PENANGGULANGAN *CYBER CRIME* MELALUI *PENAL POLICY*

Oleh : Marwin*

Abstraksi

Perkembangan teknologi informasi dan komunikasi menyebabkan hubungan dunia menjadi tanpa batas dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung dengan demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum. Di satu sisi kemajuan teknologi membawa dampak positif, namun juga membawa dampak negatif, dengan munculnya berbagai jenis high tech crime dan cyber crime. Dilihat dari perspektif hukum pidana, upaya penanggulangan cyber crime dengan penal policy, khususnya di Indonesia dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana), aspek pertanggungjawaban pidana atau pemidanaan, dan aspek jurisdiksi, juga patut mendapat perhatian adalah tindakan penyidikan terhadap cyber crime dalam upaya mengungkap dan memberikan sanksi bagi setiap pelaku cyber crime.

Kata kunci: *cyber crime, penal policy.*

A. Pendahuluan

Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (*borderless*) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung dengan demikian cepat. Teknologi informasi saat ini menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

Kehidupan manusia modern saat ini tidak dapat dilepaskan dari bahkan terkadang sangat bergantung pada kemajuan teknologi canggih/maju (*high tech* atau *advanced technology*) di bidang informasi dan elektronik melalui jaringan internasional (internet). Di satu sisi kemajuan teknologi membawa dampak positif, seperti adanya *e-mail; e-commerce; e-learning; EFTS (Electronic Funds Transfer System); Internet Banking; Cyber Bank; On-line Business* dan sebagainya. Namun juga membawa dampak negatif, dengan munculnya berbagai jenis *high tech crime* dan *cyber crime*, sehingga dinyatakan bahwa *cyber crime is the most recent type of crime* dan *cyber crime is part of the seamy side of the Information Society* (*cyber crime* merupakan bagian sisi paling buruk dari Masyarakat informasi).

Berkembangnya *cyber crime* dapat dilihat dari muculnya berbagai istilah seperti *economic cyber crime; EFT (Electronic Funds Transfers) Crime, Cybank Crime; Internet Banking Crime; On-line Business Crime; Cyber/electronic Money Laundering; High Tech WWC (White Collar Crime); Cyber Terorism; Cyber Sex; Cyber Criminals* dan sebagainya. Bahkan dalam *back-ground paper* lokakarya *Measures to Combat Computer-related Crime* Kongres XI PBB dinyatakan bahwa teknologi baru yang mendunia di bidang komunikasi dan informasi memberikan bayangan gelap (*a dark shadow*), karena memungkinkan terjadinya bentuk-bentuk eksploitasi baru, kesempatan baru untuk aktivitas kejahatan, dan bentuk-bentuk baru dari kejahatan.

Oleh karena itu dilihat dari perspektif hukum pidana, upaya penanggulangan *cyber crime* khususnya di Indonesia dapat dilihat dari berbagai aspek, antara lain aspek kebijakan kriminalisasi (formulasi tindak pidana); aspek pertanggungjawaban pidana atau pemidanaan (termasuk aspek alat bukti/pembuktian); dan aspek jurisdiksi. Hal lain yang juga patut mendapat

* Penulis adalah Dosen Tetap pada Fakultas Syari'ah IAIN Raden Intan Lampung

perhatian adalah tindakan penyidikan terhadap *cyber crime* dalam upaya mengungkap dan memberikan sanksi bagi setiap pelaku *cyber crime*.

