentukan mana sasaran pertama, mana sasaran berikutnya. Kejahatan internet tidak terbatas pada pembobolan website (hacking), ada beberapa modus operasi kejahatan internet lainnya seperti: cardingkejahatan pemakaian kartu kredit untuk transaksi e-commerce dengan memakai kartu kredit asli tapi palsu (memakai kartu kredit orang lain), viruses- seperti juga virus dalam dunia "nyata" virus komputer merusak website, bahkan bisa masuk ke dalam program-program komputer pemakai jaringan. Pornografi dan Pornoaksi juga merupakan kejahatan yang terjadi di internet. Pornografi dan pornoaksi dilakukan dengan membuat website yang mengandung pesan-pesan tidak senonoh di internet, bahkan kadang-kadang disertai dengan perdagangan anak, dan perilaku asosial lainnya. Kejahatan-kejahatan tersebut perlu dicermati agar internet dapat lebih bermakna positif¹⁰

Paparan di atas dapat dipahami sebagai berikut:

1. Kejahatan (*crime*) merupakan potret realitas konkrit dari perkembangan kehidupan masyarakat, yang secara langsung maupun tidak telah atau sedang menggugat kondisi masyarakat, bahwa di dalam kehidupan masyarakat niscaya ada celah kerawanan yang potensial melahirkan individu-individu berperilaku menyimpang. Di dalam diri masyarakat ada pergulatan kepentingan yang tidak selalu dipenuhi dengan jalan yang benar, artinya ada cara-cara tidak benar dan melanggar hukum yang dilakukan oleh seseorang atau sekelompok orang guna memenuhi

- kepentingannya.
- 2. Cyber Crime dapat disebut sebagai kejahatan yang berelasi dengan kepenting an seseorang atau sekelompok orang. Ada seseorang yang memanfaatkan dan dimanfaatkan untuk memperluas daya jangkau cyber crime. Kepentingan bisnis, politik, budaya, agama, dan lain sebagainya dapat saja menjadi motif, alasan dan dalil yang membuat seseorang dan sekelompok orang terjerumus pada cyber crime.
- 3. Cyber Crime merupakan salah satu jenis kejahatan yang membahayakan kehidupan individu, masyarakat, dan negara. Jenis kejahatan ini (cyber crime) tidak tepat jika disebut sebagai "crime without victim", tetapi dapat dikategorikan sebagai kejahatan yang dapat menimbulkan korban berlapislapis baik secara privat maupun publik. Hak privat dapat terancam, terganggu, bahkan hilang/rusak akibat ulah segelintir orang atau beberapa orang yang memanfaatkan kelebihan ilmunya dan teknologi dengan modus operandi yang tergolong dalam cyber crime.
- 4. Cyber Crime telah menjadi kejahatan serius yang bisa membahayakan keamanan individu, masyarakat, negara, dan tatanan kehidupan global, karena pelaku-pelaku cyber crime secara umum adalah orang-orang yang mempunyai keunggulan kemampuan keilmuan dan teknologi. Siapapun orangnya yang puna kemampuan menggunakan internet bisa terjebak menjadi korban kejahatan ini. Namun, sebaliknya, seseorang juga dapat dengan mudah menjadi penjahatpenjahat akibat terkondisikan secara terus menerus atau dipaksa secara psikologis dan budaya untuk mengikuti serta berkiblat kepada pengaruh kriminalitas dan disnormatifitas yang dipenetrasi masyarakat global.
- 5. Korban dari kejahatan ruang maya (cyber crime) semakin hari semakin

¹⁰ Abdul Wahid & Mohammad Labib. 2010, *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT Refika Aditama, hlm. 134-135.

beragam. Kegiatan - kegiatan kenegaraan yang tentu sajasangat penting bagi kelangsungan hidup masyarakat dan negara tidak selalu bisa dijamin aman dari ancaman penjagapenjahatdi jagad maya ini. Hal ini menjadi suatu bukti, bahwa kemampu an intelektualitas dan teknologi pelaku kejahatan tidak bisa dianggap ringan oleh aparat penegak hukum. Dalam realitasnya, tindak kejahatan ini sudah demikian maju, yang tentu saja sulit disejajarkan dengan kemampuan aparat untuk menanganinya, apalagi bila aparat-aparatnya tidak selalu mendapat kan pelatihan-pelatihan yang memadai untuk mengimbangi dan mengantisipasi gerak kejahatan bargaya kontemporer.¹¹

Efektivitas Penerapan Undang-Undang ITE

Efektivitas berlakunya aspek pidana dalam UU ITE dilihat dari aspek subtansi dan struktur hukumnya yang meliputi penegak hukum, sumber daya aparatur penegak hukumnya peran serta masyarakat dalam konteks penegakan hukum dan juga harus didukung sarana dan prasarana supaya penegakan hukum terwujud.

