

# EFEKTIVITAS UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK DI INDONESIA DALAM ASPEK HUKUM PIDANA

Radita Setiawan  
(raditasetiawan@rocketmail.com)  
Muhammad Okky Arista  
(okkyariesta@gmail.com)

## Abstrak

Jurnal ini bertujuan untuk mengetahui ke-efektifitas-an dari Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik di dalam perkembangan kejahatan pidana yang terjadi di Indonesia, khususnya dalam tindak pidana siber (Cyber Crime). Secara normatif, dengan dibentuknya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagai aturan baru yang berlaku dan semua penduduk dianggap telah mengetahui. Sebagai sebuah produk hukum dari kekuasaan Negara, Undang-Undang tersebut mempunyai fungsi sebagai alat kontrol negara terhadap sistem informasi dan transaksi elektronik yang bebas. Namun demikian ada beberapa hambatan yang dikatakan mengganggu efektifitas Undang-undang Informasi dan Transaksi Elektronik di Indonesia, yaitu antara lain, pertama, dalam efektifitas peraturan belum adanya pengaturan terhadap tindak pidana penipuan dengan menggunakan komputer. Kedua, dalam efektifitas tujuan undang-undang tersebut dikatakan belum mampu mencapai tujuan yang dimuat didalamnya. Perlu dilakukan beberapa pembenahan sistem dalam kehidupan masyarakat sebagai subyek hukum dan sebagai pengguna sarana teknologi informasi elektronik.

**Kata Kunci:** Undang-Undang No.11 tahun 2008, Informasi dan Transaksi Elektronik, Efektifitas, Hambatan, Perkembangan kejahatan pidana, Tindak Pidana Siber.

## Abstract

*The journal aims to find out the effectiveness of Indonesian Law no 11 of 2008 about Information and Electronic Transaction in the development of criminal offense that occurred in Indonesia, especially in the cyber criminal (cyber crime).*

*Normatively, Indonesian citizen is considered already know about the establishment of Information and Electronic Transaction Law no 11 of 2008 as the new regulation. As product of law from the state, regulation have a function as control system of Information and Electronic Transaction freedom. However, there are several barriers that is interfere the effectiveness of Indonesian regulation, such as firstly, there is not regulation of deception crime by using computer in the effectiveness rule. Secondly, in effectiveness rule, the goal of this regulation is not able yet to achieve the goal set forth therein. It needs to clearly the system of living as the subject of law and as Electronic Information Technology users.*

**Keywords:** Law no 11 of 2008, Information and Transaction Electronic, Effectiveness, Barrier, Development of criminal offense, Cyber crime.

## A. PENDAHULUAN

Kemajuan teknologi komputer yang terintegrasi dengan dunia *cyber* (internet) tidak dapat disangkal telah memunculkan berbagai macam kemudahan dalam berinteraksi antar subyek dalam satu negara bahkan antar dunia. Hal tersebut sebagai sebuah jaringan dunia yang telah dibentangkan dalam kemudahan komunikasi dan interaksi antar individu lintas jagad raya melalui media layar-layar mini berwujud datar. Inilah yang akhirnya dikenal dengan kemunculan dunia datar (*the world is flat*) yang mengesampingkan pendapat dan fakta bahwa dunia itu bulat dalam perwujudannya. Setiap orang di berbagai belahan dunia manapun, dengan bermodal sebuah alat komunikasi yang telah terhubung dengan jaringan internet, dapat mengakses dan memperoleh beragam data yang dia inginkan di dunia baru yang dinamakan dunia *cyber*.

Secara khusus, perkembangan teknologi komputer dan internet memberikan implikasi-implikasi yang signifikan dalam pengaturan dan pembentukan regulasi dalam ruang *cyber* dan hukum *cyber* serta terhadap perkembangan kejahatan dalam *cyberspace* atau yang sering disebut sebagai *cybercrimes*. Dari berbagai hal tersebut perlu ditekankan bahwa internet pada awalnya tidak pernah dirancang untuk *tracking and tracing user behavior*, tetapi dirancang untuk kebutuhan militer dalam menghadapi perang dunia pada saat itu.

