

**PENEGAKAN HUKUM TERHADAP
UNDANG-UNDANG NO. 11 TAHUN 2008
TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK***

Puteri Hikmawati**

Abstract

Technology information can bring at the same time advantages and disadvantages for humankind. From negative perspective, technology information can be misused for organizing cyber crimes. In Indonesia, the number of cyber crimes cases is one of the highest in the world. To combat such sort of crimes, the country has passed Law No. 11/2008 on electronic information and transaction two years ago. In addition to this, the government and DPR have prioritized a new bill on cyber crime for their national legislation projects for 2009 and 2010, which if agreed, it would immediately replace the Law No. 11/2008. This essay analyzed how the practices of using and misusing technology information in Indonesian society and problems in law enforcement.

Kata Kunci : Cyber Crime, UU ITE, teknologi informasi

I. Pendahuluan

A. Latar Belakang

Arus bebas informasi sebagai konsekuensi dari globalisasi menempatkan Indonesia sebagai bagian dari masyarakat informasi dunia. Peran komputer dan internet menjadi sangat strategis karena menghadirkan suatu dunia tanpa batas jarak, ruang, dan waktu. Selain itu, perkembangan teknologi telah menimbulkan dampak pada perkembangan sosial, budaya, dan ekonomi. Ada kemajuan yang signifikan dalam perkembangan dan penerapan teknologi informasi dan alat-alat telekomunikasi, seperti komputer dan internet.

*Tulisan ini merupakan hasil penelitian yang dilakukan di Provinsi Bali pada tanggal 30 November sampai dengan 6 Desember 2009.

** Peneliti Madya bidang Hukum Pidana pada Pusat Pengkajian Pengolahan Data dan Informasi (P3DI) Setjen DPR RI, email: puterihw@yahoo.com.

Penggunaan komputer diharapkan dapat meningkatkan produktivitas dan efisiensi yang pada akhirnya dapat meningkatkan kesejahteraan. Namun, kemajuan teknologi juga menciptakan kemungkinan baru dalam melakukan tindak pidana. Komputer juga menjadi sarana efektif perbuatan melawan hukum. Penggunaan komputer dapat memberikan peluang kepada seseorang untuk melakukan kejahatan-kejahatan baru dalam bentuk kejahatan dunia maya (*cyber crime*) yang lebih canggih. *Cyber crime* adalah kejahatan dimana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber* atau dunia maya yaitu dengan melalui internet.¹ Hal ini tentunya akan berdampak negatif pada produktivitas dan efisiensi yang semula diharapkan.

Kegiatan dunia maya adalah kegiatan virtual. Meskipun bersifat virtual tetapi kegiatan dunia maya dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Dengan demikian subyek pelakunya harus dikualifikasikan pula sebagai telah melakukan perbuatan hukum secara nyata, dengan alat bukti elektronik.² Sehingga, secara yuridis, dalam dunia maya sudah tidak pada tempatnya untuk mengkategorikan sesuatu dengan ukuran dan kualifikasi konvensional untuk dapat dijadikan obyek dan perbuatan, sebab jika cara ini yang tetap ditempuh akan terlalu banyak tindak kejahatan dengan menggunakan teknologi informasi yang bisa lolos dari jerat hukum.

Data dari Asosiasi Penyedia Jasa Internet tahun 2008 menunjukkan bahwa pengguna internet di Indonesia hanya 14,5 juta orang dari total penduduk yang mencapai 220 juta. Meskipun tidak mencapai 10 persennya, Indonesia pernah menduduki peringkat pertama dalam kejahatan dunia maya. Tahun 2007 posisi Indonesia sempat turun di posisi empat setelah Ukraina dan beberapa negara Eropa Timur yang membukukan angka kejahatan dunia maya lebih banyak.³ Posisi Indonesia nomor satu di dunia dalam kasus *cyber crime* juga dikatakan oleh Brigjen Anton Tabah, staf ahli Kepala Kepolisian Republik Indonesia dalam acara peluncuran buku Panduan Bantuan Hukum Indonesia (PBHI) di Jakarta, 25 Maret 2009. Anton mengatakan, jumlah kasus *cyber crime* atau kejahatan di dunia maya yang terjadi di Indonesia merupakan yang tertinggi

¹ "Cyber Crime/Kejahatan Dunia Maya", <http://riya93.blogspot.com/2009/03/blog-spot----26.html>, diakses tanggal 20 Oktober 2009.

² *Menuju Kepastian Hukum di Bidang: Informasi dan Transaksi Elektronik*, Departemen Komunikasi dan Informatika, Tahun 2005, hal. 2.

³ "Cyber Crime/Kejahatan Dunia Maya", <http://riya93.blogspot.com/2009/03/blog-spot----26.html>, *op.cit.*

di dunia. Tingginya kasus *cyber crime* dapat dilihat dari banyaknya kasus pemalsuan kartu kredit dan pembobolan sejumlah bank.⁴

Kejahatan dunia maya telah mengalahkan penjualan obat-obatan terlarang sebagai penghasil uang kejahatan. Setiap 3 detik satu identitas tercuri. Kejahatan dunia maya saat ini lebih menghancurkan kehidupan daripada menghancurkan komputer.⁵ Adapun jenis-jenis kejahatan dalam dunia maya (*cyber crime*), di antaranya adalah pelanggaran isi *situs web* (pornografi dan pelanggaran hak cipta), kejahatan dalam perdagangan elektronik (penipuan *online* dan kartu kredit), dan kejahatan lainnya, seperti *hacker*, *piracy* (pembajakan), dan *fraud* (penipuan).

Bagi Indonesia, regulasi mengenai hukum dunia maya menjadi bagian penting dalam sistem hukum positif secara keseluruhan. Hukum pidana nasional (Kitab Undang-undang Hukum Pidana/KUHP) belum bisa menjangkau atau memidana para pelaku kejahatan dunia maya dengan tepat. Oleh karena itu, DPR RI dan Pemerintah membentuk sistem hukum mengenai *cyber law*, yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE merupakan aturan hukum yang mengarahkan pada kegiatan pemanfaatan teknologi informasi dan transaksi elektronik kepada pemanfaatan yang baik, bertanggung jawab dan mempunyai nilai positif bagi masyarakat pada umumnya.

UU ITE antara lain mengatur mengenai informasi, dokumen, dan tanda tangan elektronik; penyelenggaraan sertifikasi elektronik dan sistem elektronik; transaksi elektronik; perbuatan yang dilarang; penyelesaian sengketa; penyidikan; dan ketentuan pidana. UU juga mengatur peran Pemerintah dan masyarakat. Dengan dibentuknya UU ITE, segala aktivitas dalam dunia maya dan kaitannya dengan penggunaan teknologi informasi dalam transaksi bisnis memiliki rujukan. UU tersebut sekaligus mengisi kekosongan hukum terhadap pemberlakuan dokumen elektronik sebagai alat bukti hukum yang berlaku di pengadilan.

Pemberlakuan UU ITE sempat menimbulkan kontroversi, yaitu dalam penanganan kasus Prita. Prita yang menyatakan ketidakpuasannya terhadap pelayanan Rumah Sakit Omni Internasional Alam Sutera Tangerang melalui *email* kepada kalangan terbatas, dianggap telah mencemarkan nama Rumah Sakit tersebut. Kemudian, dia diajukan ke pengadilan dengan dakwaan Pasal 45 ayat

⁴ "Cyber Crime", Indonesia Tertinggi di Dunia", <http://nasional.kompas.com/read/xml/2009/03/25/18505497/Cyber.....>, diakses tanggal 10 Agustus 2009.

