

**MENGANALISIS KESIAPAN INDONESIA DALAM PENANGGULANGAN DAN  
PENEGAKAN HUKUM KEJAHATAN GLOBAL BERBASIS INTERNET BERDASARKAN  
UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK**

**Agus Riwanto**

*Pengajar Fakultas Hukum dan Program Pascasarjana Ilmu Hukum  
Universitas Sebelas Maret Surakarta  
Email : [agusriwanto@yahoo.com](mailto:agusriwanto@yahoo.com)*

**ABSTRACT**

*Utilization of information technology, media and internet-based communications have changed the behavior of the global community and civilization. The world is now flooded with information that is fast, accurate and perfect. The crimes accelerating adverse financial, social, cultural and political. Cybercrimes can be categorized as an extraordinary crime because it has crossed the state border. Cybercrimes prevention can not be done using ordinary legal models only (conventional), but also by a special law design (cyberlaw). Indonesia has had Act 11 of 2008 on Information and Electronic Transactions. (UU ITE).*

*This study examines and learn more on this cybercrimes prevention policies based on UU ITE. Is the model of the arrangement was in accordance with the principles of the theory of criminalization policies and efforts to what should be done so that UU ITE can be effectively enforced, when compared with the setting cybercrimes committed several countries.*

*The method used is a socio-legal research, legal research that combines science, law and social science (interdisciplinary) With the approach of the principles / legal purposes. Data obtained from secondary data, literature (library research).*

*It was found that, setting criminalization is harmonization with the model adopted set forth in the Convention on Cybercrimes, but do not provide specific about pornography and child exploitation. Then the model is to make special rules. ITE Law does not regulate the matter of crime of Phishing and Spamming. The sanctions pidana still adhered to the classical model (classic school), reflected by the still imposing sanctions of imprisonment and fines and other sanctions are no alternatives. Criminalization policy in UU ITE is not in accordance with the theories of criminal policy is still multiple interpretations and ambiguous, not in accordance with the principles of the model law adopted in the Organization for Economic Co-operation and Development (OECD). This law is contrary to the Criminal Code in addition also contrary to the human rights aspects and in granting sanction differ from the prevalence of crime in the setting of a specific nature (lex), like the Election Law, the Child Protection Law, Law on Corruption, the Law Narkoba. Desain criminal policy in this ITE Law can not be effective, especially*

*when compared with the setting cybercrimes committed several countries, namely Azerbaijan, Beylorusia, Georgia, Hungary, Kazakhstan, Latvia, Peru and Russia were put, criminal social work, fines and revocation of certain rights as a way of giving sanctions on crime cybercrimes. In order UU ITE is to be effective then forwards the criminal politics cybercrmes Indonesia needs to adopt the models in these countries.*

**Keywords:** *Prevention and Law Enforcement, Cybercrimes, ITE Act.*

Pemanfaatan teknologi informasi, media dan komunikasi berbasis internet telah mengubah perilaku masyarakat maupun peradaban global. Dunia kini dibanjiri informasi yang cepat, akurat dan sempurna. Kejahatannyapun mengalami percepatan yang merugikan finansial, sosial, budaya dan politik. Kejahatan berbasis internet (*cybercrimes*) dapat dikategorikan sebagai kejahatan luar biasa (*extraordinary crimes*) karena telah melintasi batas negara (*transnational crimes*). Penanggulangan *cybercrimes* tidak dapat dilakukan dengan menggunakan model hukum biasa (konvensional), melainkan dengan melakukan desian hukum khusus (*cyberlaw*). Indonesia telah memiliki Undang-Undang No.11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik. (UU ITE).

Penelitian ini mengkaji dan mendalami tentang kebijakan penanggulangan kejahatan *cybercerimes* ini berdasarkan UU ITE. Apakah model pengaturannya telah sesuai dengan asas-asas dalam teori kebijakan kriminalisasi dan upaya apa yang harus dilakukan agar UU ITE ini dapat efektif ditegakan, bila dibandingkan dengan pengaturan *cybercrimes* yang dilakukan beberapa negara.

Metode yang digunakan adalah penelitian sosio-legal, yakni penelitian hukum menggabungkan ilmu hukum dan ilmu sosial (interdisipliner). Dengan pendekatan asas-asas/tujuan hukum. Data diperoleh dari data sekunder berupa data kepustakaan (*library research*).

Ditemukan hasil bahwa, pengaturan kriminalisasinya menganut model harmonisasi dengan kriminalisasi yang diatur dalam *Convention on Cybercrimes*, namun tidak mengatur secara tegas soal pornografi dan eksploitasi anak. Kemudian modelnya adalah dengan membuat aturan *lex specialis*. UU ITE ini tidak mengatur soal kejahatan *Phising* dan *Spamming*. Adapun pemberian sanksi pidanya masih menganut model klasik (*classic school*), dicerminkan dengan masih menjatuhkan sanksi pidana penjara dan denda dan tidak menyediakan alternatif sanksi lain. Kebijakan kriminalisasi dalam UU ITE tidak sesuai dengan teori-teori kebijakan kriminal masih multitafsir dan ambigu, tidak sesuai dengan asas *model law* yang dianut dalam *Organization for Economic Co-operation and Development* (OECD). UU ini selain bertentangan dengan KUHP juga bertentangan dengan aspek HAM dan dalam pemberian sanksinya berbeda dari kelaziman dalam pengaturan kejahatan yang bersifat khusus (*lex specialis*), seperti UU Pemilu, UU Perlindungan Anak, UU Korupsi, UU Narkoba. Desain kebijakan kriminal

dalam UU ITE ini tidak dapat berlaku secara efektif, terutama bila dibandingkan dengan pengaturan *cybercrimes* yang dilakukan beberapa negara, yakni Azerbaijan, Beylorusia, Georgia, Hungaria, Kazakstan, Latvia, Peru dan Rusia yang menempatkan, pidana kerja sosial, denda dan pencabutan hak-hak tertentu sebagai cara memberikan sanksi pada tindak kejahatan *cybercrimes*. Agar UU ITE ini dapat berlaku efektif maka ke depan politik kriminal *cybercrmes* Indonesia perlu mengadopsi pada model di negara-negara tersebut.

**Kata Kunci:** *Penanggulangan dan Penegakan Hukum, Kejahatan Internet, UU ITE.*

## I. PENDAHULUAN

Hari-hari ini hubungan antar manusia di berbagai belahan dunia dalam berbagai aspek: ekonomi, sosial, politik, tak lagi ada batas limitatif demografis dan seolah telah menyatu dalam satu rangkaian. Batas negara dan warga negara seolah hanyalah persoalan administrasi kependudukan saja, soal selera, gaya hidup dan kebutuhan telah mendunia. Inilah yang disebut dengan globalisasi, ia telah dijembatani oleh teknologi komunikasi yang modern yang berbasis komputer dan internet yang menyatukan antar manusia dalam satu jaringan global (*global networking*).