Selain itu, pada awal pembentukan internet segala bentuk kerja dan sistemnya berada dalam sebuah kontrol administrator yang ketat. Sistem administrator ini mengontrol secara penuh sistem perangkat keras serta jaringan sebagai perangkat lunaknya. Terkait dengan apa yang dijelaskan tersebut, pada awalnya pengguna internet merupakan anggota komunitas yang dapat diidentifikasi sehingga ketika seorang pengguna melakukan penyalahgunaan jaringan dan perangkat, sistem administrator dapat secara sigap menindaklanjuti dan memberikan sanksi atas pelanggaran yang telah dilakukan. Akan tetapi, setelah internet dilegalisasikan untuk publik, sistem administrator yang dulunya berpusat pada satu titik (*central*) telah hilang dan bermunculan berbagai sistem administrator dari berbagai domain internet yang kemudian dikatakan beralih ke sistem administrator yang desentralisasi. Hal ini mengakibatkan aparat penegak hukum tidak memiliki kontrol yang kuat dalam pelacakan pelaku tindak pidana.

Hasil survei dari MarkPlus Insight Netizen Survei menyebutkan bahwa jumlah pengguna internet di Indonesia telah mencapai 61 juta orang pada tahun 2012. Jumlah itu membuat persentase pengguna internet dibanding jumlah penduduk adalah 23,5%. Dari jumlah tersebut, 40% di antaranya mengakses internet lebih dari 3 jam sehari. Adapun jumlah pengguna internet yang menggunakan perangkat mobile seperti ponsel dan tablet mencapai 58 juta jiwa. Sebuah penelitian yang dikutip dari Silicon India menyebutkan Indonesia menempati posisi ke delapan negara dengan pengguna internet terbanyak di dunia. Penelitian dari Boston Consulting Group menilai jumlah pengguna internet di Indonesia akan terus meningkat. Sampai angka tiga kali lipat di tahun 2015 dibandingkan tahun 2010. (Fino Yurio Kristo, *inet.detik.com* diakses pada 22 Oktober 2013, Pukul 16.30 WIB)

Kemajuan dalam hal informasi dan teknologi tersebut tidak selamanya berdampak positif bagi negara atau masyarakat karena dalam dampak positif selalu diikuti pula dampak negatifnya. Kemajuan terkadang justru menjadi sarana yang subur bagi perkembangan suatu kejahatan, dalam hal ini terkhusus kejahatan *cyber*.

Munculnya revolusi teknologi informasi dewasa ini dan masa depan tidak hanya membawa dampak pada perkembangan teknologi itu sendiri, akan tetapi juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi, masyarakat bahkan bangsa dan negara. Jaringan informasi global atau internet saat ini telah menjadi salah satu sarana untuk melakukan kejahatan baik domestik maupun internasional. Internet menjadi medium bagi pelaku kejahatan untuk melakukan kejahatan dengan sifatnya yang mondial, internasional dan melampaui batas ataupun kedaulatan suatu negara. Semua ini menjadi motif dan modus operandi yang amat menarik bagi para penjahat digital. (Abdullah, *cybercrime100.blogspot.com* diakses pada 20 September 2013, Pukul 21.00 WIB)

Secara normatif, dengan dibentuknya Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagai aturan baru yang berlaku dan semua penduduk dianggap telah mengetahuinya. Sebagai sebuah produk hukum dari kekuasaan Negara, Undang-Undang tersebut mempunyai fungsi sebagai alat kontrol negara terhadap sistem informasi dan transaksi elektronik yang bebas. Proses dalam menjalankan fungsinya tersebut akan terus berlangsung secara bertahap sesuai dengan kebutuhan dalam realitanya.

Dari latar belakang yang telah diuraikan di atas, persoalan yang muncul adalah apakah UU ITE dalam penerapannya telah mencapai efektifitas peraturannya maupun tujuannya?

## **B. PENDEKATAN DAN PENGATURAN CYBERLAW**

Realitas saat ini yang berakar dari konsep membuktikan bahwa masyarakat secara umum tidak dapat dipisahkan dengan kemajuan teknologi yang mendasari adanya kemudahan dalam mendapat informasi secara cepat. Meskipun kemajuan ini pertama kali hanya diusung oleh sekelompok orang tetapi merupakan proses dari sebuah sistem yang telah membudaya di masyarakat. Maka perlu diberlakukan sebuah hukum sebagai pengatur hal tersebut.

Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindak (perilaku) seseorang dan masyarakat yang telah melakukan pelanggaran dikenakan sanksi oleh negara. Meskipun dunia siber

adalah dunia virtual, hukum tetap diperlukan untuk mengatur sikap tindak masyarakat setidaknya karena dua hal. Pertama masyarakat yang ada di dunia virtual ialah masyarakat yang berasal dari dunia nyata; masyarakat memiliki nilai dan kepentingan baik secara sendiri-sendiri maupun bersama-sama yang harus dilindungi. Kedua, walaupun terjadi di dunia virtual transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata, baik secara ekonomis maupun non ekonomis. (Josua Sitompul, 2012 : 39)

Telah ada beberapa pendekatan atau teori untuk menggambarkan hubungan antara teknologi dan hukum, yaitu teori substantif dan teori instrumental.

#### 1. Teori Instrumental

Dalam teori Instrumental dijelaskan bahwa teknologi adalah alat yang dikembangkan secara rasional untuk memenuhi kebutuhan tertentu. Karena dikembangkan dengan prinsip rasionalitas dan efisiensi, teknologi memberikan pilihan-pilihan dan kebutuhan-kebutuhan yang rasional pula bagi masyarakat. Oleh karena itu, teknologi bersifat netral (tidak bersifat baik atau buruk) dan terpisah dari proses ekonomi, politik, sosial, dan budaya. Produktivitasnya dapat diukur secara obyektif, terlepas dari budaya, sehingga teknologi dapat dialihkan dari satu masyarakat ke masyarakat lain, atau dengan kata lain teknologi dapat diterapkan secara universal. (Cockfield and Pridmore, 2007 : 476)

Dalam hal tersebut dapat ditarik kesimpulan dari teori instrumental bahwa jika terjadi penyalahgunaan teknologi, maka pihak yang harus dipersalahkan adalah orang yang menyalahgunakan dan bukan teknologi itu sendiri.

#### 2. Teori Substantif

Dalam teori substantif diterangkan bahwa teknologi tidak netral karena teknologi teknologi berkaitan erat dengan kepentingan dari subjek yang membuat teknologi tersebut, sesuai yang dijelaskan pada bagian pendahuluan, sejarah perkembangan teknologi komputer dan internet dimaksudkan untuk memenuhi kebutuhan perang. Oleh karena itu, teknologi dapat menjadi sebuah alat yang berbahaya karena pembuat teknologi dapat mengontrol atau mendominasi orang atau masyarakat yang menggunakan teknologi tersebut melalui teknologi yang dibuatnya. (Cockfield and Pridmore, 2007 : 483)

Kedua teori tersebut dapat diterapkan dalam pembuatan kebijakan atau regulasi. Teori Instrumentalis memberikan pendekatan yang konservatif, kaku dan melihat ke belakang (*backward-looking*) dalam pembentukan kebijakan atau regulasi. Pendekatan ini disebut sebagai pendekatan “teknologi adalah hukum” (*technology is law*). (Josua Sitompul, 2012 : 41)

Dilain pihak, teori substantif memberikan pendekatan yang fleksibel, liberal, dan “melihat ke depan” (*forward-looking*) dalam pembentukan kebijakan atau regulasi. Pendekatan ini disebut sebagai pendekatan hukum adalah teknologi (*law is technology*). (Cockfield, 2004 : 501)

Perlunya dikembangkan dari kedua teori tersebut yang dipergunakan dalam pembentukan regulasi dengan maksud sebagai landasan pola pikir untuk memahami teknologi dan hukum yang dapat diterapkan dalam pembentukan regulasi di bidang teknologi, khususnya di bidang *cybercrime*.

### C. KEBERLAKUAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK DI INDONESIA

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) merupakan Undang-Undang pertama yang secara khusus mengatur tindak pidana siber di Indonesia. Berdasarkan surat presiden RI. No.R. /70/Pres/9/2005 tanggal 5 September 2005, naskah UU ITE secara resmi disampaikan kepada DPR RI kemudian disahkan pada tanggal 21 April 2008.