⁵ "Kejahatan Virtual Kian Mengganas", *Media Indonesia*, 12 Oktober 2009.

(1) *juncto* Pasal 27 ayat (3) UU ITE.⁶ Kontroversi timbul karena beberapa kalangan termasuk Menteri Hukum dan HAM, Patrialis Akbar, menyatakan UU tersebut telah membatasi hak orang untuk menyampaikan pendapat.⁷ Sementara Jaksa Penuntut Umum yang menangani kasus Prita mendakwakan Prita dengan Pasal 45 ayat (1) *juncto* Pasal 27 ayat (3) UU ITE karena Prita dianggap telah mencemarkan nama Rumah Sakit Omni Internasional dengan menyatakan rasa ketidakpuasannya terhadap pelayanan Rumah Sakit tersebut melalui *email* dan disebarakan melalui *mailing list*. Berita kecewa itu akhirnya menyebar dari satu *email* ke *email* lainnya.⁸

B. Permasalahan dan Pertanyaan Penelitian

Indonesia telah memiliki UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik untuk menangani *cyber crime*. Pemberlakuan UU tersebut belum berjalan dua tahun, namun dalam daftar Program Legislasi Nasional (Prolegnas) terdapat RUU tentang *Cyber Crime* sebagai prioritas tahun 2009, kemudian RUU tentang Tindak Pidana Teknologi Informasi dan RUU tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagai prioritas tahun 2010. Oleh karena itu, permasalahan yang akan dikaji adalah bagaimana penegakan hukum terhadap UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?

Adapun yang menjadi pertanyaan penelitian adalah:

1. Bagaimana pemanfaatan teknologi informasi dan penyalahgunaannya oleh masyarakat?
2. Bagaimana norma hukum yang diatur dalam UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik?
3. Apa saja kendala yang dihadapi dalam penegakan hukum terhadap UU No. 11 Tahun 2008?

⁶ "Kasus Prita Mulyasari vs RS Omni dan Internet Marketing", <http://www.baliorange.web.id/kasus-prita-mulyasari-vs-rs-omni-dan-internet-marketing>, diakses tanggal 1 Maret 2010.

⁷ "Jangan Atur Semua Informasi Internet, *Cyber Crime* Saja", <http://id.news.yahoo.com/dtik/20091222/tpl-jangan-atur-semua-info..>, diakses tanggal 23 Desember 2009.

⁸ "Kasus Prita Mulyasari vs RS Omni dan Internet Marketing", <http://www.baliorange.web.id/kasus-prita-mulyasari-vs-rs-omni-dan-internet-marketing/>, *op.cit.*

C. Tujuan dan Kegunaan Penelitian

Penelitian ini ditujukan untuk mengkaji bagaimana penegakan hukum terhadap UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Hasil penelitian ini diharapkan dapat bermanfaat baik secara teoritis maupun praktis. Secara teoritis hasil penelitian diharapkan dapat memperkuat kasanah ilmu pengetahuan hukum dalam bidang hukum pidana. Sedangkan secara praktis, hasil penelitian ini diharapkan dapat digunakan sebagai bahan masukan bagi Anggota DPR RI dalam menjalankan fungsi legislasi, yaitu dalam membahas RUU yang berkaitan dengan *cyber crime* dan RUU tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, yang masuk dalam daftar Program Legislasi Nasional Prioritas Tahun 2010.

D. Kerangka Pemikiran

Pelaksanaan hukum dalam kehidupan masyarakat sehari-hari mempunyai arti yang sangat penting, karena apa yang menjadi tujuan hukum justru terletak pada pelaksanaan hukum itu. Terdapat pendapat yang berbeda-beda dalam merumuskan apa yang menjadi tujuan hukum. Menurut teori etis (*etische theorie*), hukum hanya semata-mata bertujuan mewujudkan keadilan. Menurut teori utilities (*utilities theorie*), hukum bertujuan semata-mata apa yang berfaedah saja. Hukum bertujuan menjamin adanya kebahagiaan sebanyak-banyaknya pada orang sebanyak-banyaknya. Teori selanjutnya yang merupakan campuran dari kedua teori tersebut, menegaskan bahwa isi hukum harus ditentukan menurut dua asas, yaitu keadilan dan faedah.⁹

Hukum mengatur masyarakat dan bermanfaat dengan menetapkan apa yang diharuskan atau dibolehkan dan sebaliknya. Dengan demikian, dapat ditarik garis antara apa yang dimaksud hukum dan apa yang dimaksud melawan hukum. Hukum dapat mengkualifikasi sesuatu perbuatan sesuai dengan hukum atau mendiskualifikasinya sebagai melawan hukum. Perbuatan yang sesuai dengan hukum tidak merupakan masalah dan tidak perlu dipersoalkan; yang menjadi masalah adalah perbuatan yang melawan hukum. Perhatian dan penggarapan perbuatan itulah yang merupakan penegakan hukum. Terhadap perbuatan yang melawan hukum dikenakan sanksi.¹⁰

⁹ Riduan Syahrani, *Rangkuman Intisari Ilmu Hukum*, Pustaka Kartini, Jakarta, Cetakan pertama, Juli 1991, hal. 23-24.

¹⁰ Sudarto, *Kapita Selekta Hukum Pidana*, Alumni, Bandung, 1986, hal. 111.

Dilihat secara fungsional, sistem penegakan hukum itu merupakan suatu sistem aksi. Ada sekian banyak aktivitas yang dilakukan oleh alat perlengkapan negara dalam penegakan hukum. Yang dimaksud dengan alat penegak hukum biasanya adalah "kepolisian dan kejaksaan". Tetapi kalau penegakan hukum itu diartikan secara luas, maka penegakan hukum itu menjadi tugas pembentuk undang-undang, hakim instansi pemerintah, dan aparat eksekusi pidana.¹¹

Dalam menegakkan hukum ada tiga hal yang harus diperhatikan, yaitu kepastian hukum, kemanfaatan, dan keadilan.¹² Oleh karena itu, Satjipto Rahardjo menyatakan, bahwa penegakan hukum merupakan suatu usaha untuk mewujudkan ide-ide tentang keadilan, kepastian hukum dan kemanfaatan sosial menjadi kenyataan. Proses perwujudan ide-ide itulah yang merupakan hakikat dari penegakan hukum.¹³

Hukum harus dilaksanakan dan ditegakkan. Menurut Soerjono Soekanto, penegakan hukum bukan semata-mata berarti pelaksanaan perundang-undangan, tetapi penegakan hukum yang mengandung nilai-nilai yang sesuai dengan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.¹⁴ Adapun faktor-faktor yang mempengaruhi penegakan hukum adalah:

1. Faktor hukumnya sendiri. Dalam hal ini, yang dimaksud adalah undang-undang dalam arti materiel, yaitu peraturan tertulis yang berlaku umum dan dibuat oleh penguasa pusat maupun daerah yang sah. Dengan demikian, maka undang-undang dalam arti materiel mencakup:
 - a. Peraturan pusat yang berlaku untuk semua warga negara atau suatu golongan tertentu saja maupun yang berlaku umum di sebagian wilayah negara.
 - b. Peraturan setempat yang hanya berlaku di suatu tempat atau daerah saja.¹⁵
2. Faktor penegak hukum, yakni pihak-pihak yang membentuk maupun menerapkan hukum. Ruang lingkup dari istilah "penegak hukum" adalah luas sekali, karena mencakup mereka yang secara langsung dan tidak langsung berkecimpung di bidang penegakan.¹⁶

¹¹ *Ibid.*, hal. 112.