B. Kebijakan Kriminalisasi atau Formulasi Tindak Pidana *Cyber Crime*

Kebijakan penanggulangan *cyber crime* dengan hukum pidana termasuk bidang *penal policy* yang merupakan bagian dari *criminal policy* (kebijakan penanggulangan kejahatan). Dilihat dari sudut *criminal policy*, upaya penanggulangan kejahatan (termasuk penanggulangan *cyber crime*) tidak dapat dilakukan semata-mata secara parsial dengan hukum pidana (sarana penal), tetapi harus pula ditempuh dengan pendekatan integral/sistemik.[1] Sebagai salah satu bentuk *high tech crime* yang dapat melampaui batas-batas negara (bersifat *transnational/transborder*), merupakan hal yang wajar jika upaya penanggulangan *cyber crime* juga harus ditempuh dengan pendekatan teknologi (*techno prevention*). Di samping itu, diperlukan pula pendekatan budaya/kultural, pendekatan moral/edukatif, dan bahkan pendekatan global melalui kerjasama internasional.

Operasionalisasi kebijakan penal meliputi kriminalisasi, dekriminalisasi, penalisasi dan depenalisasi. Penegakan hukum pidana tersebut sangat tergantung pada perkembangan politik hukum, politik kriminal, dan politik sosial. Oleh karena itu, penegakan hukum tidak hanya memperhatikan hukum yang otonom, melainkan memperhatikan juga masalah kemasyarakatan dan ilmu perilaku sosial.[2]

Kebijakan kriminalisasi merupakan suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana).[3] Jadi pada hakikatnya, kebijakan kriminalisasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (*penal*) sehingga itu termasuk bagian dari kebijakan hukum pidana (*penal policy*), khususnya kebijakan formulasi.

Menurut Bassiouni, keputusan untuk melakukan kriminalisasi dan dekriminalisasi harus didasarkan pada faktor-faktor kebijakan tertentu yang mempertimbangkan bermacam-macam faktor, termasuk:[4]

1. Keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil-hasil yang ingin dicapai;
2. Analisis biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;
3. Penelitian atau penafsiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas-prioritas lainnya dalam pengalokasian sumber-sumber tenaga manusia;
4. Pengaruh social dari kriminalisasi dan dekriminalisasi yang berkenaan dengan atau dipandang dari pengaruh-pengaruhnya yang sekunder.

Sudarto menyatakan dalam melakukan kriminalisasi suatu perbuatan perlu diperhatikan empat hal berikut:[5]

1. Penggunaan hukum pidana perlu memperhatikan tujuan pembangunan nasional, yaitu mewujudkan masyarakat adil dan makmur yang merata baik material maupun spiritual berdasarkan Pancasila;
2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana seyogyanya merupakan perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian (material dan/atau spiritual) pada warga masyarakat;
3. Penggunaan hukum pidana perlu mempertimbangkan prinsip "biaya dan hasil" (*cost and benefit principle*);
4. Penggunaan hukum pidana perlu pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum pidana, jangan sampai ada kelebihan beban tugas (*overbelasting*).

---

[1] Barda Nawawi Arief, *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan*, Citra Aditya Bakti, Bandung, 2005, hlm. 125.

[2] Bambang Poernomo, *Kapita Selekta Hukum Pidana*, Liberty, Yogyakarta, 1988, hlm. 52

[3] Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, Citra Aditya Bakti, Bandung, 2003, hlm. 240.

[4] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, Citra Aditya Bakti, Bandung, 2002, hlm. 32.

[5] Sudarto, *Hukum dan Hukum Pidana*, Alumni, Bandung, 1981, hlm. 44-48.

Berkenaan dengan kebijakan kriminalisasi perbuatan dalam dunia *cyber* (maya), dalam lokakarya/workshop mengenai *computer related crime* yang diselenggarakan dalam kongres PBB X pada bulan April 2000, dinyatakan bahwa negara-negara anggota harus berusaha melakukan harmonisasi ketentuan-ketentuan yang berhubungan dengan kriminalisasi, pembuktian, dan prosedur (*states should seek harmonization of the relevant provisions on criminalization evidence and procedure*). Jadi masalahnya bukan sekedar bagaimana membuat kebijakan hukum pidana (kebijakan kriminalisasi/formulasi/legislasi) di bidang penanggulangan *cyber crime* tetapi bagaimana ada harmonisasi kebijakan penal di berbagai negara. Ini berarti bahwa kebijakan kriminalisasi tentang masalah *cyber crime* bukan semata-mata masalah kebijakan nasional Indonesia, tetapi juga terkait dengan kebijakan regional dan internasional.