Kini bahkan pemanfaatan teknologi informasi internet telah merambah di semua sektor kehidupan, dari bisnis, politik, administrasi sampai hiburan yang berbasis domain *website* tertentu. Tak pelak lagi teknologi internet kian mempermudah akses publik untuk kesempurnaan hidup. Dunia kini dibanjiri informasi yang cepat, akurat dan sempurna begitupula kegiatan-kegiatan bisnis telah berbasis *e-commerce*, bahkan dalam politik dan demokrasi partisipasi publik dan menegemen telah meningkat pula dengan memanfaatkan basis internet berupa *e-government* dan *e-democracy*.<sup>1</sup>

Namun dibalik gegap-gempita teknologi internet tak jarang kinipun kejahatan berbasis pemanfaatan teknologi informasi pun mengalami percepatan yang luar biasa yang pola, cara dan modelnya beragam yang merugikan bukan saja secara finansial, tetapi juga sosial, budaya dan politik. Aktifitas yang terkait dengan kejahatan di dunia maya (*cybercrime*), penyalahgunaan penggunaan komputer, *hacking*, membocorkan *password*, *electronic banking*, pemanfaatan internet untuk

---

<sup>1</sup>. Isu-isu pemanfaatan teknologi informasi dalam aspek globalisasi, ekonomi, politik dapat dibaca pada tulisan, David Held, 1995, *Democracy and The Global Order, From The Modern State to Cosmopolitan Governance*, Politing Press, USA.

pemerintahan (*e-government*) dan kesehatan, masalah HaKI, penyalahgunaan nama domain, dan masalah privasi.<sup>2</sup>

Bahkan modus dan varian kejahatan ini terus mengalami kemajuan dan tak lagi hanya melibatkan jaringan lokal maupun nasional melainkan telah melibatkan jaringan internasional, pelaku kejahatannya pun tidak hanya tinggal di dalam satu negara tetapi diberbagai negara. Karena itu pola dan model penegakan hukumnya haruslah tidak konvensional melainkan dengan menerapkan asas-asas hukum internasional baik perdata maupun pidana.<sup>3</sup>

*Cybercrime* secara umum dapat diartikan sebagai perbuatan melawan hukum dan/atau tanpa hak berbasis teknologi informasi atau dengan memakai komputer dan/atau jaringan komputer sebagai sarana atau alat sehingga menjadikan komputer dan/atau jaringannya sebagai obyek maupun subyek tindak pidana yang dilakukan dengan sengaja. *Cybercrime* mempunyai dua tipologi: *Pertama*, mengandung kekerasan (*cybercrime with violence*), yang tergolong ini adalah *Cyberterrorism*, *Assault by Threat* (serangan dengan ancaman), *Cyberstalking* (penguntitan di Internet), *Child Pornography* (pornografi anak). Kedua, tanpa kekerasan (*cyber without violence*), diantaranya adalah: *Cybertrespass* (memasuki jaringan tanpa izin), *Cybertheft* (mencuri informasi), *Cyberfraud* (Penipuan di internet), *Destructive Cybercrimes* (merusak jaringan), *Cyber Prostitute Ads* (iklan internet prostitusi), *cybergambling* (perjudian di Internet), *Cyber Drugs Sales* (penjualan obat & narkotika di internet), dan *Cyber Laundering* (pencucian uang).<sup>4</sup>

Sedangkan menurut *The U.S. Department of Justice* memberikan pengertian *computer crime* sebagai: "...any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution". Pengertian tersebut identik dengan yang diberikan *Organization of European Community Development*,

---

<sup>2</sup>. Budi Raharjo, "Cyberlaw: Teritori dalam Cyberspace, Realitas dan Virtualitas", *Makalah*, Dipresentasikan pada Seminar "IT Within" yang diselenggarakan oleh Himpunan Mahasiswa Informatika ITB, 18 Februari 2006. Dalam soal kebijakan hukum *cybercrime* di Indonesia dapat dibaca karya, Emiliana Krisnawati, "Problematika Cyberlaw bagi Perkembangan Hukum Indonesia", dalam Satya Arinanto (Editor), Satya Arinanto dan Ninuk Triyanti (eds), *Memahami Hukum dari Konstruksi Sampai Implementasi*, (Rajawali Press, Jakarta, 2009), hal, 178.

<sup>3</sup>. Mengenai varian dan model kejahatan *cybercrimes* berikut cara mengatasinya dengan menerapkan model hukum lokal dan internasional dapat dibaca melalui dua disertasi yang telah dibukukan: yakni Abdul Halim Barkatullah, 2009, *Perlindungan Hukum Bagi Konsumen Dalam Transaksi e-commerce Lintas Negara Indonesia*, FH UII Press, Yogyakarta dan Shinta Dewi, 2009, *Cyberlaw Atas Informasi Pribadi dalam e-commerce Menurut Hukum Internasional*, Widya Pajajaran Press, Bandung.

<sup>4</sup> . <http://balianzahab.wordpress.com/cybercrime/hacker-dan-cracker/>, diakses pada tanggal 22/4/2010.

yang mendefinisikan *computer crime* sebagai: “any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data”.<sup>5</sup>

Adapun secara hukum menurut Andi Hamzah, mengartikan kejahatan komputer sebagai: “Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal”.<sup>6</sup>

Karena cara penanggulanganyapun tidak dapat dilakukan dengan menggunakan model-model hukum biasa (konvensional) melainkan dengan melakukan desian hukum khusus (*cyberlaw*). Prakarsa menyusun peraturan khusus di bidang *Cyberlaw* ini telah dilakukan pemerintah Indonesia melalui Depkoinfo RI dan telah berhasil menyusun UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.<sup>7</sup>

Undang-Undang Informasi dan Transaksi Elektronik memuat beberapa hal yakni: masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara e-commerce, azas persaingan usaha usaha tidak sehat dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas *cybercrime*.

Di tingkat Internasional Perserikatan Bangsa-Bangsa melalui komisi khususnya, *The United Nations Commissions on International Trade Law (UNCITRAL)*, telah mengeluarkan 2 *guidelines* yang terkait dengan transaksi elektronik, yaitu *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996* dan *UNCITRAL Model Law on Electronic Signature with Guide to Enactment 2001*. Sedangkan di Uni Eropa, dalam upaya mengantisipasi masalah-masalah pidana di *cyberspace*, Uni Eropa mengadakan *Convention on Cybercrime* yang didalamnya membahas jenis-jenis kejahatan apa saja yang dikategorikan sebagai *cyber crime*. Di bidang perdagangan elektronik, Uni Eropa mengeluarkan *The General EU Electronic Commerce Directive, Electronic Signature Directive, dan Brussels Convention on Online Transactions*. Aturan-aturan serupa juga dikeluarkan lembaga-lembaga internasional seperti WTO, ASEAN, APEC dan OECD.<sup>8</sup>

Saat ini hampir seluruh negara-negara di dunia telah memiliki UU yang mengatur tentang *cybercrime* ini dengan berbagai macam model dan variasi. Berdasarkan pada *Convention on Cybercrime* yang ditandatangani di Budhapest (Hungaria) pada tanggal 23 November 2001. Paling tidak 70 negara telah

---

<sup>5</sup> . ([www.usdoj.gov/criminal/cybercrimes](http://www.usdoj.gov/criminal/cybercrimes)), diakses pada tanggal 26/4/2010.

<sup>6</sup> . Andi Hamzah. 1989, *Hukum Pidana Yang Berkaitan dengan Komputer*, Sinar Grafika, Jakarta.

<sup>7</sup> . Cahyana Ahmad Jayadi, “Perlunya Cyberlaw dalam Rangka Menghadapi dan Menanggulangi Kejahatan Dunia Maya”, *Makalah* di sampaikan dalam seminar RUU ITE, pada 12 April 2007.

<sup>8</sup> . Arifyadi, “Cyberlaw: Tantangan Bagi Perkembangan Hukum di Indonesia” <http://teguharifyadi.blogspot.com/2008/04/cyberlaw-tantangan-bagi-perkembangan.html>, diakses pada tanggal, 21/4/2010. Baca pula untuk soal yang sama, Jamal Wiwoho, “Instrumen Internasional di Bidang Informasi dan Transaksi Elektronik”, *Bahan Kuliah*, Hukum dan Teknologi Informasi, Program Doktor FH UNS.

memberlakukan *cyberlaw* di negaranya. Dengan empat alternatif pengaturan: (1) memberlakukan KUHP konvensional dengan memperluas istilah-istilah tertentu melalui penafsiran hukum; (2) melakukan amandemen KUHP; (3) menerbitkan peraturan perundang-undangan secara khusus yang mengatur kejahatan yang berhubungan dengan komputer; dan (4) mengamandemen KUHP sekaligus menerbitkan UU khusus mengatur *cybercrime*.<sup>9</sup>

Masing-masing negara telah melakukan implementasi konvensi tersebut dengan cara harmonisasi hukum sebagai standar minum hukum. Negara-negara tersebut dalam mengadopsi dan mengharmonisasi konvensi tersebut menyesuaikan politik kriminal di masing-masing negara. Terutama dalam hal menyesuaikan dengan kultur masyarakatnya, jenis tindak kejahatan yang diatur, pemberian sanksi pidananya dan proses penegakannya. Karena itu kendati bersumber dari standar hukum minimal yang sama namun memiliki kekhasan dan keunikan masing-masing.