Secara nyata di era globalisasi ini kita merasakan kemudahan dan manfaat yang besar atas hasil konvergensi antara telekomunikasi, informasi dan komputer dimana orang menyebutnya sebagai revolusi teknologi informasi. Hasil konvergensi tersebut salah satunya adalah aktivitas dalam dunia siber yang ber implikasi luas pada seluruh aspek kehidupan dan tidak mustahil dalam berbagai aktivitasnya terhadap berbagai permasalahan hukum.

Hal ini dirasakan dengan adanya pemanfaatan menyimpang atas berbagai bentuk aktivitas teknologi informasi, dapat dikatakan bahwa teknologi informasi digunakan sebagai sarana atau alat untuk melakukan kejahatan atau sebaliknya. Pengguna teknologi informasi dijadikan sasaran, sebagai contoh: sebuah data yang ada dalam CPU, data inilah yang sangat mudah untuk diubah, disadap, dipalsukan, dan dikirim ke berbagai Negara dalam hitungan detik dan akibatnyapun sangat dahsyat.

Perkembangan teknologi informasi tidak memberikan manfaat yang maksimal pada masyarakat. Teknologi digital memungkinkan penyalahgunaan informasi secara mudah, sehingga masalah keamanan sistem informasi menjadi sangat penting.

Pendekatan keamanan informasi harus dilakukan secara holistik, karena itu terdapat tiga pendekatan untuk mem pertahankan keamanan di dunia maya:

- 1. Pendekatan Teknologi
- 2. Pendekatan Sosial Budaya
- 3. Pendekatan Hukum¹²

Untuk mengatasi gangguan keamanan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa pengamanan jaringan akan sangat mudah disusupi, diintersepsi atau diakses secara ilegal dan tanpa hak untuk mengantisipasi segala persoalan kejahatan yang bersinggungan dengan teknologi informasi pemerintah telah mewujudkan rambu-rambu hukum yang tertuang dalam Undang-Undang Transaksi dan Informasi Elektronik (UU No. 11 Tahun 2008 yang disebut UU ITE), ini bentuk perlindungan kepada seluruh masyarakat dalam rangka menjamin kepastian hukum, dimana sebelumnya hal ini menjadi kerisauan semua pihak khususnya berkenaan dengan munculnya berbagai kegiatan berbasis elektronik.

Implementasi UU ITE memang belum efektif dalam menanggulangi cyber crime, terbukti dalam pasal 27 (3) UU ITE; yaitu "Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau

¹¹ Ibid, hlm. 134-135.

¹² Ahmad Romli, 2004, Cyberlaw dan HAKI Dalam Sistem Hukum di Indonesia, RefikaAditama, Hlm. 3

membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yamg memiliki muatan penghinaan dan/ataupencemaran nama baik".¹³

Bunyi pasal tersebut telah terjadi over criminalization dan berpotensi untuk disalah gunakan. Selain itu Pasal 27(3) dinilai tidak menyebutkan secara tegas, pasti, dan limitatif tentang perbuatan apa yang diklasifikasikan sebagai penghinaan.

Contoh Kasus Prita Mulyasari yang "curhat" melalui media elektronik berupa surat elektronik (e-mail) terhadap RS. Omni Internasional. Kejadian ini dapat terjadi setelah Prita Mulyasari menjadi pasien dari rumah sakit tersebut dan mengalami kesalahan diagnosis terhadap penyakitnya. Prita berasumsi bahwa terdapat kesenjangan dari pihak rumah sakit dalam memberikan diagnosis, namun hal ini dibatah dengan keras oleh pihak RS, Omni Internasional. "Curhatan" Prita inilah yang dianggap oleh pihak rumah sakit sebagai pencemaran nama baik.