¹² Sudikno Mertokusumo dalam "Mengetahui Hukum" sebagaimana dikutip dalam Riduan Syahrani dalam "Rangkuman Intisari Ilmu Hukum", Pustaka Kartini, Juli 1991, hal. 161.

¹³ Satjipto Rahardjo dalam Masalah Penegakan Hukum sebagaimana dikutip dalam Riduan Syahrani, *ibid.*

¹⁴ Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, PT RajaGrafindo Persada, Jakarta, 2008, hal. 7.

¹⁵ *Ibid.*, hal. 11.

¹⁶ *Ibid.*, hal 19.

3. Faktor sarana atau fasilitas yang mendukung penegakan hukum. Sarana atau fasilitas tersebut antara lain mencakup tenaga manusia yang berpendidikan dan terampil, organisasi yang baik, peralatan yang memadai, keuangan yang cukup, dan seterusnya.¹⁷
4. Faktor masyarakat, yakni lingkungan di mana hukum tersebut berlaku atau diterapkan. Penegakan hukum berasal dari masyarakat dan bertujuan untuk mencapai kedamaian di dalam masyarakat. Masyarakat dapat mempengaruhi penegakan hukum.¹⁸
5. Faktor kebudayaan, yakni hasil karya, cipta dan rasanya yang didasarkan pada karsa manusia di dalam pergaulan hidup. Faktor kebudayaan sebenarnya bersatu padu dengan faktor masyarakat.¹⁹

Kelima faktor tersebut saling berkaitan dengan eratnya, karena merupakan esensi dari penegakan hukum serta menjadi tolok ukur efektivitas penegakan hukum.²⁰

Berkaitan dengan penanganan *cyber crime*, maka faktor hukum yang dimaksud adalah UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan peraturan perundang-undangan lain yang terkait termasuk peraturan pelaksanaannya. Faktor penegak hukum meliputi para pihak yang langsung atau tidak langsung berkecimpung dalam penegakan UU No. 11 Tahun 2008, yaitu kepolisian, kejaksaan, pengadilan, dan instansi pemerintah yang menangani teknologi informasi. Sedangkan faktor sarana atau fasilitas yang mendukung penegakan hukum *cyber crime* antara lain organisasi dan cara kerja para penegak hukum, peralatan yang memadai, dan keuangan yang cukup. Adapun faktor masyarakat dan kebudayaan dalam penegakan hukum *cyber crime* adalah lingkungan di mana hukum tersebut berlaku atau diterapkan. Dalam hal ini termasuk kebiasaan/budaya dan kondisi sosial ekonomi masyarakat setempat.

Walaupun sudah ada norma hukum yang mempunyai sifat memaksa, namun belum ada jaminan bahwa norma hukum tersebut ditaati oleh masyarakat. Agar norma-norma tersebut ditaati diadakan ancaman hukuman, yaitu hukuman perdata, hukuman administrasi, dan/atau hukuman pidana untuk norma-norma hukum yang bersangkutan. Pelaku (subyek) dan tingkah laku yang dirumuskan (norma) serta ancaman hukuman (sanksi) disebut sebagai hukum materiil.

¹⁷ *Ibid.*, hal. 37.

¹⁸ *Ibid.*, hal. 45.

¹⁹ *Ibid.*, hal. 59.

²⁰ *Ibid.*, hal. 8-9.

Sedangkan untuk dapat melaksanakan ancaman hukuman, diadakan ketentuan yang mengatur kekuasaan badan-badan peradilan dan ketentuan tentang acara penyelesaian pelanggaran hukum materiil yang disebut sebagai hukum formil.²¹ Norma hukum formil bukan mengatur tingkah laku yang terlarang/diharuskan, melainkan mengatur kekuasaan badan-badan peradilan dan acaranya.

Pelaksanaan tugas badan-badan peradilan dilakukan oleh hakim, jaksa/penuntut umum dan penyidik/polisi. Hakim memeriksa dan mengadili perkara pidana maupun perdata yang diajukan kepadanya. Jaksa/penuntut umum melakukan penuntutan yang pelaksanaannya hanya dalam bidang hukum pidana. Sedangkan penyidik melakukan penyidikan hanya dalam bidang hukum pidana.

II. Metode Penelitian

A. Waktu dan Tempat Penelitian

Penelitian tentang "Penegakan Hukum terhadap Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik" ini merupakan suatu penelitian hukum yang melakukan analisis terhadap norma-norma yang terdapat dalam peraturan perundang-undangan yang berkaitan dengan kejahatan dunia maya, pendapat dan pengalaman aparat penegak hukum dalam menangani kejahatan dunia maya, serta peran Pemerintah/Pemerintah Daerah dalam mencegah dan memberantas kejahatan dunia maya.

Penelitian dilaksanakan pada bulan Oktober sampai dengan Desember 2009. Sedangkan penelitian lapangan dilakukan pada tanggal 30 November sampai dengan 6 Desember 2009. Adapun daerah yang menjadi lokasi penelitian adalah Denpasar (Bali). Pemilihan daerah tersebut karena Bali merupakan daerah budaya, pariwisata, dan bisnis dimana komputer menjadi suatu kebutuhan yang digunakan sebagai prasarana. Di samping itu, menurut Kepala Unit IT dan *Cyber Crime* Bareskrim Polri Komisararis Besar Petrus R. Golose, dari hasil penelusuran Polri, Bali merupakan daerah yang rawan kejahatan seksual *cyber*. Untuk menangkal kejahatan yang menyalahgunakan teknologi di Indonesia, Polda Bali merupakan salah satu Polda yang dilengkapi dengan piranti lunak penangkal eksploitasi anak secara *online* lewat *CETS (Child Exploitation Tracking System)*.²²

²¹ S.R. Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*, Penerbit Alumni Ahaem – Petehaem, Jakarta 1989, hal. 10-11.

²² "Bocah Bali dan Lombok Rawan Kejahatan Seksual Cyber", <http://www.detikinet.com/read/2007/11/22/164308/856256/398/boc...>, diakses tanggal 11 Agustus 2009.

B. Bahan/Cara Pengumpulan Data

Data yang diperlukan dalam penelitian ini adalah data primer dan data sekunder. Data primer diperoleh langsung dari hasil wawancara secara mendalam dengan para pihak berdasarkan panduan wawancara yang telah dipersiapkan sebelumnya. Adapun para pihak yang diwawancarai adalah Hakim Pengadilan Negeri, Polisi, dan Jaksa, serta pejabat Pemerintah/Pemerintah Daerah terkait di tempat penelitian. Sedangkan data sekunder mencakup dokumen resmi (peraturan perundang-undangan terkait), buku-buku dan hasil penelitian, kliping, dan berbagai data yang diakses dari internet. Pengumpulan data sekunder dalam bentuk dokumen atau bahan pustaka dilakukan sebelum dan setelah penelitian dilakukan.

C. Metode Analisis Data

Data yang ada dianalisis dengan metode penelitian kualitatif, yaitu data yang terkumpul atau diperoleh, baik data sekunder maupun data primer disusun dan dianalisis dengan mengacu pada norma hukum yang terdapat dalam peraturan perundang-undangan dan norma-norma yang hidup dan berkembang dalam masyarakat.

III. Hasil Penelitian dan Pembahasan

A. Pemanfaatan Teknologi Informasi dan Penyalahgunaannya oleh Masyarakat

Peningkatan kualitas hidup semakin menuntut manusia untuk melakukan berbagai aktivitas dengan mengoptimalkan sumber daya yang dimilikinya. Untuk itu, penggunaan teknologi informasi dalam aktivitas manusia menjadi suatu keharusan. Perkembangan ilmu pengetahuan dan teknologi, terutama teknologi informasi seperti internet, sangat menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat.