Meskipun telah terbentuk UU ITE di Indonesia tetapi dalam kenyataan atau realitanya dunia siber tetap sulit untuk dijinakkan karena *cyberspace* merupakan dunia virtual yang sulit ditemukan secara nyata tetapi dapat dikunjungi oleh berjuta pengguna di seluruh dunia setiap saat. Karakteristik inilah yang mempengaruhi UU ITE itu mempunyai kendala dalam penerapannya, karena pada kenyataannya tindak pidana siber sering bersifat lintas negara sehingga menimbulkan pertanyaan mengenai yuridiksi yang berlaku atas perbuatan atau akibat tindak pidana serta atas pelakunya. Hal ini disadari oleh Indonesia bahwa keterbatasan perundang-undangan konvensional yang dimiliki sulit untuk menjawab masalah ini, sehingga memandang perlu untuk menyesuaikan hukumnya untuk tetap menjaga kedaulatan negara serta kepentingan negara dan warganya.

Keberlakuan undang-undang pidana Indonesia yang diatur dalam KUHP didasarkan pada asas-asas yang berlaku secara internasional, antara lain asas teritorialitas, asas nasionalitas aktif, dan asas nasionalitas pasif. Dalam KUHP, asas teritorial yang dimaksud diatur dalam Pasal 2 KUHP, sedangkan perluasan asas ini diatur dalam pasal 3 KUHP.

Di dalam realita terjadinya suatu kejahatan dalam hal informasi dan transaksi elektronik terdapat beberapa hal yang menjadi masalah pokok dalam penegakan kasus tertentu. Dan yang menjadi pertanyaan besar adalah bilamana seorang warga negara asing atau badan hukum asing yang melakukan kejahatan di luar wilayah Indonesia, tetapi memiliki akibat hukum di Indonesia. Masalah seperti inilah yang menjadi salah satu keunikan tindak pidana *cyber* bahwa tindak pidana yang dilakukan di suatu negara dapat menimbulkan akibat yang dilarang di negara lain. Dari hal inilah timbul suatu permasalahan mengenai yuridiksi yang dapat melakukan *law enforcement* terhadap tindak pidana tersebut, maka tiap negara memiliki kedaulatan penuh terhadap wilayahnya. Sebagai solusi jitu menekankan bagi aparat hukum untuk melakukan kerjasama (*mutual assistance*) dengan aparat penegak hukum negara lain dalam mengungkap satu tindak pidana dan kepentingan tersebut harus dijustifikasi dengan peraturan perundang-undangan di negara Indonesia. Oleh karena itu, banyak negara menambahkan asas lain agar perundang-undangan pidananya tetap berlaku dalam kondisi-kondisi yang tidak dapat dijangkau dengan asas teritorialitas, khususnya dalam kondisi seperti diatas. Asas ini lebih dikenal dengan asas ekstrateritorialitas. (Josua Sitompul, 2012 : 137)

Dari hal ini dapat ditarik kesimpulan bahwa UU ITE menganut asas *extra territorial jurisdiction*. Hal ini terdapat dalam pasal 2 UU ITE. UU ITE berlaku untuk setiap Orang yang melakukan perbuatan melawan hukum sebagaimana diatur dalam UU ITE 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.

**Gambar 1. Asas Ekstrateritorial UU ITE**



Pasal 2 UU ITE tidak hanya menegaskan prinsip-prinsip teritorialitas yaitu bahwa undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum dalam wilayah Indonesia, tetapi juga memperluas ruang lingkup pengaturan prinsip ekstrateritorial yang diatur dalam KUHP dan dapat dikatakan memperluas cakupan asas ekstrateritorial nasionalitas pasif dalam KUHP dengan menambahkan kepentingan-kepentingan nasional yang dilindungi berdasarkan UU ITE. (Josua Sitompul 2012 : 139)

Dengan demikian, perbuatan hukum yang dilakukan baik oleh WNI maupun WNA di luar wilayah Indonesia atau baik oleh badan hukum Indonesia maupun badan hukum asing, sepanjang memiliki akibat hukum di Indonesia, dapat ditindak sesuai dengan UU ITE. ([www.batan.go.id](http://www.batan.go.id) Diakses pada 20 September 2013, Pukul 20.00 WIB)

#### D. CAKUPAN MATERI UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

Gejala kemunculan berbagai pelanggaran dari kebebasan dalam mendapatkan informasi secara cepat tersebut merupakan sebuah gejala mendunia. Tidak hanya terjadi dalam negara yang notabene merupakan negara maju, tetapi juga terjadi di negara-negara berkembang. Maka tidak mengherankan jika di Indonesia *cybercrimes* sudah sering terjadi akhir-akhir ini.