## II. POKOK MASALAH

Berdasar pada uraian di atas makalah ini akan mencoba mengulas dua persoalan utama, yakni:

1. Bagaimana desain kebijakan kriminalisasi yang dianut oleh UU No.11/2008, terutama dalam model pengaturannya yang dikaitkan dengan isu-isu global, soal pengaturan kriminalisasi dan pemberian sanksi ?
2. Apakah kebijakan kriminalisasi yang dianut oleh UU No.11/2008 itu telah sesuai dengan teori-teori kebijakan kriminal ?
3. Desain kebijakan kriminalisasi apa yang mesti dilakukan agar UU No.11/2008 ini dapat berlaku efektif untuk penanggulangan kejahatan berbasis internet (*cybercrimes*), bila dibandingkan dengan pengaturan yang dilakukan beberapa negara ?

## III. PEMBAHASAN

### A. Peta Kejahatan Internet di Indonesia

Pengguna internet di Indonesia, tumbuh lebih dari 1.000 persen dalam 10 tahun terakhir. Tahun 2008, total pengguna internet mencapai 25 juta. Jumlah ini memang masih terbilang kecil bila dibandingkan dengan total penduduk Indonesia yang mencapai 237,5 juta jiwa atau berkisar 10 persen saja. Di Cina, pengguna internet mencapai 253 juta atau 19 persen dari jumlah populasi.<sup>10</sup>

Positif, negatif ibarat pedang bermata ganda, perkembangan gadget di Indonesia berdampak positif di satu sisi dan negatif di sisi lain. Sebagai sumber ilmu, perkembangan gadget telah menjadi "surga" ilmu penge- tahuan dan informasi dunia maya. Menkominfo Tifarul Sembiring menyebutnya sebagai *giant library*.

---

<sup>9</sup> . Widodo, 2009, *Sistem Pemidanaan dalam Cyer Crime, Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime*, Laksbang Mediatama, Yogyakarta, hal, 89.

<sup>10</sup> . [www.internetworldstats.com](http://www.internetworldstats.com).

Namun, tak dapat dinafikan, perkembangan gadget juga menjadi "neraka" pornografi paling efektif dalam membunuh karakter bangsa. Bahkan, Tifatul mengatakan, Indonesia termasuk negara pengakses situs porno terbesar di dunia. Situs berita Antara melansir, situs-situs berbau pornografi diunduh oleh sekitar 28.258 orang per detik. Bahkan, berdasarkan hasil riset yang dilansir oleh *Top Ten Re-views*, setiap detik, situs porno menyedot lebih dari 3.075,64 dolar AS.<sup>11</sup>

Tidak hanya global, situs porno merajai semua jaringan internet. Indonesia menjadi salah satu negara yang gemar dengan situs dewasa itu. Tercatat kota-kota besar seperti Bandung, Semarang, Yogyakarta, Surabaya, dan Medan sebagai pusat konsentrasi pengguna internet yang paling getol mengunduh situs porno. Apabila pengguna internet mengetikkan kata kunci seks di mesin pencari Google, setidaknya akan muncul 662 juta situs, 568.981 video, 157 juta gambar, dan 111.057.569 blog. Meski tak semua kata seks mengarah ke pornografi, data tersebut boleh jadi mengindikasikan bahwa pornografi bukanlah industri kacang. Bahkan, total pendapatan perusahaan teknologi, seperti *Microsoft, Google, Amazon, eBay, Yahoo, dan Apple* tidak dapat menyaingi pendapatan bisnis pornografi yang mencapai 97 miliar dolar AS.<sup>12</sup>

Berita Kompas Cyber Media (19/3/2002) menulis bahwa berdasarkan survei AC Nielsen 2001 Indonesia ternyata menempati posisi ke enam terbesar di dunia atau ke empat di Asia dalam tindak kejahatan di *internet*. Meski tidak disebutkan secara rinci kejahatan macam apa saja yang terjadi di Indonesia maupun WNI yang terlibat dalam kejahatan tersebut, hal ini merupakan peringatan bagi semua pihak untuk mewaspadaikan kejahatan yang telah, sedang, dan akan muncul dari pengguna teknologi informasi.<sup>13</sup>

Kasus-kasus *cybercrime* yang banyak terjadi di Indonesia setidaknya ada tiga jenis berdasarkan modusnya, yaitu:<sup>14</sup>

#### 1. Pencurian Nomor Kartu Kredit.

Menurut Rommy Alkatiry (Wakil Kabid Informatika KADIN), penyalahgunaan kartu kredit milik orang lain di *internet* merupakan kasus *cybercrime* terbesar yang berkaitan dengan dunia bisnis *internet* di Indonesia. Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat

---

<sup>11</sup> . Eriyanti Nurmala Dewi, 2009, "Dunia Maya, Pornografi dan Anomali Hukum" dalam *Pikiran Rakyat* <http://bataviase.co.id/detailberita-10419840.html>, diakses pada tanggal, 21/04/210.

<sup>12</sup> . *Ibid.*,

<sup>13</sup> . Kompas Cyber Media, "Survei AC Nielsen", 19 Maret 2002, sebagaimana dikutip oleh Danan Mursito, dkk, 2005, "Pendekatan Hukum Untuk Keamanan Dunia Cyber Serta Urgensi Cyber Law Bagi Indonesia", *Makalah*, Program Studi Teknologi Informasi Program Magister Fakultas Ilmu Komputer Universitas Indonesia, hal 8.

<sup>14</sup> . *Ibid.*, hal, 8.

(restaurant, hotel atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di *internet*.

2. Memasuki, memodifikasi atau merusak *homepage (hacking)*

Menurut John. S. Tumiwa pada umumnya tindakan *hacker* Indonesia belum separah

aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank.

3. Penyerangan situs atau *e-mail* melalui virus atau *spamming*.

Modus yang paling sering terjadi adalah mengirim virus melalui *e-mail*. Menurut RM. Roy Suryo, di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

## **B. Membedah UU No.11/2008 tentang ITE**

Undang-Undang Nomor.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) terdiri dari XIII Bab dan 54 Pasal bila dirinci terdiri dari: Ketentuan Umum (Pasal 1-2), Asas dan Tujuan (Pasal 3-4), Informasi, Dokumentasi dan Tanda Tangan Elektronik (Pasal 5-12), Penyelenggaraan Sertifikasi Elektronik dan Sistem Informasi (Pasal 13-16), Transaksi Elektronik (Pasal 17-22), Nama Domain, Hak Kekayaan Intelektual, dan Perlindungan Hak Pribadi (Pasal 23-26), Perbuatan Yang Dilarang (Pasal 27-37), Penyelesaian Sengketa (Pasal 38-39), Peran Pemerintah dan Peran Masyarakat (Pasal 40-41), Penyidikan (Pasal 42-44), Ketentuan Pidana (Pasal 45-52), Ketentuan Peralihan (Pasal 53), dan Penutup (Pasal 54).