Melakukan kriminalisasi *cyber crime* ada lima hal yang perlu diperhatikan oleh pembentuk undang-undang (legislator), yaitu:[6]

1. Kriminalisasi harus merupakan upaya yang mendukung tujuan akhir kebijakan kriminal, yaitu melindungi dan mensejahterakan masyarakat;
2. Perbuatan yang akan dikriminalisasi tersebut benar-benar dicela oleh masyarakat;
3. Perlu diperhitungkan tentang keuntungan dan kerugian kriminalisasi;
4. Perlu diupayakan agar tidak terjadi over-kriminalisasi yang dapat berpengaruh secara sekunder terhadap kepentingan masyarakat;
5. Perlu disesuaikan antara kemampuan penegak hukum dengan penegakan hukum.

Kebijakan kriminalisasi atau formulasi hukum pidana di Indonesia yang berkaitan dengan masalah *cyber crime*, selama ini dapat diidentifikasikan sebagai berikut:[7]

1. Dalam KUHP

   Perumusan tindak pidana di dalam KUHP kebanyakan masih bersifat konvensional dan belum secara langsung dikaitkan dengan perkembangan *cyber crime*, selain itu juga terdapat berbagai kelemahan dan keterbatasan dalam menghadapi perkembangan teknologi dan *high tech crime* yang sangat bervariasi. Contoh dalam hal menghadapi masalah pemalsuan kartu kredit dan transfer dana elektronik saja, KUHP mengalami kesulitan karena tidak adanya aturan khusus mengenai hal tersebut. Ketentuan yang ada hanya mengenai: (a) sumpah/keterangan palsu (Pasal 242); (b) pemaluan mata uang dan uang kertas (Pasal 244-252); (c) pemalsuan materai dan merk (Pasal 253-262); dan (d) pemalsuan surat (Pasal 263-276).

2. Undang-undang di luar KUHP

   a. UU No.36 Tahun 1999 tentang Telekomunikasi, mengancam pidana terhadap perbuatan: (1) memanipulasi akses ke jaringan telekomunikasi (Pasal 50 jo.22); (2) menimbulkan gangguan fisik dan elektromagnetik terhadap penyelenggaraan telekomunikasi (Pasal 55 jo.38); (3) menyadap informasi melalui jaringan telekomunikasi (Pasal 56 jo.40).

   b. Pasal 26A UU No. 20 Tahun 2001 tentang Perubahan Atas UU No.31 Tahun 1999 tentang Pemberantasan Tindak Pidana Korupsi; Pasal 38 UU No.15 Tahun 2002 tentang Tindak Pidana Pencucian Uang; dan pasal 44 ayat (2) UU No.30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi; mengakui *electronic record* sebagai alat bukti yang sah.

   c. UU No.32 Tahun 2002 tentang Penyiaran, antara lain mengatur tindak pidana:

      (1) Pasal 57 jo. 36 ayat (5) mengancam pidana terhadap siaran yang : a) bersifat fitnah, menghasut, menyesatkandan/atau bohong; b) menonjolkan unsur kekerasan, cabul, perjudian, penyalahgunaan narkotika dan obat terlarang; atau c) mempertentangkan suku, agama, ras, dan antar golongan.

      (2) Pasal 57 jo. 36 ayat (6) mengancam pidana terhadap siaran yng memperolokkan, merendahkan, melecehkan, dan/atau mengabaikan nilai-nilai agama, martabat manusia Indonesia, atau merusak hubungan internasional.