Teknologi informasi (TI) dapat dimanfaatkan dalam berbagai bidang kehidupan antara lain dalam bidang pendidikan, bisnis, pemerintahan, dan sosial. Dalam bidang pendidikan, manfaat TI antara lain berbagi hasil penelitian,

konsultasi dengan pakar, perpustakaan *online*, diskusi *online*, dan kelas *online*. Pemanfaatan TI sangat membantu kelancaran komunikasi dalam bisnis.²³

Peranan TI dalam bidang pemerintahan untuk meningkatkan hubungan pemerintah, dalam hal ini lembaga pemerintah yang bersangkutan dengan pihak-pihak lain, seperti masyarakat dan kalangan pengusaha/dunia usaha, serta dengan lembaga pemerintah lainnya. Sedangkan untuk memantau kondisi sosial masyarakat, Pemerintah memanfaatkan TI dengan programnya yang disebut ICT4PR (*information and communication technology for poverty reduction*). ICT4PR membangun pusat-pusat TI yang disebut *telecenter*. Manfaat *telecenter* bagi masyarakat adalah sebagai sumber informasi dan sarana belajar, menumbuhkan jiwa kewirausahaan, meningkatkan informasi, melihat peluang yang lebih luas, dan mengembangkan perdagangan.²⁴

Di samping bermanfaat bagi kehidupan manusia, TI juga dapat disalahgunakan, yaitu dalam bentuk pelanggaran hak cipta, *cyber crime*, penyebaran virus komputer, pornografi, perjudian, dan penipuan. Adapun karakteristik dari *cyber crime*²⁵ adalah:

- a. kejahatan melintasi batas negara;
- b. sulit menentukan hukum yang berlaku karena melintasi batas negara;
- c. menggunakan peralatan-peralatan yang berhubungan dengan komputer dan internet;
- d. mengakibatkan kerugian yang lebih besar dibanding kejahatan konvensional; dan
- e. pelaku memahami dengan baik internet, komputer, dan aplikasinya.

Menurut Kepala Biro Hukum Pemerintah Provinsi Bali, Bapak Mangku, dikelompokkan ke dalam *cyber crime*, penyalahgunaan TI melalui telepon selular merupakan kejahatan yang sering dilaporkan di Provinsi Bali. Modus yang digunakan biasanya melalui undian berhadiah, dimana pengguna telepon selular diinformasikan telah menjadi pemenang dan diharapkan segera mentransfer sejumlah dana. Tahun 2008 jumlah kerugian yang ditanggung dengan kejahatan SMS (*short message service*) ini mencapai 108 juta rupiah hanya dalam waktu lima menit.²⁶ Selain itu, menurut Didik B. Santoso (PT Telkom), dari berbagai

²³ Karyadi S.Pd., "Peranan dan Dampak Penggunaan Teknologi Informasi dan Telekomunikasi," <http://www.docstoc.com/docs/26072418/bab-3-PERANAN-DAN-DAMPAK-PENGGUNAAN-TEKNOLOGI-INFORMASI-DAN-TELEKOMUNIKASI>, diakses tanggal 26 April 2010.

²⁴ *Ibid.*

²⁵ *Ibid.*

²⁶ Disampaikan pada saat *focuss group discussion* tanggal 1 Desember 2009 di Kantor Pemerintah Provinsi Bali, Denpasar.

jenis kejahatan *cyber*, seperti *hacking*, *spamming*, dan melalui *e-mail*, modus yang sering muncul adalah dalam bentuk undangan untuk berinvestasi kecil dengan hasil yang besar. Sedangkan *cyber crime* yang sering terjadi di Bali cenderung mengarah pada pornografi dan kejahatan seksual *online*.²⁷

Untuk mencegah terjadinya *cyber crime*, PT Telkom telah menerapkan beberapa kebijakan yang berlaku secara nasional. *Pertama*, adalah penggunaan sistem DNS (*Domain Name Service*) Nawala yang melakukan penyaringan terhadap domain-domain URL (*The Universal Resource Locator*) yang bermuatan pornografi. *Kedua*, terkait dengan masalah *spamming* dan *phising*, Telkom telah membuat *account* khusus bagi pelanggan yang membuat pengaduan penyalahgunaan alamat *e-mail* atau *black campaign*. Mekanisme penggunaannya adalah mereka yang merasa mendapat serangan mengadukan kepada Telkom melalui *abuse@telkom.net.id* akan adanya *spamming* atau penyampaian informasi yang tidak benar. Langkah berikutnya, ada penelusuran oleh Telkom sehingga diketahui siapa yang mengirim jika alamat yang digunakan adalah alamat Telkom.²⁸

Khusus untuk mencegah terjadinya *cyber crime* di Bali, pada bulan November 2009 PT Telkom telah meresmikan Pusat Teknologi Informasi di Kuta. Empat pintu masuk ke Bali sudah terpantau, termasuk beberapa titik di Kota Denpasar juga sudah terpantau dengan *integrated system*. PT Telkom daerah Bali telah sering bekerja sama dengan pihak Kepolisian dalam pengawasan *information and communication technology* (ICT). Selain itu, Telkom juga mendukung Kepolisian dalam pemanfaatan dan pengamanan CCTV.²⁹

Berdasarkan hal di atas, PT Telkom telah memberikan dukungan kepada aparat Kepolisian dalam melakukan pencegahan terjadinya *cyber crime*, baik dengan menerapkan berbagai kebijakan secara nasional maupun upaya khusus yang dilakukan di daerah tertentu, seperti Bali.

B. Pengaturan *Cyber Crime* dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mulai berlaku pada tanggal 21 April 2008 telah mengisi kekosongan aturan hukum di dunia maya, terutama masalah dokumen elektronik

²⁷ Disampaikan pada saat *focus group discussion* tanggal 1 Desember 2009 di Kantor Pemerintah Provinsi Bali, Denpasar.

²⁸ *Ibid.*

²⁹ *Ibid.*

atau perilaku *cyber crime* seperti pemalsuan kartu kredit (*carding*), pornografi, perjudian internet, dan *hacking*. UU tersebut diharapkan dapat menjamin kepastian hukum bagi masyarakat yang melakukan transaksi secara elektronik.

Yayasan Lembaga Konsumen Indonesia (YLKI) menyambut baik disetujuinya Rancangan Undang-Undang (RUU) ITE menjadi undang-undang. Pengurus YLKI, Sudaryatmo, mengatakan selama ini banyak konsumen yang terjebak iklan di internet. Ada 3 masalah yang sering muncul, *pertama*, produk yang dijual tidak sesuai dengan yang diterima; *kedua*, kepastian pengantaran produk; *ketiga*, masalah sengketa bila ada konsumen yang tidak puas. Dalam UU ITE hal ini sudah diatur dalam Pasal 9, yang menyebutkan, bahwa "Pelaku usaha yang menawarkan produk melalui Sistem Elektronik harus menyediakan informasi yang lengkap dan benar berkaitan dengan syarat kontrak, produsen, dan produk yang ditawarkan."

UU ITE mengatur pemanfaatan teknologi informasi dan transaksi elektronik serta mendukung pengembangan teknologi informasi melalui infrastruktur hukum. Adapun yang dimaksud dengan teknologi informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.³⁰ Sedangkan transaksi elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.³¹

Penyelenggaraan sertifikasi elektronik dan sistem elektronik dalam undang-undang diatur dalam bab tersendiri. Penyelenggara sertifikasi elektronik harus menyediakan informasi yang akurat, jelas, dan pasti kepada setiap pengguna jasa,³² yang meliputi:

- a. metode yang digunakan untuk mengidentifikasi penandatanganan;
- b. hal yang dapat digunakan untuk mengetahui data diri pembuat tanda tangan elektronik; dan
- c. hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan tanda tangan elektronik.