Pada awalnya Prita Mulyasari dijerat dengan 3 (tiga) pasal tuntutan alternatif oleh jaksa penuntut umum yaitu pasal 45 ayat (1) jo. Pasal 27 ayat (3) UU no.11 tahun 2008 tentang ITE, pasal 310 ayat (2) dan pasal 311 ayat(1). Sebagaimana diketahui, 3(tiga) pasal tersebut dirancang untuk menjerat bagi pelaku yang diduga melakukan pencemaran nama baik dan penghinaan. Tetapi dinyatakan Prita Mulyasari bersalah pasal 27 ayat (3)jo. Pasal 45(1)UU No 11 tahun 2008 tentang ITE.

Meskipun sudah tertulis secara jelas pencemaran nama baik diatur dalam pasal 27 ayat 3 UU ITE tetapi sejak awal pengundangannya Dewan Pers sudah menolak keras dan meminta pemerintah dan DPR untuk meninjau kembali keberadaan isi dari beberapa pasal yang terdapat dalam UU ITE tersebut.Karena undang – undang tersebut sangat berbahaya

dan telah membatasi kebebasan berekpresi (mengeluarkan pendapat) seseorang. Selain beberapa aliansi menilai bahwa rumusan pasal tersebut sangatlah lentur multi interprestasi. Sehingga peraturan yang terdapat dalam pasal dan ayat Undang-Undang ITE tersebut harus dimaknai secara jelas dan dapat ditafsirkan secara rinci.

Pasal 27 ayat (3) telah melanggar lex certa dan kepastian hukum karena pasal 27(3) tidak dimuat dalam rumusan delik sejelas- jelasnya dan perumusan ketentuan pidana yang tidak jelas atau terlalu rumit hanya akan memunculkan ketidak pastian hukum,bahkan lebih jauh lagi melanggar kebebasan berekpresi, berpendapat, menyebarkan informasi, sebagai salah satu elemen penting dalam demokrasi.

Dari berbagai permasalahan atau kasus yang muncul dalam kejahatan cyber, memang tidak semua bisa diakomodir dalam undang-undang ITE, karena didalam undang-undang ITE tidak mengatur cara khusus hal-hal yang menyangkut cyber *crime*. Hal ini juga bisa kita lihat dalam bab ketentuan umum tidak secara jelas digambarkan tentang penjelasan kejahatankejahatan yang menggunakan komputer dalam dunia maya tidak tergambar secara jelas dan hanya sepotong-potong mengatur pemanfaatan teknologi yang sudah ber kembang dengan pesat dalam penggunaan nya. Disini bisa kita lihat peran pemerintah dalam proses membentuk undang-undang ITE masih menggunakan pendekatan politis - pragmatis dan tidak menggunakan kebijakan publik yang mekibatkan lebih banyak kalangan, sehingga tidak heran kalau UU ITE ini hanya sepotong-potong mengatur pemanfaatan teknologi yang sudah begitu luas penggunaannya di berbagai aspek kehidupan manusia.

Kalau kita cermati lebih dalam lagi seperti misalnya,yang diatur dalam KUHP

¹³ Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).

¹⁴ Zuliana Istichomah, 2013, Tinjauan UU No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Kasus Cyber Crime Oleh Iwab Piliang Berdasarkan Teori Hukum Pidana.

yaitu masalah khilaf dan lalai sedang dalam UU ITE belum diatur. hal ini sering dilakukan manusia untuk melakukan kejahatan ITE.Padahal akibat lalai yang dilakukan dalam kejahatan ITE menimbul kan kerugian pihak yang terkena dampak sangat luar biasa kerugiannya dan bahkan bisa fatal, bahkan akan mengancam atau menghancurkan sebuah negara, Dalam Undang - Undang ITE tidak menyebutkan sedikit pun tentang kelalaian yang dibuat oleh pembuat situs sehingga hacker bisa masuk dangan leluasa.Kegiatan yang lain yang sama pentingnya yaitu tentang percobaan sebagaimana yang dalam KUHP yaitu pasal 53 KUHP, juga tentang turut serta dalam kejahatan hacking dapat dipidana apa tidak belum jelas pengaturan nya. Begitu juga halnya tentang masa daluwarsa perbuatan pidana hacking. Semua kegiatan kejahatan tersebut diatur dalam bab tentang perbuatan - perbuatan apa saja yang dilarang, sehingga terkesan seperti pasal kranjang sampah.

Pada umumnya reaksi yang muncul para korban hacker hitam (cracker) adalah enggan untuk melaporkan kejahatan tersebut kepolisi karena mereka hanya beranggapan bahwa ini semua hanya sebuah kecelakaan, karena korban merasa malu kena tipu yang muncul hanya kesal pada para hacker, sebenarnya korban tau apa yang dilakukan cracker itu merupakan kejahatan.