Jika dibedah maka dalam UU ITE ini terdapat sejumlah kaidah-kaidah yang merupakan pembagian dalam rumpun hukum, yakni kaidah hukum pidana yaitu pada Pasal 45 sampai dengan Pasal 52. Kaidah hukum administrasi tercermin dari Pasal 10, kaidah hukum Perdata tersedia melalui Pasal 23 ayat (2), Pasal 26 ayat (2), Pasal 18 ayat (1) Pasal 19 Pasal 20, dan kaidah hukum internasional tercermin dari munculnya Pasal 18 ayat (2) dan (3).

Adapun maksud dan tujuan yang terkandung dari kelahiran UU ITE ini adalah sebagaimana tercermin dalam ketentuan Pasal 4, yaitu:

1. Mencerdaskan kehidupan bangsa sebagai bagian dari masyarakat informasi dunia;
2. Mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan masyarakat;
3. Meningkatkan efektivitas dan efisiensi pelayanan publik;
4. Membuka kesempatan seluas-luasnya kepada setiap Orang untuk memajukan pemikiran dan kemampuan di bidang penggunaan dan pemanfaatan Teknologi Informasi seoptimal mungkin dan bertanggung jawab; dan
5. Memberikan rasa aman, keadilan, dan kepastian hukum bagi pengguna dan penyelenggara Teknologi Informasi.

Adapun kualifikasi kejahatan yang diatur dalam UU ITE ini sebagaimana dijelaskan pada ketentuan Bab VII (pasal 27-37): Pasal 27 (Asusila, Perjudian, Penghinaan, Pemerasan). Pasal 28 (Berita Bohong dan Menyesatkan, Berita Kebencian dan Permusuhan). Pasal 29 (Ancaman Kekerasan dan Menakutkan). Pasal 30 (Akses Komputer Pihak Lain Tanpa Izin, Cracking). Pasal 31 (Penyadapan, Perubahan, Penghilangan Informasi). Pasal 32 (Pemindahan, Perusakan dan Membuka Informasi Rahasia). Pasal 33 (Virus, Membuat Sistem Tidak Bekerja (DOS)). Pasal 35 (Menjadikan Seolah Dokumen Otentik (phising)).

#### IV. ANALISIS DISAIN KEBIJAKAN KRIMINALISASI UU ITE

##### 1. Desain Kebijakan Kriminalisasi Cybercrime dalam UU ITE

Membaca dari pasal-pasal yang tersedia dalam UU ITE ini tampak bahwa kriminalisasi atau kualifikasi kejahatan yang dianut hampir mendekati jenis-jenis kriminalisasi yang tertuang dalam *Convention on Cybercrime 2001* yang ditandatangani di Budapest Hongaria, namun tidak termasuk unsur kriminalisasi terhadap eksploitasi kejahatan terhadap anak terutama aspek pelanggaran pornografi terhadap anak. Oleh karena itu aspek pornografi terhadap anak tidak diatur spesifik dalam satu pasal tersendiri.

Adapun kualifikasi kejahatan dunia maya (*cyber crime*), menurut *Convention on Cyber Crime 2001* di Budapest Hongaria, yaitu :

1. *Illegal access*: yaitu sengaja memasuki atau mengakses sistem komputer tanpa hak.
2. *Illegal interception*: yaitu sengaja dan tanpa hak mendengar atau menangkap secara diam diam pengiriman dan pemancaran data komputer yang tidak bersifat publik ke, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis.
3. *Data interference*: yaitu sengaja dan tanpa hak melakukan perusakan, penghapusan, perubahan atau penghapusan data komputer.
4. *System interference*: yaitu sengaja melakukan gangguan atau rintangan serius tanpa hak terhadap berfungsinya sistem komputer.
5. *Misuse of Devices*: penyalahgunaan perlengkapan komputer, termasuk program komputer, password komputer, kode masuk (*access code*)
6. *Computer related Forgery*: Pemalsuan (dengan sengaja dan tanpa hak memasukkan, mengubah, menghapus data autentik menjadi tidak autentik dengan maksud digunakan sebagai data autentik)
7. *Computer related Fraud*: Penipuan (dengan sengaja dan tanpa hak menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data computer atau dengan mengganggu berfungsinya computer/sistem computer, dengan tujuan untuk memperoleh keuntungan ekonomi bagi dirinya sendiri atau orang lain).
8. *Child Pornografi* (tayangan gambar pornografi anak).

## 2. Disain Model Pengaturan Cyberlaw yang Dianut dalam UU ITE

Berdasar studi Widodo, saat ini hampir seluruh negara-negara di dunia telah memiliki UU yang mengatur tentang *cybercrime* ini dengan berbagai macam model dan variasi. Berdasarkan pada *Convention on Cybercrime* yang ditandatangani di Budhapest (Hungaria) pada tanggal 23 November 2001. Paling tidak 70 negara telah memberlakukan *cyberlaw* di negaranya.

Dengan empat alternatif pengaturan: (1) memberlakukan KUHP konvensional dengan memperluas istilah-istilah tertentu melalui penafsiran hukum; (2) melakukan amandemen KUHP; (3) menerbitkan peraturan perundang-undangan secara khusus yang mengatur kejahatan yang berhubungan dengan komputer; dan (4) mengamandemen KUHP sekaligus menerbitkan UU khusus mengatur *cybercrime*.<sup>15</sup>

Sebelum Indonesia memiliki UU ITE ini tindak kejahatan berbasis komputer penegakan hukumnya dilakukan dengan mengunkana pasal-pasal KUHP yang relevan dengan kasus dan ditafsirkan secara ekstensif.

Namun kini dengan lahirnya UU ITE ini maka model yang dianut Indonesia dalam melakukan penegakan hukum terhadap kejahatan berbasis komputer (*cybercrime*) adalah dengan melakukan model yang ke-3 (tiga), yakni membuat peraturan khusus (*lex specialis*)<sup>16</sup> yang mengatur soal kejahatan yang berhubungan dengan komputer.

## 3. Disain Globalisasi Hukum dan UU ITE

Kriminalisasi dalam UU ITE ini terdapat kelemahan fatal yang tercermin di hampir keseluruhan Bab VII Perbuatan yang dikualifikasikan sebagai tindak kejahatan, terutama pada Pasal 27 ayat (1) masalah kesusilaan, dimana persoalan ini sangat multitafsir terutama dalam soal standar yang dipergunakan untuk mengukur standar kesulian.

Demikian pula pada Ayat (2) soal muatan perjudian juga tidak tersedia definisi secara cermat dalam UU ITE ini sehingga berakibat multiinterpretasi terhadap muatan perjudian berikut standar maksimal dan minimal muatan perjudian itu, terutama jumlah keuntungannya, modelnya dan tempatnya.

Selanjutnya Ayat (3) soal muatan penghinaan dan/atau pencemaran nama baik. ini dianggap dapat membatasi hak kebebasan berekspresi, mengeluarkan pendapat dan bisa menghambat kreativitas dalam ber-internet, terutama para blogger, pasal ini dan ayat ini dianggap membatasi hak asasi manusia (HAM). Pasa dan ayat ini adalah cermin muatan pasal karet (*haatzai artikelen*), karena bersifat lentur, subjektif, dan sangat tergantung interpretasi pengguna UU ITE ini. Dan telah

---

<sup>15</sup> . Widodo, *ibid.*, hal, 89.