UU ITE juga memuat ketentuan yang tegas mengenai perbuatan yang dilarang, yaitu dalam Pasal 27, sebagai berikut:

- (1) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik

³⁰ Pasal 1 angka 3 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

³¹ Pasal 1 angka 2 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

³² Pasal 14 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.

- (2) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.
- (3) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.
- (4) Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Selain perbuatan di atas, UU ITE juga melarang perbuatan menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik, dan menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).³³

Disamping itu, setiap orang yang mengirimkan informasi elektronik dan/atau dokumen elektronik yang berisi ancaman kekerasan atau menak-nakuti yang ditujukan secara pribadi juga dapat dikenakan sanksi pidana. UU ITE melindungi semua informasi dan transaksi elektronik, baik berupa *email*, nota elektronik, *short message service (SMS)*, layanan *mobile banking*, layanan *content provider*, dan lain-lain.

Sanksi pidana yang dapat dikenakan terhadap pelaku tindak pidana dalam UU ITE sangat berat. Tindakan melawan hukum yang sanksi pidananya paling ringan adalah dengan sengaja dan melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 600.000.000,- (enam ratus juta rupiah).³⁴ Ancaman sanksi pidana terhadap orang yang mendistribusikan dan membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik, seperti yang dituduhkan terhadap Prita, dipidana dengan

³³ Pasal 28 UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

³⁴ Pasal 46 ayat (1) jo Pasal 30 ayat (1) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu milyar rupiah).³⁵ Sedangkan ancaman sanksi pidana yang paling berat dikenakan terhadap korporasi yang melakukan perbuatan yang dilarang dalam UU ITE, dipidana dengan pidana pokok ditambah dua pertiga.³⁶

Dengan ancaman pidana yang berat, UU ITE sebagai peraturan yang baru perlu disosialisasikan. Untuk itu Telkom secara internal telah mengadakan sosialisasi sejak tahun 2008 sampai ke Nusa Tenggara. Sosialisasi eksternal sudah pernah dilaksanakan oleh Telkom di daerah Jakarta, Semarang, dan Surabaya.

Sementara UU ITE masih disosialisasikan, dalam daftar Program Legislasi Nasional (Prolegnas) prioritas RUU yang akan dibahas dalam tahun 2010 terdapat Rancangan Undang-Undang (RUU) tentang Tindak Pidana Teknologi Informasi. Sampai saat ini RUU yang rencananya diajukan oleh Pemerintah belum masuk ke DPR. Namun, penulis memperoleh draf RUU tentang Tindak Pidana di Bidang Teknologi Informasi dari seorang staf di Departemen Komunikasi dan Informatika. Dalam RUU disebutkan bahwa "Teknologi Informasi adalah suatu teknik atau cara elektronik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan menyebarkan informasi".³⁷

RUU memuat sejumlah pelanggaran pemanfaatan teknologi informasi dalam Pasal 8, berbunyi sebagai berikut:

"Hal-hal yang merupakan pelanggaran dalam Undang-Undang ini adalah memanfaatkan Teknologi Informasi dengan melawan hukum; melakukan intersepsi dengan melawan hukum; dengan sengaja dan melawan hukum merusak atau mengganggu data yang tersimpan dalam alat penyimpan data elektronik yang tersusun sebagai bagian dari sistem komputer; dengan sengaja menghilangkan bukti-bukti elektronik yang dapat dijadikan alat bukti sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer; dengan sengaja merusak atau mengganggu sistem informasi, sistem komputer, jaringan komputer, dan Internet; memanfaatkan Teknologi Informasi untuk

³⁵ Pasal 45 ayat (1) jo Pasal 27 ayat (3) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

³⁶ Pasal 53 ayat (4) UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

³⁷ Pasal 1 angka 7 Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, disusun oleh Mas Wigrantoro Roes Setiyadi, *Country Coordinator, Global Internet Policy Initiative-Indonesia*, Jakarta, Juli, 2005.

menipu, menghasut, memfitnah, menjatuhkan nama baik seseorang atau organisasi; memanfaatkan Teknologi Informasi untuk menyebarkan gambar, tulisan atau kombinasi dari keduanya yang mengandung sifat-sifat pornografi; memanfaatkan Teknologi Informasi untuk membantu terjadinya percobaan, atau persekongkolan yang menjurus pada kejahatan.”

Pelanggaran pemanfaatan teknologi informasi di atas dalam UU ITE sudah termasuk dalam perbuatan yang dilarang dan dikenakan ancaman sanksi pidana, kecuali “dengan sengaja menghilangkan bukti-bukti elektronik yang dapat dijadikan alat bukti sah di pengadilan yang terdapat pada suatu sistem informasi atau sistem komputer” dan “setiap badan hukum penyelenggara jasa akses internet atau penyelenggara layanan teknologi informasi, baik untuk keperluan komersial maupun keperluan internal perusahaan, dengan sengaja tidak menyimpan atau tidak dapat menyediakan catatan transaksi elektronik sedikitnya untuk jangka waktu dua tahun.”

Pelanggaran “memanfaatkan teknologi informasi dengan melawan hukum” sifatnya sangat umum, sehingga setiap tindakan pelanggaran atau tindak pidana di bidang teknologi informasi dapat dikategorikan sebagai memanfaatkan Teknologi Informasi dengan melawan hukum. Disamping itu, apabila dicermati, pelanggaran pemanfaatan teknologi informasi dalam RUU merupakan delik hukum karena dalam KUHP sudah dinyatakan sebagai tindakan yang bertentangan dengan hukum atau peraturan tertulis, sehingga tidak tepat apabila dikategorikan sebagai bentuk pelanggaran. Tindakan tersebut seharusnya dikategorikan sebagai kejahatan.

RUU tentang Tindak Pidana di Bidang Teknologi Informasi juga memuat sejumlah tindak pidana pemanfaatan teknologi informasi, yaitu Kejahatan terhadap nyawa dan keselamatan negara; Pencurian; Mengakses Tanpa Hak; Mengakses Tanpa Hak terhadap Sistem Informasi Strategis; Pemalsuan Identitas; Mengubah dan Memalsukan Data; Mengubah Data yang Merugikan Orang Lain; Perubahan Asusila; Pornografi Anak-anak; Bantuan Kejahatan; Mengakses Tanpa Hak terhadap Komputer yang Dilindungi; dan Teror.

Disamping itu, RUU juga memuat tindak pidana yang berkaitan dengan Teknologi Informasi sebagai Sasarannya, yaitu Intersepsi; Merusak Situs Internet; Penyadapan terhadap Jaringan Komunikasi Data; Pemalsuan Nomor *Internet Protocol*; Merusak *Database* atau Enkripsi; Penggunaan Nama Domain

Tidak Sah; Penyalahgunaan Surat Elektronik; Pelanggaran Hak Cipta; dan Pelanggaran Hak Privasi.

Melihat rincian tindak pidana di atas, maka RUU memuat tindak pidana secara lebih rinci dibandingkan dengan UU ITE. RUU memuat tiga jenis pelanggaran/kejahatan pemanfaatan teknologi informasi, *pertama*, pelanggaran pemanfaatan teknologi informasi, *kedua*, tindak pidana pemanfaatan teknologi informasi, dan *ketiga*, tindak pidana yang berkaitan dengan teknologi informasi sebagai sasarannya.