Aparat Penegak hukum dalam hal ini adalah polisi menjadi sorotan para korban Cracker dalam menangani aktivitas hacking. Polisi belum dapat menangkap Cracker yang menghack sebuah situs, termasuk ketidak mampuannya menangkap Cracker yang menyerang situs Polri sendiri,sehingga langkah awal dari proses labeling justru didapat dari laporan—laporan media massa yang secara gencar memberitahukan akivitas Hacking, hal ini berkaitan sumber daya manusia para penegak hukum yang kurang memadai sehingga perlu adanya peningkatan

kualitasnya, karena merupakan kendala dalam proses pengungkapan tindak pidana cyber, dimana modus kejahatan cyber berkembang dengan pesat.

Dalam kasus - kasus yang terjadi seperti cyber crime sering mengalami hambatan terutama dalam hal penangkapan tersangka dan penyitaan barang bukti, seringkali kepolisian tidak dapat menentu kan secara pasti siapa pelakunya, karena para pelaku kejahatan dalam melakukan aksinya malalui komputer yang ada di "warnet", dimana di warnet jarang sekali melakukan "regristasi", inilah yang menyulitkan penyidikan untuk mencari barang bukti. Begitu juga dengan kasus "carding", saksi korban kebanyakan berada diluar negeri sehingga sangat menyulitkan dalam melakukan pelaporan dan pemeriksa an untuk dimintai keterangan dalam berita acara pemeriksaan saksi korban.

Penyelesaian berkas perkara, setelah penyidikan lengkap dan dituangkan dalam bentuk berkas perkara maka permasalahan yang ada adalah masalah barang bukti kerena belum samanya persepsi diantara aparat penegak hukum karena penafsiran yang berbeda mengenai isi undang – undang, serta barang bukti digital adalah barang bukti dalam kasus cyber crime yang perumusannya dan pengumpulan barang buktinya membutuh kan keahlian khusus sebab digital evidence tidak selalu dalam bentuk fisik yang nyata, hingga saat ini mengenai bentuk dari pada barang bukti digital (digital evidence) yang masih membutuhkan penafsiran dari ahli untuk menentukan keabsahannya.15

Penyempurnanan rumusan delik cyber crime, rumusan kriminalisasi perbuatan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan sebuah sistem elektronik masih terlalu banyak unsur yang harus

¹⁵ Besse Sugiswati. 2011, Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi. Surabaya: Fakultas Hukum Universitas Wijaya Kusuma Surabaya. Hal. 65

dibuktikan. Dalam Pasal 30 ayat (3) Undang-Undang ITE tidak dijelaskan tentang definisi *cyber crime*,jadi tidak diketahui sampai sejauh mana yang dinyatakan dengan unsur *cyber crime*, apakah akan melakukan atau percobaan melakukan kejahatan *cyber crime* dapat dikategorikan kejahatan belum jelas tertulis didalamnya.

Lain dari pada itu Undang-Undang ITE tidak mengatur mengenai pemidanaan bagi pelaku-pelaku yang perbuatan pidananya seharusnya masuk dalam kategori kejahatan cyber, antara lain: data leakage and espionage (membocorkan data dan mematai),identity theft and fraud. Oleh karena itu revisi Undang-Undang ITE diperlukan agar payung hukum atas tindak pidana cyber (cyber crime) bisa lebih konkrit dan komplit dalam menyelesaikan masalah-masalah cyber crime.

Penyempurnaaan hukum acara pemeriksaan cyber crime, untuk lebih meningkatkan efektivitas dan keberhasilan penegakkan hukum di dunia cyber crime, maka ketentuan yang mengatur mengenai hukum acara cybercrime atau pemeriksaan dalam setiap tingkatan perlu lebih diperjelas dan diperkuat. Kedudukan dan hubungan antara Undang -Undang ITE dan peraturan perundang-undangan terkait lainnya harus jelas dan harmonis agar tidak menimbulkan keragu-raguan dari aparat penegak hukum dalam penanganan perkara ITE. Karena sekarang ini banyak masyarakat yang menulis ajaran yang bersifat kebencian, tapi apa yang disampaikan di media sosial tersebut benar adanya, kalau aparat penegak hukum hanya memahami deliknya saja, maka penegak hukum seperti ini dianggap berjalan kebelakang, sehingga hukum acara yang digunakan dalam tindak pidana ITE haruslah diatur secara khusus.