<sup>16</sup> . Tentang Syarat-syarat *lexspecialis derogat legi generalis*, yakni: ketentuan-ketentuan yang didapat dalam aturan hukum umum tetap berlaku, kecuali yang diatur khusus dalam aturan khusus tersebut, ketentuan yang diatur harus sederajat, ketentuan harus dalam satu lingkungan hukum (*regime*). Baca tulisan Bagir Manan, 2004, *Hukum Positif Indonesia, Satu Kajian Teoritik*, UII Press, Jakarta, hal, 58.

menelan korban Prita Mulyasari yang menulis di *millnglist* soal keluhan RS Omni Internasional dan Kho Seng Seng yang menulis surat pembaca di media cetak yang mengadakan pengembang Duta Pertiwi Jakarta menyangkut nama seorang Caleg DPR.<sup>17</sup>

Dari sejumlah isi UU ITE ini dari aspek kriminalisasi belum memasukkan kualifikasi kejahatan *Phising*, yakni kegiatan memancing pemakai komputer di internet (*user*) agar mau memberikan informasi data diri pemakai (*username*) dan kata sandinya (*password*) pada suatu *website* yang sudah di-*deface*. *Phising* biasanya diarahkan kepada pengguna online banking. Isian data pemakai dan password yang vital yang telah dikirim akhirnya akan menjadi milik penjahat tersebut dan digunakan untuk belanja dengan kartu kredit atau uang rekening milik korbannya.<sup>18</sup>

Selain itu belum pula mengkuualifikasikan kejahatan *Spamming*, yakni pengiriman berita atau iklan lewat surat elektronik (*e-mail*) yang tak dikehendaki. Spam sering disebut juga sebagai bulk email atau junk e-mail alias “sampah”. Meski demikian, banyak yang terkena dan menjadi korbannya. Yang paling banyak adalah pengiriman *e-mail* dapat hadiah, lotere, atau orang yang mengaku punya rekening di bank di Afrika atau Timur Tengah, minta bantuan netters untuk mencairkan, dengan janji bagi hasil. Kemudian korban diminta nomor rekeningnya, dan mengirim uang/dana sebagai pemancing, tentunya dalam mata uang dolar AS, dan belakangan tak ada kabarnya lagi. Seorang rektor universitas swasta di Indonesia pernah diberitakan tertipu hingga Rp1 miliar dalam karena *spamming* seperti ini.<sup>19</sup>

Melihat kriminalisasi yang dianut dalam UU ITE ini tampaklah bahwa UU ini sesungguhnya merupakan bagian dari pola dan model transparansi dan harmonisasi hukum yang berkembang di dunia Internasional terutama ditujukan untuk menyesuaikan dengan kebutuhan dan kepentingan pergaulan global dalam hal ini adalah perkembangan hukum yang berbasis teknologi informasi sebagaimana tercermin dalam *Convnetion On Cybercrime* tahun 2001 yang diadopsi oleh hampir negara-negara di seluruh dunia.

Karena penyesuaian dengan pergaulan global pertama-tama dilakukan dengan merekayasa masyarakatnya dengan mengandalkan hukum sebagai satu-satunya pilarnya. Hukum menurut J.M Otto, W.S.R. Stoter and J.Arnschiedt sebagaimana dikutip Hari Purwadi, dianggap sangat penting sebagai cara vital untuk mempromosikan pertumbuhan ekonomi, hak asasi manusia dan demokrasi yang bergulat antara dua ide transparansi hukum dan pembangunan hukum.<sup>20</sup>

<sup>17</sup> . Tanggapan kasus Prita Mulyasari dapat dibaca melalui karya, Insan Budi Maulana, “UU ITE atau Penegak Hukum Yang Tanpa Jiwa”, *Bisnis Indonesia*, 29 September 2009 dan “Pemerintah Harus Basmi Mafia Haki”, *Bisnis Indonesia*, 3 Februari 2009.

<sup>18</sup> . <http://balianzahab.wordpress.com/cybercrime/hacker-dan-cracker/>, diakses pada tanggal, 22/4/2010.

<sup>19</sup> . *Ibid.*,

<sup>20</sup> . J.M Otto, W.S.R. Stoter and J.Arnschiedt, “Using Legislative Theory to Improve Law and Development Projects, dalam Regal Maat, 2004/4, hal 121, sebagaimana dikutip

Melihat betapa penuh multitafsir dan ambigu dalam penentuan kriminalisasi dalam UU ITE ini maka jelaslah bahwa ia bertentangan dengan prinsip-prinsip pembuatan UU yang baik sesuai rekomendasi model law yang dirancang *Organization for Economic Co-operation and Development* (OECD terutama bertentangan dengan prinsip *Precision Principle*, dimana seharusnya ketentuan hukum pidana harus tepat dan teliti menggambarkan suatu tindak pidana. Perumusan hukum pidana yang bersifat samar dan umum harus dihindari. Juga bertentangan dengan *Clearness Principle*, dimana seharusnya tindakan yang dikriminalisasikan harus digambarkan secara jelas dalam ketentuan hukum pidana. Begitu juga bertentangan dengan *Principle of Defferntiation*, dimana seharusnya jelas perbedaan yang satu dengan yang lain. Hindari perumusan yang bersifat global/terlalu luas, *multipurpose* atau *all embracing*.<sup>21</sup>

#### 4. Disain Sanksi Pidana dalam UU ITE

Dari konteks sanksi pidana UU ITE ini sangat inkonsisten dengan UU yang pernah ada yang mengatur pada soal yang sama terutama dalam KUHP, misalnya saja dalam Pasal 27 (Pencemaran nama baik), yang menjatuhkan acaman pidananya sangat tinggi dan menetapkan dengan model delik formil bukan delik aduan ini bertentangan dengan Pasal 310 KUHP yang menempatkan pencemaran nama baik bukan delik formil melainkan delik aduan. Kendati telah diajukan *judicial review* ke Mahkamah Konstitusi (MK) terhadap Pasal ini. Dua permohonan pengujian UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang diajukan ke Mahkamah Konstitusi (MK) kandas. Majelis hakim konstitusi yang dipimpin oleh Mahfud MD menyatakan Pasal 27 ayat (3) dan Pasal 45 ayat (1) UU ITE tidak bertentangan dengan UUD 1945. MK menolak permohonan Iwan Piliang, sedangkan permohonan Amrie Hakim Cs dinyatakan tidak dapat diterima.<sup>22</sup>

Demikian pula ancaman pidana pada pasal-pasal lain teramat tinggi dan tidak memiliki standar yang cukup jelas, mengapa kejahatan-kejahatan yang dikriminalisasi dalam UU ITE ini begitu. Padahal dalam teori pembedaan haruslah diperjelas pada tingkat keseriusan kejahatan dan dampak dari kejahatan ini terhadap korban. Apakah sebegitu berat dan serius (*ordinary crimes*) dan berdampak luar biasa pada korban sehingga hukuman dan tindak kriminal pada UU ITE sangat luar biasa tinggi dan ditambah denda yang kisarannya jumlahnya miliaran rupiah.

---

oleh Hari Purwadi, Reformasi Hukum Nasional: Problem dan Prospeknya, dalam Satya Arinanto dan Ninuk Triyanti (eds), *Memahami Hukum dari Konstruksi Sampai Implementasi*, (Rajawali Press, Jakarta, 2009), hal, 61-67.

<sup>21</sup> . Teguh Prasetyo, 2010, *Kriminalisasi Dalam Hukum Pidana*, Nusa Media, Bandung, hal 28.

<sup>22</sup> . <http://www.hukumonline.com/berita/baca/hol21918/dua-permohonan-pengujian-uu-ite-kandas>, diakses pada tanggal, 26 April 2010.

Jika membaca pada sanksi pidana yang dianut dalam UU ITE ini yang masih menempatkan sanksi pidana penjara jelas ini di lihat dari politik kriminal ini merupakan cermin dari pembentuk UU yang masih terpengaruh pada pemikiran aliran klasik (*classical school*) dalam hukum pidana, meskipun tidak mutlak. Buktinya, dalam penentuan jenis dan ukuran pidana sangat kaku (*rigid*), sehingga sifat tindak pidana dan pelaku tindak pidana serta kondisi masyarakat belum terakomodasi secara memadai dalam pembuatan hukum. Dimana dalam aliran klasik ini sangat membatasi kebebasan hakim untuk menetapkan pidana dan ukuran pidananya dan melarang penggunaan prinsip individualisasi.<sup>23</sup>

Padahal pidana penjara adalah model generasi pertama dalam pemberian sanksi, disusul urutan kedua pidana kurungan, dan strafmaat ancaman minimum dan maksimum, urutan ketiga pidana denda dan urutan mutakhir keempat adalah pidana kerja sosial (*community Serves Order*) sebagai reaksi terhadap keraguan atas pelaksanaan pidana denda yang diberlakukan secara meluas.<sup>24</sup>

Dilihat dari sisi jenis pidana pokok yang diancamkan hanya ada 2 (dua) yaitu pidana penjara dan pidana denda yang diancamkan secara campuran, yaitu menggabungkan antara sistem alternatif dan kumulatif. Yang dapat berakibat hakim dapat memilih salah satunya atau memilih secara bersamaan dan hakim tidak memiliki alternatif lain dalam menjatuhkan pidana, kecuali hanya menentukan lama tidaknya dan jumlah dendanya.