Di dalam Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) yang merupakan bentuk formal dari sebuah sistem dengan tujuan memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi. Kecemasan pengguna dan penyelenggara inilah maka terbentuklah sebuah Undang-Undang yang diyakini mampu sebagai *sistem kontrol* teknologi informasi.

Dalam sebuah Undang-Undang pasti mempunyai cakupan materi yang menjelaskan sejauh apa aturan di dalamnya. Hal ini tentunya perlu dijelaskan dan perlu diketahui tentang materi apa yang dicakup dalam UU ITE yang merupakan *cyberlaw* pertama di Indonesia yang mengatur secara khusus tentang informasi dan transaksi teknologi. Materi UU ITE dapat dikelompokkan menjadi dua bagian besar yaitu pengaturan informasi dan transaksi elektronik, dan pengaturan mengenai perbuatan yang dilarang (*cybercrime*). Dari pembagian besar tersebut hal ini dapat dilihat secara jelas dari struktur UU ITE itu sendiri, yaitu :

- *BAB I : Ketentuan UMUM*
- *BAB II : Asas dan Tujuan*
- *BAB III : Informasi, Dokumentasi, dan Tanda Tangan Elektronik*
- *BAB IV : Penyelenggara Sertifikasi Elektronik dan Sistem Elektronik*
- *BAB V : Transaksi Elektronik*
- *BAB VI : Nama Domain, HAKI, dan Perlindungan Hak Pribadi*
- *BAB VII : Perbuatan Yang Dilarang*
- *BAB VIII : Penyelesaian Sengketa*
- *BAB IX : Peran Pemerintah dan Peran Masyarakat*
- *BAB X : Penyidikan*
- *BAB XI : Ketentuan Pidana*
- *BAB XII : Ketentuan Peralihan*
- *BAB XIII : Ketentuan Penutup*

Dari banyaknya cakupan materi yang ada ada dalam strukturnya maka banyak yang beranggapan bahwa UU ITE ini terkesan tidak fokus. Dan dianggap lebih condong mengatur tentang teknologi informasi dalam pengertian yang luas. Dalam menanggapi keganjalan tersebut, pemerintah memberikan tanggapan bahwa cakupan *cyberlaws* sangat luas, karena meliputi transaksi elektronik, alat bukti elektronik, privasi, yurisdiksi, intellectual property, termasuk tindak pidana yang sering terjadi secara realita dan sulit di prediksi secara khusus.

Sebenarnya ada beberapa kelebihan yang diperoleh dengan menyatukan materi-materi tersebut dalam satu undang-undang. *Pertama*, penyatuan ini menghemat waktu karena jika tiap materi diatur dalam undang-undang sendiri, akan membutuhkan waktu lama untuk dibahas di DPR. *Kedua*, tim dapat melihat keseluruhan materi secara holistik dan mengatur agar keterkaitan materi-materi tersebut secara komprehensif.

Selain semua materi yang dicakup di dalamnya, UU ITE juga memiliki ketentuan-ketentuan yang telah berlaku secara internasional. UU ITE merujuk ketentuan dan prinsip-prinsip yang merupakan regulasi internasional dan sudah banyak diterapkan oleh negara-negara Eropa, Amerika dan Asia, ketentuan-ketentuan tersebut meliputi:

- UNCITRAL Model Law on Electronic Commerce;
- UNCITRAL Model Law on Electronic Signature;
- EU Directives on Electronic Commerce;
- EU Directives on Electronic Signature; dan
- Convention on Cybercrime;