Mengatasi kendala-kendala yang terdapat dalam Undang-Undang ITE dalam penanganan berbagai bentuk kejahatan dunia maya, upaya refisi Undang-Undang ITE, redefinisi pengertian dan peristilahan, perlu dilakukan dalam peraturan perundang-undangan ITE, sehingga tidak menimbulkan celah hukum (loopholes).¹⁶

Kesimpulan

Di era globalisasi ini kejahatan di dunia maya adalah persoalan baru dan perbuatan pidana yang berdimensi baru. Lahirnya Undang-Undang Informasi dan Transaksi Elektronik diharapkan dapat memayungi kejahatan telematika.Namun Undang-Undang tersebut masih memiliki kendala yuridis dan kendala penanganan tersangka. Masih banyak hal-hal/ketentuan ketentuan yang menyangkut perbuatan yang dapat di hukum belum masuk dalam Undang-Undang tersebut, sudah waktunya UU ITE direvisi agar tidak ada lagi yang dirugikan oleh pasal-pasal yang termuat didalam UU tersebut, sehingga dapat tercipta suatu tujuan hukum yang tidak hanya memberikan kepastian hukum tetapi juga memberikankeadilan dan kemanfaatan hukum, maka Undang-Undang Informasi Elektronik tidak efektif untuk melindungi kepentingan seluruh warga negara Indonesia. Dan juga Undang-Undang ITE tidak akan dapat dijalankan dan diterapakan dengan baik apabila tidak adanya kerjasama antara aparat penegak hukum dengan masyarakat luas. Dengan demikian faktor yang dapat mempengaruhi efektivitas suatu perundang-undangan adalah profesional dan optimal pelaksanaan peran, wewenang dan fungsi dari para penegak hukum, baik didalam menjalankan tugas yang dibebankan terhadap diri mereka ataupun dalam menegakkan peundang-undangan tersebut.

Saran

Undang-Undang ITE merupakan UU yang masih tergolong baru sehingga masih perlu perbaikan-perbaikan (revisi) terkait

16 Ibid, hal 65

dengan substansi/isinya, dan perlu adanya kecermatan dan ketelitian bagi para penegak hukum untuk memperoleh pemahaman yang integral mengenai substansi dari UU tersebut sehingga tidak ada lagi pihak yang merasa dirugikan.

Daftar Pustaka

- Abdul Wahid & Mohammad Labib, 2010, Kejahatan Mayantara (Cyber Crime), Bandung: PT Refika Aditama.
- Ade Maman Suherman, 2002, Kejahatan <u>Internet Cybercrime</u>, <u>http://myeptik-nolnol.blogspot.co.id/2015/04/kejahatan-internet-cybercrime 21.html</u>
- Ahmad Romli, 2004, *Cyberlawdan HAKI Dalam Sistem Hukum di Indonesia*,

 Refika Aditama.
- Ari Juliano Gema, 2000, Cyber Crime: Sebuah Fenomena di Dunia Maya, diakses pada www.theceli.com
- Besse Sugiswati, 2011, Aspek Hukum Pidana Telematika Terhadap Kemajuan Teknologi Di Era Informasi. Surabaya: Fakultas Hukum Universitas Wijaya Kusuma Surabaya.

- Edmon makarim,2004, *Kompilasi Hukum Telematika,jakarta:Rajar grafindo Persada*.
- Indra Safitri, 1999, *Tindak Pidana di dunia* cyber, Insiler, Legal, Journal From Indonesia Capital and Insvesment Market, diakses http.businness for funecity.com
- Jimly Assidiqie, 2006, Sekretaris Konstitusi dan Konstitusi Analisme, Jakarta: Sekretaris Jenderal dan Kepaniteraan Mahkamah Konstitusi RI.
- Kenny Wiston, 2002, The Internet: Issue of Jurisdictio and Controversies Surrounding Domain Names, Bandung: Citra Aditya.
- Maskun, 2013, *Kejahatan Siber(Cyber Crime)*, Jakarta: Kencana.
- Richardus EkoIndrajit, 2000, Sistem Informasi dan Teknologi Informasi, ELex Media Komputindo, Jakarta: Gramedia,
- Zuliana Istichomah, 2013, Tinjauan UU No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Kasus Cyber Crime Oleh Iwab Piliang Berdasarkan Teori Hukum Pidana.