UU ITE ini tidak mengenal pidana minimum dan ini bertentangan dengan kebijakan kriminalisasi pada UU yang bersifat khusus (*lex specialis*) di Indonesia yang biasanya menggunakan model pidana minimal tidak maksimal. Lihatlah misalnya pada UU Pemilu, UU Korupsi, UU Narkoba, Hak Cipta, Fiducia dan Perlindungan Anak.

## **5. Disain UU ITE dan Perbandingan antar Negara**

UU ITE ini belum mengikuti kecenderungan positif global dalam konteks kebijakan kriminal terutama kebijakan pemberian sanksi pidana tidak lagi berorientasi pidana penjara melainkan telah berubah menjadi pidana kerja sosial, pengawasan dan pencabutan hak-hak tertentu. Sebagaimana dimintakan PBB agar setiap negara perlu mencari pidana alternatif pengganti pidana penjara dengan pidana yang lebih bermanfaat sesuai dengan kondisi suatu negara dan lebih banyak melibatkan masyarakat luas dalam rangka rehabilitasi korban. Paling ada tiga, (1) kontrak/perjanjian untuk pembinaan (*contract treatment*); (2) pencabutan dan pembatasan-pembatasan terhadap hak-hak tertentu (*deprivation and interdicts concerning rights or licencies*) dan (3) pidana kerja sosial (*community service*).<sup>25</sup>

Seperti tercermin dari dari penelitian Widodo, dalam yang melakukan studi

---

<sup>23</sup> . Widodo, *Ibid*, hal 228

<sup>24</sup> . *Ibid*,. hal 152-153

<sup>25</sup> . Widodo, *Ibid*,. hal 149-150

perbandingan pada politik kriminalisasi dalam regulasi *cybercrime* di 70 negara di dunia telah ada kecenderungan pergeseran dari pidana penjara ke bentuk lain. Misalnya, Azerbaijan, Beylorusia, Georgia, Hungaria, Kazakstan, Latvia, Peru dan Rusia yang menempatkan pidana kerja sosial dan denda sebagai cara memberikan sanksi pada tindak kejahatan *cybercrimes*.<sup>26</sup>

Bila dipetakan secara sistematis maka dapat digambarkan sebagai berikut:

**Tabel Perbandingan Bentuk Kejahatan yang Diancam Pidana Kerja Sosial, Urutan Ancaman, Istilah, dan Lama Pidana kerja Sosial di 8 Negara Asing.**<sup>27</sup>

NO	Negara	Bentuk Kejahatan Yang diancam Pidana Kerja Sosial	Urutan jenis Ancaman Pidana	Istilah	Lama Pidana Kerja Sosial
1	Azerbaijan	Akses, modifikasi, mengkopi, merusak, menghapus, data dalam sistem atau jaringan komputer	a. Pencabutan hak-hak tertentu atau b. Kerja Sosial	<i>Social work</i>	2 tahun
2	Beylorusia	Kopi, intersepsi, akses tidak sah	a. Kerja Sosial atau b. Denda, atau c. Penjara	<i>Social work</i>	Tidak ditentukan
3	Georgia	Akses, modifikasi, mengkopi, merusak, menghapus, data dalam sistem atau jaringan komputer	a. Denda, atau b. Kerja sosial	<i>Socially useful work</i>	180 sampai 200 jam paling lama dilaksanakan dalam jangka waktu 2 sampai 3 tahun
4	Hungaria	Memasukkan data, merusak pengaman, mengetahui rahasia pribadi orang lain secara tidak sah	a. Penjara b. Kerja Sosial c. Denda	<i>Work in community service</i>	Tidak ditentukan
5	Kazakstan	Akses,	a. Denda, atau	<i>Socially</i>	120 sampai

<sup>26</sup> . Widodo, *Ibid.*, hal, 162-165.

<sup>27</sup> . Bagan dikutip dari Widodo, *Ibid.*, hal, 162-164.

		modifikasi, mengkopi, merusak, menghapus, data dalam sistem atau jaringan komputer	b. Kerja sosial	<i>useful work</i>	180 jam, paling lama dilaksanakan dalam jangka waktu 1 tahun
--	--	--	-----------------	--------------------	--

6	Latvia	Mengganggu proses dan sistem penyimpanan data, mencuri data, merusak data secara tidak sah, dan tindakan lain yang membahayakan	a. Penjara b. Kerja sosial c. Denda	<i>Com-Munity service</i>	Tidak ditentukan
7	Peru	a. Akses, memodifikasi, kopi tidak sah, dengan korban individu	a. Penjara, atau b. Kerja Sosial	<i>Com-Munity service</i>	52 sampai 104 hari
		b. Akses, memodifikasi, kopi tidak sah, dengan korban korporasi	a. Penjara, atau b. Kerja Sosial	<i>Com-Munity service</i>	100 hari
8	Rusia	Melakukan akses tidak sah, menghalangi akses, menghapus, mengubah dan merusak sistem atau jaringan komputer	a. Perampasan hak-hak tertentu atau b. Wajib lapor	<i>Obligatory work</i>	180 sampai 200 jam, paling lama dilaksanakan dalam jangka 2 tahun

Ada dua kepentingan sebenarnya jika saja para pembuat UU ITE ini menempatkan pidana *cybercrimes* ini dalam bentuk alternatif lain, misalnya pidana kerja sosial dan pengawasan.

*Pertama*, para pelaku kejahatan *cybercrimes* dimanapun didunia biasanya masih berusia muda, dari kalangan terdidik, penuh kreatifitas, dan cerdas maka alangkah ruginya jika model orang-orang cerdas ini harus dipidana penjara. Akan lebih tepat jika mereka diberi sanksi kerja sosial di lembaga-lembaga yang berbasis komputer terutama instansi-instansi publik, disamping tenaga dan kecerdasannya dapat dimanfaatkan negara juga pengawasannya dapat dilakukan secara simultan oleh lembaga yang ditunjuk.

*Kedua*, dengan pidana kerja sosial untuk pelaku *cybercrimes* akan dapat mengurai problem pemerajaraan atau model pemasyarakatan kita yang sampai hari tidak cukup baik. Namun kita belakangan ini dipaksa untuk melihat realitas paradoks di LP dan nasib para narapidana yang tak manusiawi. Lihatlah, belakangan ini tersiar tingginya angka kematian di LP (813 orang) yang disebabkan oleh aneka macam penyakit yang tak tertolong, uniknya akibat terkena virus HIV/AIDS menduduki rangking tertinggi kematian.<sup>28</sup> Jual-beli dan penggunaan *putaw* dan narkoba marak di LP, adanya realitas napi kelas borjuis (kaya) dan proletar (miskin). Maraknya suasana bentrok antar napi, perkelahian dan melarikan diri.