Salah satu instrumen internasional yang mengatur *cybercrimes* secara regional adalah *Convention on Cybercrime*. Konvensi ini bertujuan untuk mengharmonisasikan hukum dari negara-negara anggota, baik hukum materiil maupun hukum prosedural, termasuk pengaturan mengenai kerjasama internasional dalam menagani *cybercrimes*. Oleh karena itu, konvensi ini mengatur tiga bagian penting, seperti : beberapa definisi yang digunakan dalam konvensi; hukum pidana materiil dan hukum pidana formil; serta kerjasama internasional. Materi yang ada dalam konvensi ini dijadikan acuan utama dalam pembentukan peraturan perundang-undangan mengenai tindak pidana siber oleh negara-negara di dunia, termasuk diterapkan dalam Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik di Indonesia. (Josua Sitompul, 2012 : 108)

Berdasarkan semua cakupan materi yang dibahas, dapat ditarik sebuah kesimpulan bahwa UU ITE secara keseluruhan banyak menerapkan *Convention on Cybercrime*. Apabila dilihat dari ketentuan Substantif (*substantive law*) dalam *Convention on Cybercrime* dibandingkan dengan perbuatan yang dilarang dalam UU ITE diperoleh hasil dalam tabel sebagai berikut:

**Gambar 2. Perbandingan *Cybercrime* dalam *Convention on Cybercrime* dan UU ITE**

<i>Convention on Cybercrime</i>	UU ITE
1. Article 2 - illegal access;	1. Distribusi, transmisi, membuat dapat diaksesnya konten tertentu yang ilegal (Pasal 27 s.d Pasal 29 UU ITE);
2. Article 3 - illegal interception;	2. illegal access (Pasal 30);
3. Article 4 - data interference;	3. illegal interception (Pasal 31);
4. Article 5 - system interference;	4. data interference (Pasal 32);
5. Article 6 - misuse of device;	5. system interference (Pasal 33);
6. Article 7 - computer-related forgery;	6. misuse of device (Pasal 34);
7. Article 8 - computer-related fraud;	7. computer related forgery (Pasal 35);
8. Article 9 - offence related to child pornography;	
9. Article 10 - offences related to infringements of copyright and related rights;	
10. Article 11 - attempt and aiding or abetting;	

Dari tabel diatas dapat dilihat bahwa pendekatan *Law is Technology* digunakan untuk *Cybercrime* yang ditujukan kepada kerahasiaan, integritas, ketersediaan informasi elektronik dan sistem elektronik.

#### **E. EFEKTIVITAS PERATURAN DAN TUJUAN DALAM PENERAPAN UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK**

Berbicara tentang efektifitas hukum mengharuskan penarikan kesimpulan terhadap realitas yang dapat mendorong dan menghambat bagi berlakunya dan pencapaian terhadap tujuan dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. Dalam hukum untuk menghantarkan pembicaraan kepada efektifitas Undang-Undang perlu dilakukan pembahasan dalam efektifitas atas peraturan dan efektifitas atas tujuan. Efektifitas peraturan adalah pembahasan atas Undang-undang berdasarkan norma positif yang termuat di dalamnya, sedangkan efektifitas tujuan adalah pembahasan atas pertanyaan apakah suatu undang-undang dapat mencapai tujuan yang diinginkan dengan dibentuknya suatu undang-undang. Perbedaan diantara efektifitas peraturan dan efektifitas tujuan perlu dilakukan karena tidak setiap peraturan yang berlaku efektif dapat mengantarkan kepada tujuan dibuatnya suatu peraturan. Rumusan normatif adalah rumusan analitis, dan rumusan analitis tidak dapat mengungkapkan semua faktor-faktor sosiologis, sebab faktor sosiologis sering muncul setelah berlakunya suatu undang-undang. Efektifitas peraturan lebih mudah dicapai daripada efektifitas tujuan. Karena efektifitas peraturan dikondisikan oleh variabel yang relatif lebih sedikit, lebih sederhana dan relatif dapat dianalisis secara normatif dan didukung oleh alat kekuasaan negara. Sedangkan efektifitas tujuan dikondisikan oleh variabel yang relatif lebih jauh, lebih kompleks, dan lebih rumit karena menyangkut faktor-faktor sosiologis yang kadang-kadang merupakan bentuk reaksi adanya suatu undang-undang.