Berdasarkan modus dan korban, *cyber crime* dikelompokkan menjadi 2 (dua) bagian,³⁸ yaitu *pertama*, kejahatan yang menggunakan teknologi informasi dan telekomunikasi untuk melakukannya; dan *kedua*, kejahatan yang dilakukan dengan tujuan dan sasaran teknologi informasi dan telekomunikasi. RUU sudah membagi *cyber crime* seperti pengelompokan tersebut.

Namun, jika RUU tentang Tindak Pidana di Bidang Teknologi Informasi dibahas untuk menjadi UU maka akan terjadi tumpang tindih peraturan dengan UU ITE. Oleh karena itu, RUU tentang Tindak Pidana di Bidang Teknologi Informasi perlu ditinjau kembali. Alternatif lain, mengakomodasi substansi yang belum terdapat dalam UU ITE dalam revisi UU ITE. Di antara 12 RUU Tambahan dan Perubahan Penyiapan Penyusunan RUU dalam Prolegnas RUU Prioritas Tahun 2010, RUU tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik termasuk yang ditetapkan untuk dibahas dalam tahun 2010.³⁹

C. Kendala dalam Penegakan Hukum terhadap UU No. 11 Tahun 2008

Cyber crime merupakan transnasional *crime* yang tidak menimbulkan "fear of crime" namun dampaknya sangat besar terhadap dunia teknologi informasi, perdagangan, perbankan, dan sebagainya. Oleh karena itu, diperlukan penanganan yang serius dari semua pihak mengingat teknologi informasi khususnya internet telah dijadikan sebagai sarana untuk membangun masyarakat yang berbudaya informasi. Keberadaan undang-undang yang mengatur *cyber crime* memang diperlukan, tetapi undang-undang tidak ada

³⁸ "Penegakan Hukum *Cyber Crime* di Indonesia", <http://my.opera.com/sibbyan/blog/show.dml/2844461>, diakses tanggal 10 Agustus 2009.

³⁹ Lampiran Keputusan Dewan Perwakilan Rakyat Republik Indonesia Nomor 119/PIMP/II/2009-2010 tentang Penetapan 12 Rancangan Undang-Undang Tambahan dan Perubahan Penyiapan Penyusunan Rancangan Undang-Undang dalam Program Legislasi Nasional Rancangan Undang-Undang Prioritas Tahun 2010.

artinya jika pelaksana dari undang-undang tidak memiliki kemampuan atau keahlian dalam bidang itu.

Penyidik pada Unit *Transnational Crime Team* Kepolisian Daerah (Polda) Bali, Komisaris Polisi Tri Kuncoro, ketika diwawancarai mengatakan bahwa dalam penyidikan kasus *cyber crime*, penyidik dihadapkan pada problematika yang rumit, terutama dalam mengumpulkan dan menyita alat bukti. Ada kendala dalam pengumpulan bukti-bukti yang amat rumit terkait dengan teknologi informasi dan kode-kode *digital* yang membutuhkan sumber daya manusia serta peralatan komputer forensik yang baik.⁴⁰

Kesulitan lain yang dihadapi penyidik adalah dalam upaya menangkap pelaku seringkali penyidik dihadapkan pada sulitnya menentukan secara pasti siapa pelaku *cyber crime* karena mereka melakukan tindak pidana cukup melalui komputer yang dapat dilakukan di mana saja tanpa ada yang mengetahuinya sehingga tidak ada saksi yang mengetahui secara langsung. Hasil pelacakan paling jauh hanya dapat menemukan *An Internet Protocol (IP Address)* dari pelaku dan komputer yang digunakan. Hal itu akan semakin sulit apabila menggunakan komputer di warnet sebab saat ini masih jarang sekali warnet yang melakukan registrasi terhadap pengguna jasa mereka sehingga kita tidak dapat mengetahui siapa yang menggunakan komputer tersebut pada saat terjadi tindak pidana. Disamping itu, banyak tersangka maupun saksi yang berada di luar yurisdiksi hukum Indonesia, sehingga untuk melakukan pemeriksaan maupun penindakan amatlah sulit.⁴¹

Disamping adanya kendala dalam proses penyidikan, kendala lain adalah belum adanya persamaan persepsi dalam penanganan kasus *cyber crime* antara penyidik dan penuntut umum, dimana terhadap kasus yang terkait *cyber crime* kepolisian sudah menggunakan UU ITE sedangkan dalam tuntutananya kejaksaan menggunakan KUHP.⁴² Sebaliknya, kepolisian menggunakan KUHP, kejaksaan menambahkan dengan UU ITE, seperti dalam kasus Prita.

Berkaitan dengan perbuatan yang dilarang dalam Pasal 27 UU ITE, bulan Mei 2009 timbul kasus yang menimbulkan kontroversi, dikenal dengan kasus Prita, di mana Prita Mulyasari diajukan ke persidangan karena dianggap telah mencemarkan nama Rumah Sakit Omni Internasional Alam Sutra Tangerang (RS Omni). Prita yang kecewa dengan pelayanan RS Omni menumpahkan rasa

⁴⁰ Wawancara dilakukan pada tanggal 3 Desember 2009.

⁴¹ *Ibid.*

⁴² Berdasarkan wawancara dengan Komisaris Polisi Tri Kuncoro, Unit *Transnational Crime Team* Polda Bali, tanggal 3 Desember 2009.

kecewanya itu melalui *email* dan disebarakan melalui *mailing list*. Berita kecewa itu akhirnya menyebar dari satu *email* ke *email* lainnya, sampai terbaca oleh pihak RS Omni. RS Omni memperkarakan Prita dan berujung pada penahanan di Lembaga Pemasyarakatan Wanita Tangerang selama 20 hari sejak tanggal 13 Mei 2009 dengan tuduhan pencemaran nama baik.⁴³

Prita didakwa dengan Pasal 45 ayat (1) *juncto* Pasal 27 ayat (3) UU ITE yang menyebutkan: "Setiap orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik." Sedangkan sanksinya tercantum dalam Pasal 45 ayat (1), bahwa "Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), dan ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp. 1.000.000.000,- (satu milyar rupiah)."

Penanganan kasus tersebut oleh aparat penegak hukum mendapat kecaman dari berbagai pihak, antara lain Kepala Divisi Monitoring Pelayanan Publik *Indonesia Corruption Watch* (ICW), Ade Irawan, yang menduga kuat terdapatnya unsur gratifikasi dari RS Omni kepada kejaksaan. Agar kejadian seperti itu tidak terjadi lagi di masa mendatang, Komisi Pemberantasan Korupsi (KPK) harus terlibat secara tuntas dalam pengusutan dugaan itu, paling tidak dengan cara melakukan pengawasan secara terus menerus terkait hal tersebut.⁴⁴ Serikat Rakyat Miskin Indonesia (SRMI) melakukan unjuk rasa di Kantor Departemen Kesehatan Jakarta, mengecam kasus yang dialami Prita Mulyasari. Ketua Umum SRMI Marlo Sitompul mengatakan, aksi yang melibatkan kaum ibu dan anak-anak tersebut dilakukan untuk menuntut dihentikannya liberalisasi sektor kesehatan. Mereka menuntut Prita Mulyasari dibebaskan dari segala tuduhan, cabut UU ITE dan segera disahkan RUU tentang Rumah Sakit.⁴⁵

Disamping itu, beberapa tokoh memberikan dukungan moril kepada Prita dengan mengunjunginya di Lembaga Pemasyarakatan Tangerang, antara lain, Ketua Umum Partai Demokrasi Indonesia Perjuangan (PDIP) Megawati didampingi oleh anggota terpilih PDIP Rieke Dyah Pitaloka dan Wakil Ketua

⁴³ "Kasus Prita Mulyasari vs RS Omni dan Internet Marketing", <http://www.baliorange.web.id/kasus-prita-mulyasari-vs-rs-omni-dan-internet-marketing/>, *op.cit.*

⁴⁴ "ICW Menduga ada Gratifikasi di RS Omni Internasional", <http://www.jimmyzakaria.com/berita/icw-menduga-ada-gratifikasi-di-rs-omni-international/>, diakses tanggal 1 Maret 2010.