Fenomena itu juga mengilustrasikan LP telah menjadi lembaga pembinaan bukan pembinaan. Kalau ini terus dibiarkan dipastikan LP tak akan mampu menjalankan tugas pokok, visi dan misinya malah mungkin menjadi lembaga pelanggaran Hak Asasi Manusia (HAM), karena melakukan pembiaran (*by omission*) terhadap perlakuan yang tak manusiawi terhadap narapidana.<sup>29</sup>

Kondisi fasilitas LP yang manusiawi ini mengakibatkan pada terbaikannya tugas pembinaan terhadap napi oleh petugas LP (Lapas), karena jumlah napi yang terus membengkak, sementara jumlah Lapas tak sebanding dengan jumlah napi. Data di Dirjen Pemasyarakatan Dep.Hukum dan HAM (2007) memperlihatkan jumlah napi dan tahanan terus menumpuk dari tahun ke tahun, tahun 2003 tercatat sejumlah 71.587, tahun 2004 tercatat 86.450, tahun 2005 terdeteksi 97.671 dan terus meningkat di tahun 2006 menjadi 116.688 orang.<sup>30</sup>

Jika dibandingkan<sup>31</sup> dengan negara-negara tersebut jelaslah bahwa UU ITE sebenarnya sudah saatnya melakukan pergeseran pemberian sanksi pidana dan sistem pemidanaan. Dengan menerapkan sanksi kerja sosial selain denda dan tidak lagi menempatkan pidana penjara. Kendati pidana penjara tetap merupakan bagian yang tetap paling favorit di banyak negara terutama negara-negara modern. Namun dalam konteks politik kriminal di negara berkembang sebagaimana tercermin dari studi Widodo di atas dalam *cybercrimes* telah membuat lompatan besar untuk tidak selalu terikat dengan kecenderungan politik kriminal global yang menempatkan pidana penjara sebagai hal yang utama.

Indonesia sebenarnya dalam politik kriminalnya dapat mengadopsi model negara-negara berkembang tersebut terutama dalam konteks pemberian saksi pidana dalam *cybercrimes*. Ini penting dilakukan terutama ditujukan agar memberikan kesempatan bagi perkembangan teknologi informasi dan kebebasan berekspresi masyarakat Indonesia. Sebab bila ancaman sanksi pidananya tinggi

<sup>28</sup> . Kompas, 5-7 April 2007.

<sup>29</sup> . Agus Riewanto, "Reformasi Pemasyarakatan dan Narapidana", Kolom Wacana, *Suara Merdeka*, 6 Februari 2010.

<sup>30</sup> . <http://www.depkuham.go.id>.

<sup>31</sup> . Tentang studi perbandingan hukum pidana dapat dibaca karya Barda Nawawi Arief, 2002, *Perbandingan Hukum Pidana*, Rajawali Press, Jakarta.

dengan pidana penjara sekaligus. Hal ini dikhawatirkan akan dapat menghambat kreatifitas masyarakat dalam pemanfaatan teknologi informasi berbasis internet yang saat ini mulai berkembang. Bukankah saat ini disparitas antara mereka yang melek teknologi dan tidak sangat berjarak.

#### **6. Disain UU ITE dan Perlunya Harmonisasi Internal UU Serta Pranata Lembaga**

Kebijakan kriminalisasi UU ITE ini juga terkait dengan persoalan harmonisasi, yaitu harmonisasi materi/substansi dan harmonisasi eksternal (internasional/global) Mengenai harmonisasi substansi, bukan hanya KUHP yang akan terkena dampak dari dibuatnya undang-undang tentang *cybercrime*.

Kementerian Komunikasi dan Informasi RI mencatat ada 21 undang-undang, misalnya UU No.5/1999 tentang Larangan Praktek Monopoli dan Persaingan Usaha Tidak Sehat, UU No.19/2002 tentang Hak Cipta, UU 15/2001 tentang Merek, UU No.36/1999 tentang Telekomunikasi yang akan terkena dampak dari UU ITE ini . Ini merupakan pekerjaan besar di tengah kondisi bangsa yang belum stabil secara politik maupun ekonomi. Harmonisasi eksternal berupa penyesuaian perumusan pasal-pasal *cybercrime* dengan ketentuan serupa dari negara lain, terutama dengan *Draft Convention on Cyber Crime* dan pengaturan *cybercrime* dari negara lain. Persoalan *cybercrime* ini diperlukan standardisasi dan harmonisasi dalam tiga area, yaitu *legislation*, *criminal enforcement* dan *judicial review* Ini menunjukkan bahwa persoalan harmonisasi merupakan persoalan yang tidak berhenti dengan diundangkannya undang-undang yang mengatur *cybercrime*, lebih dari itu adalah kerjasama dan harmonisasi dalam penegakan hukum dan peradilannya.<sup>32</sup>

Selain secara substansi efektifitas pemberlakuan UU ini juga masih memerlukan sejumlah Peraturan Pemerintah dan peraturan setingkat menteri, paling tidak 9 (sembilan) dan 2 (dua) lembaga yang baru. Lembaga sertifikasi keandalan, Penyelenggaraan sertifikasi elektronik, Tanda Tangan Elektronik, Penyelenggaraan sistem elektronik, Penyelenggaraan transaksi elektronik, Penyelenggara agen elektronik, Pengelolaan nama domain dan Tatacara intersepsi.<sup>33</sup>

#### **V. PENUTUP DAN KESIMPULAN**

Desain kebijakan kriminalisasi yang dianut oleh UU No.11/2008, terutama dalam model pengaturannya yang dikaitkan dengan isu-isu global, soal pengaturan

---

<sup>32</sup>. Agus Raharjo, "Kebijakan Kriminalisasi dan Penanganan Cybercrime di Indonesia", *Makalah* disampaikan pada Bedah Buku "Tindak Pidana Mayantara, Perkembangan Cybercrime Di Indonesia" (karya Barda Nawawi Arief, 2006, Jakarta: Rajawali Press), diselenggarakan dalam rangka Bulan Kunjung Perpustakaan oleh Perpustakaan FH Undip Semarang, 12 September 2006. Baca Pula tulisan Budi Agus Riswandi, 2003, *Hukum dan Internet di Indonesia*, UII Press, Yogyakarta. Gagasan yang hampir serupa baca pula karya Tan Kamello, "Aspek Perlindungan Hukum Dalam Transaksi Melalui Media Internet", *Jurnal Equality*, Vol. 10 No.1 Februari 2005.

<sup>33</sup>. Tentang Matrik Keterkaitan hukum nasional bagi dunia *Cyber* dengan instrumen hukum nasional dapat dibaca tulisan. Ahmad M.Ramli, 2006, *Cyberlaw dan Haki dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung. Terutama pada Bab kedua.

kriminalisasi dan pemberian sanksi. Ternyata pengaturan kriminalisasi menganut model harmonisasi dengan kriminalisasi yang diatur dalam *Convention on Cybercrimes*, namun tidak mengatur secara tegas soal pornografi dan eksploitasi anak. Kemudian modelnya adalah dengan membuat aturan *lex specialis*. Disamping itu UU ITE ini tidak mengatur soal kejahatan *Phising* dan *Spamming*. Adapun pemberian sanksi pidanya masih menganut model klasik (*classic school*), dicerminkan dengan masih menjatuhkan sanksi pidana penjara dan denda dan tidak menyediakan alternatif sanksi lain.

Kebijakan kriminalisasi yang dianut oleh UU No.11/2008 itu tidak sesuai dengan teori-teori kebijakan kriminal yang cermin dari pengaturan kejahatan (kriminalisasinya) melalui Bab VII masih multitafsir, ambigu, kurang cermat cermat dan kurang teliti karena itu ia tidak sesuai dengan asas *model law* yang dianut dalam *Organization for Economic Co-operation and Development* (OECD). UU ini selain bertentangan dengan KUHP juga bertentangan dengan aspek HAM dan dalam pemberian sanksinya berbeda dari kelaziman dalam pengaturan kejahatan yang bersifat khusus (*lex specialis*), seperti UU Pemilu, UU Perlindungan Anak, UU Korupsi, UU Narkoba, dan lain-lain, karena itu belum lama berselang UU ini telah menelan korban Prita dan Sheng.