Oleh karena itu, berikut ini dijelaskan mengenai efektifitas peraturan dan efektifitas tujuan dari Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

### 1. Efektifitas Peraturan dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Sebagai Undang-undang pertama dalam mengatur tentang hal yang berhubungan dengan teknologi elektronik, tentunya Undang-undang ini banyak memiliki berbagai kekurangan dalam pengaturannya. Berdasarkan materi cakupan yang telah dibahas sebelumnya, pembahasan dalam UU ITE itu terkesan tidak fokus dikarenakan banyaknya hal yang diatur tiap-tiap bab di dalamnya. Kemudian berdasarkan implementasi terhadap *Convention on Cybercrime* yang banyak digunakan sebagai pedoman penerapan oleh negara-negara secara umum dalam pengaturan hukumnya, banyak ketentuan *article 11 -attemp and aiding or abetting* dalam *Convention on Cybercrime* yang tidak diatur secara khusus dalam UU ITE. Hal tersebut dikarenakan dalam UU ITE tidak mengatur mengenai perbuatan penipuan dengan menggunakan komputer (*computer-related fraud*) seperti apa yang diatur dalam *Convention on Cybercrime*.

Berdasarkan hal tersebut dapat dikatakan bahwa UU ITE dalam peraturan yang dimuat belum efektif. Hal ini dikarenakan tidak dimuatnya perbuatan penipuan dengan menggunakan komputer dalam cakupan materi UU ITE. Dan secara realitas di Indonesia kejahatan penipuan dengan menggunakan sarana komputer masih relatif tinggi, seperti penipuan dengan menggunakan kartu kredit atau kartu ATM palsu. Pada tahun 2007 kasus pencurian identitas meningkat dari 748 laporan dan menimbulkan kerugian sekitar 4 miliar (2006) menjadi 451.198 laporan dan menimbulkan kerugian 6 miliar. Hal ini tentunya mengakibatkan kepentingan masyarakat luas menjadi terganggu dan kepercayaan dunia Internasional dalam melakukan transaksi secara elektronik di Indonesia dapat terancam.

Melalui berbagai penjelasan tersebut dapat ditarik sebuah kesimpulan bahwa perlu adanya pengaturan mengenai penipuan dengan menggunakan sarana komputer (*computer-related fraud*) dalam hukum positif Indonesia karena di dalam UU ITE pengaturan mengenai penipuan belum mencakup jenis kejahatan penipuan dengan menggunakan teknologi canggih dan kompleks. Dari hal tersebut dapat diharapkan adanya efektifitas peraturan dari Undang-undang tersebut.

### 2. Efektifitas Tujuan dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Dalam pembentukan setiap undang-undang pasti memiliki tujuan tertentu. Begitu pula dengan apa yang tercantum di dalam UU ITE, dijelaskan berbagai tujuan terhadap maksud dari pembentukannya. Dalam pasal 4 UU ITE dijelaskan mengenai pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan untuk mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia; mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat; meningkatkan efektifitas dan efisiensi pelayanan publik; membuka kesempatan seluas-luasnya kepada setiap orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; kemudian yang menjadi tujuan sebuah undang-undang secara umum adalah memberikan rasa aman, keadilan, dan kepastian hukum dalam undang-undang ini khususnya bagi pengguna dan penyelenggara Teknologi Informasi.

Kemudian dalam penerapan UU ITE agar mencapai tujuan seperti apa yang termuat dalam pasal 4, Indonesia mempunyai beberapa faktor penghambat, sebagai berikut:

- a. Jika dilihat dari segi teknologi, masyarakat dalam menggunakan fasilitas modern seperti teknologi masih cenderung bebas, artinya belum mengenal batasan-batasan dan aturan-aturan yang ada dalam UU ITE.
- b. Dalam tujuan perkembangan perdagangan dan perekonomian dengan menggunakan teknologi sebagai sarana, masyarakat Indonesia dalam bertransaksi elektronik masih kerap menjadi sorotan publik atas terjadinya pelanggaran yang sering terjadi, seperti : banyak pihak yang dirugikan dari jual-beli Online melalui website maupun Sosial Media.
- c. Di Indonesia dalam tujuan memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi dinyatakan belum kompeten, karena masih banyak pengguna yang masih mendistribusikan konten ilegal melalui website maupun sosial media, seperti : pornografi, SARA, pengancaman, dan pencemaran nama baik.