⁴⁵ "SRMI Mengecam Kasus Prita Mulyasari", <http://www.jimmyzakaria.com/berita/srmi-mengecam-kasus-prita-mulyasari/>, diakses tanggal 1 Maret 2010.

Dewan Pers Leo Batubara didampingi anggota Dewan Pers Abdullah Alamudi beserta rombongan.⁴⁶

Akhirnya, Prita mendapat penanggungan penahanan menjadi tahanan kota dan hasil eksaminasi dari Jaksa Agung Muda Pidana Umum menunjukkan adanya ketidakprofesionalan Jaksa yang menangani kasus tersebut. Ketidakprofesionalan tersebut bermula ketika Jaksa melihat ada kekurangan pasal dalam berkas acara yang diajukan Polisi ke Kejati Banten. Melihat hal itu, Jaksa meminta Polisi menambahkan Pasal 27 *juncto* Pasal 45 UU No. 11 Tahun 2008 mengenai ITE. Kemudian oleh Kepolisian pasal itu hanya ditaruh di atas berkas, tidak ditaruh dalam berita acara pendapat kepolisian. Kekeliruan terjadi karena Jaksa lalu menetapkan berkas sudah P-21 atau lengkap, padahal penambahan pasal itu tidak dimasukkan dalam berita acara.⁴⁷

Mendasarkan pada penanganan kasus Prita, aparat penegak hukum belum sepenuhnya memahami apa itu *cyber crime*. Dengan perkataan lain, kondisi sumber daya manusia khususnya aparat penegak hukum masih lemah. Oleh karena itu, dalam rangka meningkatkan pengetahuan, kemampuan, dan keterampilan dalam penyidikan *cyber crime*, kepolisian telah mengikutsertakan penyidik dan penyidik pembantu untuk mengikuti pelatihan maupun seminar untuk mengikuti kursus *Cyberlaw* (Hukum Telematika) maupun seminar di bidang *Information Technology*.⁴⁸

Salah satu hal menarik dalam dinamika perkembangan organisasi Kepolisian Daerah Bali, sebagaimana dikatakan Komisariss Besar Polisi Made Sudarsana yang mengepalai Bidang Telekomunikasi dan Informatika di Kepolisian Daerah Bali, adalah keberadaan Bali *Security Council*. Lembaga ini digagas oleh Kapolda Bali pada saat itu, Inspektur Jenderal Polisi Drs. Made Mangkupastike yang sekarang menjabat Gubernur Bali. Pasca Bom Bali I. Pemerintah Pusat memberikan atensi yang cukup besar (bantuan dana 16 miliar rupiah) terhadap lembaga ini dengan membentuk *call centre* berteknologi tinggi dan salah satunya diharapkan dapat menanggulangi masalah *cyber crime*.⁴⁹

⁴⁶ "Prita Mulyasari akan Dikunjungi Dewan Pers", <http://www.jimmyzakaria.com/berita/prita-mulyasari-akan-dikunjungi-dewan-pers>, diakses tanggal 1 Maret 2010.

⁴⁷ "Jaksa Kasus Prita tidak Profesional", <http://www.jimmyzakaria.com/berita/jaksa-kasus-prita-tidak-profesional>, diakses tanggal 1 Maret 2010.

⁴⁸ *Ibid*.

⁴⁹ Disampaikan pada saat *focuss group discussion* tanggal 1 Desember 2009 di Kantor Pemerintah Provinsi Bali, Denpasar.

Selain itu, Kepolisian Indonesia juga telah melakukan kerjasama dengan kepolisian negara lain dalam berbagai bentuk. Akademi Kepolisian di Semarang merupakan salah satu institusi kepolisian yang sudah lama menjalin kerjasama dengan negara lain. Sedangkan Polda Bali bekerjasama dengan pemerintah Australia dalam pendirian *Transnational Crime Unit* Bali. Bantuan disampaikan oleh pemerintah Australia dan *Australian Federal Police (AFP)*. Kerjasama dengan Australia dalam menangani kasus kejahatan transnasional termasuk salah satunya kejahatan yang terkait dengan *cyber crime* dimana perjanjian tersebut dilakukan dalam bentuk *Memorandum of Understanding (MoU)*.⁵⁰

Timbulnya kasus Prita ternyata berdampak pada penanganan *cyber crime*. Dari hasil penelitian di Bali, terungkap bahwa aparat penegak hukum menjadi "takut" menerapkan UU ITE. Gede Edy Bujanayasa, jaksa pada Kejaksaan Negeri Denpasar, mengatakan, bahwa "belajar dari kasus Prita yang mengenakan UU ITE dalam kasus pencemaran nama baik terhadap RS Omni Internasional melalui internet, kejaksaan sangat berhati-hati dalam menggunakan UU tersebut".⁵¹ Hal ini terlihat dari kenyataan bahwa untuk kejahatan *cyber* di daerah Bali hanya terdapat dua kasus yang sudah dilimpahkan ke kejaksaan dan dasarnya masih menggunakan KUHP.⁵² Keberadaan UU ITE ternyata belum dapat menjamin *cyber crime* dapat tertangani dengan baik, dibutuhkan keberanian dan kecermatan aparat penegak hukum dalam menerapkan UU ITE.

IV. Penutup

A. Kesimpulan

Pemanfaatan teknologi informasi seperti komputer dan internet dapat meningkatkan produktivitas dan efisiensi dalam bidang pendidikan, bisnis, pemerintahan, dan sosial. Hal ini pada akhirnya dapat meningkatkan kesejahteraan masyarakat. Disamping bermanfaat dalam kehidupan manusia, teknologi informasi juga dapat disalahgunakan dan menjadi sarana efektif perbuatan melawan hukum dalam bentuk *cyber crime* (kejahatan dunia maya). *Cyber crime* merupakan kejahatan transnasional dan mempunyai karakteristik tertentu, antara lain menggunakan sarana komputer dan internet dalam melakukan kejahatan.

⁵⁰ *Ibid.*

⁵¹ Wawancara dilakukan pada tanggal 2 Desember 2009.

⁵² *Ibid.*

Untuk menangani kejahatan dunia maya, DPR RI dan Pemerintah telah membentuk UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE mengatur pemanfaatan teknologi informasi dan transaksi elektronik serta ketentuan mengenai perbuatan yang dilarang dan ketentuan pidana. UU diharapkan dapat menjamin kepastian hukum bagi masyarakat dalam melakukan transaksi secara elektronik.

Berdasarkan hasil penelitian, penerapan UU ITE terhadap *cyber crime* masih menimbulkan persoalan. Aparat penegak hukum belum mempunyai persamaan persepsi terhadap ketentuan yang diatur dalam UU ITE terutama mengenai perbuatan yang dilarang, seperti dalam kasus Prita. Sementara itu, dalam Program Legislasi Nasional prioritas RUU yang akan dibahas dalam tahun 2010 terdapat RUU tentang Tindak Pidana Teknologi Informasi dan RUU tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Substansi RUU tentang Tindak Pidana di Bidang Teknologi Informasi terdapat tumpang tindih peraturan dengan UU ITE.