Desain kebijakan kriminal dalam UU No.11/2008 ini kemungkinan tidak dapat berlaku secara efektif, terutama bila dibandingkan dengan pengaturan *Cybercrimes* yang dilakukan beberapa negara, yakni Azerbaijan, Belyorusia, Georgia, Hungaria, Kazakstan, Latvia, Peru dan Rusia yang menempatkan, pidana kerja sosial, denda dan pencabutan hak-hak tertentu sebagai cara memberikan sanksi pada tindak kejahatan *cybercrimes*. Ke depan politik kriminal Indonesia perlu mengadopsi pada model di negara-negara tersebut.

## DAFTAR PUSTAKA

- Abdul Halim Barkatullah, 2009, *Perlindungan Hukum Bagi Konsumen Dalam Transaksi e-commerce Lintas Negara Indonesia*, FH UII Press, Yogyakarta.
- Andi Hamzah. 1989, *Hukum Pidana Yang Berkaitan dengan Komputer*, Sinar Grafika, Jakarta.
- Agus Raharjo, 2006, "Kebijakan Kriminalisasi dan Penanganan Cybercrime di Indonesia", *Makalah* disampaikan pada Bedah Buku "Tindak Pidana Mayantara, Perkembangan Cybercrime Di Indonesia" (karya Barda Nawawi Arief, 2006, Jakarta: Rajawali Press), diselenggarakan dalam rangka Bulan Kunjung Perpustakaan oleh Perpustakaan FH Undip Semarang, 12 September 2006.
- Agus Riewanto.2010, "Reformasi Pemasarakatan dan Narapidana", Kolom Wacana, *Suara Merdeka*, 6 Februari 2010.
- Ahmad M.Ramli, 2006, *Cyberlaw dan Haki dalam Sistem Hukum Indonesia*, Refika Aditama, Bandung. Terutama pada Bab kedua.

Arifyadi, "Cyberlaw: Tantangan Bagi Perkembangan Hukum di Indonesia"

<http://tequharifyadi.blogspot.com/2008/04/cyberlaw-tantangan-bagi-perkembangan.html>, diakses pada tanggal, 21/4/2010.

Budi Raharjo. 2006, "Cyberlaw: Teritori dalam Cyberspace, Realitas dan Virtualitas, *Makalah*, Dipresentasikan pada Seminar "IT Within" yang diselenggarakan oleh Himpunan Mahasiswa Informatika ITB, 18 Februari 2006.

Budi Agus Riswandi, 2003, *Hukum dan Internet di Indonesia*, UII Press, Yogyakarta.

Barda Nawawi Arief, 2010, *Kebijakan Legislatif dalam Penanggulangan Kejahatan Dengan Pidana Penjara*, Genta Publisng.

-----, 2002, *Perbandingan Hukum Pidana*, Rajawali Press, Jakarta.

Bagir Manan, 2004, *Hukum Positif Indonesia, Satu Kajian Teoritik*, UII Press, Jakarta.

Cahyana Ahmad Jayadi, "Perlunya Cyberlaw dalam Rangka Menghadapi dan Menanggulangi Kejahatan Dunia Maya", *Makalah* di sampaikan dalam seminar RUU ITE, pada 12 April 2007.

David Held, 1995, *Democracy and The Global Order, From The Modern State to Cosmopolitan Governance*, Polititing Press, USA.

Didik M. Arief Mansur, 2009, *Cyber Law, Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung.

Danan Mursito, dkk, 2005, "Pendekatan Hukum Untuk Keamanan Dunia Cyber Serta Urgensi Cyber Law Bagi Indonesia", *Makalah*, Program Studi Teknologi Informasi Program Magister Fakultas Ilmu Komputer Universitas Indonesia.

Emiliana Krisnawati, "Problematika Cyberlaw bagi Perkembangan Hukum Indonesia", dalam Satya Arinanto (Editor), Satya Arinanto dan Ninuk Triyanti (eds), *Memahami Hukum dari Konstruksi Sampai Implementasi*, (Rajawali Press, Jakarta, 2009).

Eriyanti Nurmala Dewi, 2009, "Dunia Maya, Pornografi dan Anomali Hukum" dalam *Pikiran Rakyat* <http://bataviase.co.id/detailberita-10419840.html>, diakses pada tanggal, 21/04/210.

<http://balianzahab.wordpress.com/cybercrime/hacker-dan-cracker/>, diakses pada tanggal, 22/2/2016.

<http://www.hukumonline.com/berita/baca/hol21918/dua-permohonan-penqujian-uu-ite-kandas>, diakses pada tanggal, 26/2/2016.

<http://www.depkuham.go.id>.

Insan Budi Maulana, 2009. "UU ITE atau Penegak Hukum Yang Tanpa Jiwa", *Bisnis Indonesia*, 29 September 2009.

- , 2009. "Pemerintah Harus Basmi Mafia Haki", *Bisnis Indonesia*, 3 Februari 2009.
- Jamal Wiwoho, 2010, "Instrumen Internasional di Bidang Informasi dan Transaksi Elektronik", *Bahan Kuliah*, Hukum dan Teknologi Informasi, Program Doktor FH UNS.
- J.M Otto, W.S.R. Stoter and J.Arnschiedt, "using Legislative Theory to Improve Law and Development Projects, dalam Regal Maat, 2004/4, hal 121, sebagaimana dikutip oleh Hari Purwadi, Reformasi Hukum Nasional: Problem dan Prospeknya, dalam Satya Arinanto dan Ninuk Triyanti (eds), *Memahami Hukum dari Konstruksi Sampai Implementasi*, (Rajawali Press, Jakarta, 2009.
- Kompas, 5-7 April 2007.
- Kompas, 21 April 2007.
- Muladi dan Barda Nawawi Arief, 1998, *Teori-Teori dan Kebijakan Pidana*, PT Alumni, Bandung.
- Republik Indonesia, *Undang-Undang Tentang Informasi dan Transaksi Elektronik*, UU Nomor 11 Tahun 2008 Lembaran Negara RI Nomor 58 Tahun 2008, TLN Nomor 4843.
- Sudarto, 19981, *Kapitaselektta Hukum Pidana*, Alumni, Bandung,
- , *Hukum dan Hukum Pidana*, Alumni, Bandung.
- Shinta Dewi, 2009, *Cyberlaw Atas Informasi Pribadi dalam e-commerce Menurut Hukum Internasional*, Widya Pajajaran Press, Bandung.
- Tan Kamello, "Aspek Perlindungan Hukum Dalam Transaksi Melalui Media Internet", *Jurnal Equality*, Vol. 10 No.1 Februari 2005.
- Teguh Prasetyo, 2010, *Kriminalisasi Dalam Hukum Pidana*, Nusa Media, Bandung.
- , 2009, "Kebijakan Kriminalisasi dalam Peraturan Daerah dan Singkronisasi Dengan Hukum Pidana Kodifikasi", dalam Sri Hastuti Puspitasari (editor), *Bunga Rampai Pemikiran Hukum Indonesia*, UII Press, Yogyakarta.
- Widodo, 2009, *Sistem Pemidanaan dalam Cyer Crime, Alternatif Ancaman Pidana Kerja Sosial dan Pidana Pengawasan Bagi Pelaku Cyber Crime*, Laksbang Mediatama, Yogyakarta.
- [www.internetworldstats.com](http://www.internetworldstats.com).
- ([www.usdoj.gov/criminal/cybercrimes](http://www.usdoj.gov/criminal/cybercrimes)), diakses pada tanggal 26/4/2010.
- Yenti Garnasih, 2003 "Kriminalisasi Pencucian Uang, (*Money Laundering*), *Disertasi*, Program Doktor Ilmu Hukum UI, Jakarta.