- d. UU ITE dikatakan belum memberikan rasa aman, keadilan, dan kepastian hukum dalam undang-undang ini khususnya bagi pengguna dan penyelenggara Teknologi Informasi. Hal ini dikarenakan aparat penegak hukum dalam menindaklanjuti kasus-kasus ITE dikatakan lelet dan tidak menimbulkan efek jera, sehingga masih banyak kejahatan ITE yang meresahkan masyarakat.

Guna mengatasi hambatan-hambatan tersebut dapat dilakukan berbagai upaya, sebagai berikut :

- a. Dilakukan berbagai seminar hukum terhadap masyarakat mengenai pentingnya penggunaan Teknologi Informasi yang baik dan benar sesuai dengan pengaturan hukum yang berlaku di Indonesia, yaitu UU ITE.
- b. Adanya penanganan yang lebih khusus terhadap *Cybercrimes* dengan pembangunan dan pengembangan *Computer Forensics*, serta pelatihan sumber daya manusia untuk mengoperasikan alat dan perangkat tersebut.
- c. Dilakukan pembatasan-pembatasan terhadap website-website yang mengandung unsur pornografi dan perjudian yang saat ini semakin banyak dan mudah untuk membuka konten tersebut.
- d. Dalam transaksi elektronik yang dilakukan tanpa perlu tatap muka antara penjual dan pembeli serta tidak adanya saksi yang melihat dan mendengar secara langsung, maka perlu dibentuknya suatu komunitas cyber sebagai wadah masyarakat dalam memberikan komentar negatif agar orang lain lebih berhati-hati terhadap berbagai website maupun oknum sebagai penawar suatu produk dan sering melakukan penipuan.

## F. PENUTUP

Undang-undang Informasi dan Transaksi Elektronik di Indonesia mempunyai potensi berlaku efektif, karena didukung oleh masyarakat yang saat ini cenderung selalu menggunakan teknologi informasi elektronik sebagai suatu kebutuhan pokok dalam menyikapi perkembangan zaman modern. Namun demikian ada beberapa hambatan yang dikatakan mengganggu efektifitas Undang-undang Informasi dan Transaksi Elektronik di Indonesia, yaitu antara lain, *pertama*, dalam efektifitas peraturan belum adanya pengaturan terhadap tindak pidana penipuan dengan menggunakan komputer, *kedua*, dalam efektifitas tujuan undang-undang tersebut dikatakan belum mampu mencapai tujuan yang dimuat didalamnya, perlu dilakukan beberapa pembenahan sistem dalam kehidupan masyarakat sebagai subyek hukum dan sebagai pengguna sarana teknologi informasi elektronik.

## DAFTAR PUSTAKA

- Abdullah. 2012. *Pelanggaran Hukum Dalam Dunia Maya (Cybercrime)*. cybercrime100.blogspot.com/2012/05/pelanggaran-hukum-dalam-dunia-maya.html. [20 September 2013, Pukul 21.00 WIB]
- Anonim. *Tanya Jawab Seputar UU ITE*. www.batan.go.id/sjk/uu-ite. [20 September 2013, Pukul 20.00 WIB]
- Cocfield, Arthur dan Jason Pridmore. *A Synthetic Theory of Law and Technology*, MINN. J.L. SCI. &TECH. 2007;8(2):475-531. www.mjlst.umn.edu. [29 September 2013, Pukul 12.00 WIB]
- Cockfield, Arthur. *Toward a Law and Technology Theory*, Manitoba Law Journal, Vol. 30, No 3. arthurcockfield.net.au.net. [29 September 2013, Pukul 14.00 WIB]
- Kristo, Fino Yurio. 2013. *Posisi Indonesia di Percaturan Teknologi Dunia*. <http://inet.detik.com/read/2013/08/21/112207/2336008/398/2/posisi-indonesia-di-percaturan-teknologi-dunia>. [22 Oktober 2013, Pukul 16.30 WIB]
- Sitompul, Josua. 2012. *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta : PT Tatanusa.