Berkaitan dengan penegakan hukum *cyber crime* terdapat kendala dalam proses penyidikan. Penyidik kesulitan dalam mengumpulkan dan menyita barang bukti, menentukan secara pasti siapa pelaku *cyber crime*, dan menyamakan persepsi dengan penuntut umum. Kasus Prita juga berdampak pada penerapan hukum terhadap *cyber crime*. Aparat penegak hukum menjadi "takut" menerapkan UU ITE. Sementara itu, terhadap penyalahgunaan teknologi di bidang informasi, PT Telkom telah menerapkan beberapa kebijakan secara internal, yaitu penggunaan sistem *domain name service* dan membuat *account* khusus bagi pelanggan yang membuat pengaduan penyalahgunaan alamat *email* atau *black campaign*.

B. Rekomendasi

Agar penerapan UU No. 11 Tahun 2008 terhadap *cyber crime* dilakukan dengan tepat dan ada persamaan persepsi di antara aparat penegak hukum, maka perlu sosialisasi UU No. 11 Tahun 2008. terhadap aparat penegak hukum. Disamping itu, aparat penegak hukum perlu meningkatkan kualitas dan kemampuannya dalam kaitannya dengan teknologi informasi dan transaksi elektronik, mengingat *cyber crime* dilakukan dengan peralatan yang canggih.

Pemerintah perlu meninjau kembali apabila ingin mengajukan RUU tentang Tindak Pidana Teknologi Informasi ke DPR agar tidak terjadi tumpang tindih peraturan dengan UU ITE. Alternatif lain, RUU tentang Perubahan atas

UU No. 11 Tahun 2008 dapat mengakomodasi substansi yang terdapat dalam RUU tentang Tindak Pidana Teknologi Informasi yang belum diatur.

DAFTAR PUSTAKA

Buku:

- Ahmad M. Ramli, *Cyber Law dan HAKI dalam Sistem Hukum Indonesia*, PT Refika Aditama, Bandung, Cetakan pertama, Oktober 2004.
- Departemen Komunikasi dan Informatika, *Menuju Kepastian Hukum di Bidang: Informasi dan Transaksi Elektronik*, Tahun 2005.
- Edmon Makarim, *Kompilasi Hukum Telematika*, PT RajaGrafindo Persada, Jakarta, Cetakan kedua, Desember 2004.
- Riduan Syahrani, *Rangkuman Intisari Ilmu Hukum*, Pustaka Kartini, Jakarta, Cetakan pertama, Juli 1991.
- Soerjono Soekanto, *Faktor-faktor yang Mempengaruhi Penegakan Hukum*, PT RajaGrafindo Persada, Jakarta, 2008.
- Sri Setianingsi Suwardi, *Masalah-masalah Hukum Perjanjian Pinjaman Internasional*, Makalah pada Fakultas Pasca Sarjana Bidang Hukum Internasional UNPAD, 1990.
- S.R. Sianturi, *Asas-asas Hukum Pidana di Indonesia dan Penerapannya*, Penerbit Alumni Ahaem – Petehaem, Jakarta 1989.
- Sudarto, *Kapita Selekta Hukum Pidana*, Alumni, Bandung, 1986.
- Sudikno Mertokusumo dalam "Mengenal Hukum" sebagaimana dikutip oleh Riduan Syahrani dalam "Rangkuman Intisari Ilmu Hukum", Pustaka Kartini, Juli 1991.

Peraturan Perundang-undangan:

- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Rancangan Undang-Undang Tindak Pidana di Bidang Teknologi Informasi, disusun oleh Mas Wigrantoro Roes Setiyadi, *Country Coordinator, Global Internet Policy Initiative-Indonesia*, Jakarta, Juli, 2005.
- Lampiran Keputusan Dewan Perwakilan Rakyat Republik Indonesia Nomor 119/PIMP/II/2009-2010 tentang Penetapan 12 Rancangan Undang-Undang Tambahan dan Perubahan Penyiapan Penyusunan Rancangan Undang-Undang dalam Program Legislasi Nasional Rancangan Undang-Undang Prioritas Tahun 2010.

Keputusan Dewan Perwakilan Rakyat Indonesia Nomor 41B/DPRI/2009-2010
tentang Program Legislasi Nasional Rancangan Undang-Undang
Prioritas Tahun 2010

Surat Kabar:

"Kejahatan Virtual Kian Mengganas", *Media Indonesia*, 12 Oktober 2009.

Internet:

"Cyber Crime", Indonesia Tertinggi di Dunia", <http://nasional.kompas.com/read/xml/2009/03/25/18505497/Cyber.....>, diakses tanggal 10 Agustus 2009.

"Penegakan Hukum *Cyber Crime* di Indonesia", <http://my.opera.com/sibbyan/blog/show.dml/2844461>, diakses tanggal 10 Agustus 2009.

"Bocah Bali dan Lombok Rawan Kejahatan Seksual *Cyber*", <http://www.detikinet.com/read/2007/11/22/164308/856256/398/boc...>, diakses tanggal 11 Agustus 2009.

"*Cyber Crime*/Kejahatan Dunia Maya", <http://riya93.blogspot.com/2009/03/blog-spot----26.html>, diakses tanggal 20 Oktober 2009.

"Jangan Atur Semua Informasi Internet, *Cyber Crime* Saja", <http://id.news.yahoo.com/dtik/20091222/tpl-jangan-atur-semua-info...>, diakses tanggal 23 Desember 2009.

"Kasus Prita Mulyasari vs RS Omni dan Internet Marketing", <http://www.baliorange.web.id/kasus-prita-mulyasari-vs-rs-omni-dan-internet-marketing/>, diakses tanggal 1 Maret 2010.

"ICW Menduga ada Gratifikasi di RS Omni Internasional", <http://www.jimmyzakaria.com/berita/icw-menduga-ada-gratifikasi-di-rs-omni-international>, diakses tanggal 1 Maret 2010.

"SRMI Mengecam Kasus Prita Mulyasari", <http://www.jimmyzakaria.com/berita/srmi-mengecam-kasus-prita-mulyasari>, diakses tanggal 1 Maret 2010.

"Prita Mulyasari akan Dikunjungi Dewan Pers", <http://www.jimmy-zakaria.com/berita/prita-mulyasari-akan-dikunjungi-dewan-pers>, diakses tanggal 1 Maret 2010.

"Jaksa Kasus Prita tidak Profesional", <http://www.jimmyzakaria.com/berita/jaksa-kasus-prita-tidak-profesional>, diakses tanggal 1 Maret 2010.

Karyadi S.Pd., "Peranan dan Dampak Penggunaan Teknologi Informasi dan Telekomunikasi," <http://www.docstoc.com/docs/26072418/bab-3-PERANAN-DAN-DAMPAK-PENG-GUNAAN-TEKNOLOGI-INFORMASI-DANTELEKOMUNI-KASI>, diakses tanggal 26 April 2010.

Informan Utama:

1. Didik B. Santoso (PT Telekomunikasi wilayah Provinsi Bali, Denpasar).
2. Mangku (Kepala Biro Hukum Pemerintah Provinsi Bali).
3. Agus Budiana (Biro Organisasi Pemerintah Provinsi Bali).
4. Krisdiyanto (Dinas Perhubungan Provinsi Bali).
5. Wayan (KPID).
6. Komisaris Polisi Tri Kuncoro (Unit *Transnational Crime Team* Polda Bali).
7. Komisaris Besar Polisi Made Sudarsana (Kepala Bidang Telekomunikasi dan Informatika Polda Bali).
8. Gede Edy Bujanayasa (jaksa tindak pidana umum pada Kejaksaan Negeri Denpasar, Bali).