      (3) Pasal 58 jo. 46 ayat (3) mengancam pidana terhadap siaran iklan niaga yang didalamnya memuat: a) promosi yang dihubungkan dengan ajaran suatu agama;

---

[6] Widodo, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta, hlm. 60-61.
[7] Barda Nawawi Arief, *Pembaharuan…*, hlm. 127-128.

ideologi, pribadi dan/atau kelompok, yang menyinggung perasaan dan/atau merendahkan martabat orang lain, ideologi lain, pribadi lain, atau kelompok lain; b) promosi minuman keras atau sejenisnya dan bahan atau zat adiktif; c) promosi rokok yang memperagakan wujud rokok; d) hal-hal yang bertentangan dengan kesusilaan masyarakat dan nilai-nilai agama; dan/atau e) eksploitasi anak di bawah umur 18 tahun.

d. UU No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU-ITE), Bab VII Perbuatan yang dilarang, memuat ketentuan pidana bagi setiap orang yang dengan sengaja dan tanpa hak atau melawan hukum mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya informasi elektronik dan/atau dokumen elektronik yang memiliki muatan:

   (1) Melanggar kesusilaan; memiliki muatan perjudian; memiliki muatan penghinaan dan/atau pencemaran nama baik; memiliki muatan pemerasan dan/atau pengancaman (Pasal 27).

   (2) Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik; menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antar golongan (SARA) (Pasal 28)

   (3) Mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi (Pasal 29).

   (4) Mengakses komputer dan/atau sistem elektronik milik orang lain; mengakses komputer dan/atau sistem elektronik dengan tujuan memperoleh informasi elektronik dan/atau dokumen elektronik; mengakses komputer dan/atau sistem elektronik dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan (Pasal 30).

   (5) Melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik; melakukan intersepsi elektronik atas transmisi informasi elektronik dan/atau dokumen elektronik yang tidak bersifat publik (Pasal 31)

   (6) Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan, suatu informasi elektronik dan/atau dokumen elektronik milik orang lain atau milik publik; memindahkan atau mentransfer informasi elektronik dan/atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak; mengakibatkan terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya (Pasal 32).

   (7) Terganggunya sistem elektronik dan/atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya (Pasal 33).

   (8) Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki (a) perangkat keras atau perangkat lunak yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud Pasal 27-33; (b) sandi lewat komputer, kode akses, atau hal lain yang sejenis dengan itu yang ditujukan agas sistem elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan dalam Pasal 27-33 (Pasal 34).

   (9) Melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan informasi elektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut dianggap seolah-olahdata yang otentik (Pasal 35).

   (10) Melakukan perbuatan sebagaimana dimaksud dalam Pasal 27-34 yang mengakibatkan kerugian bagi orang lain (Pasal 36).

   (11) Melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27-36 diluar wilayah Indonesia terhadap sistem elektronik yang berada di wilayah Yurisdiksi Indonesia (Pasal 37).

Kriminalisasi *cyber crime* di Indonesia khususnya dalam UU-ITE dapat dibagi dalam dua kategori, yaitu perbuatan yang menggunakan komputer sebagai sarana kejahatan, dan perbuatan-perbuatan yang menjadikan komputer sebagai sasaran kejahatan. Kejahatan yang menggunakan

komputer sebagai sarana adalah setiap tindakan yang mendayagunakan data komputer, sistem komputer, dan jaringan komputer sebagai alat untuk melakukan kejahatan di ruang maya bukan ruang nyata. Kejahatan yang menjadikan komputer sebagai sasaran adalah setiap perbuatan dengan menggunakan komputer yang diarahkan pada data komputer, sistem komputer, atau jaringan komputer, atau ketiganya secara bersama-sama. Perbuatan tersebut dilakukan di ruang maya bukan ruang nyata, sehingga seluruh aktivitas yang dilarang oleh peraturan perundang-undangan terjadi di ruang maya.[8]

C. Pertanggungjawaban Pidana atau Pemidanaan

Pertanggungjawaban pidana pada hakikatnya mengandung pencelaan pembuat (subjek hukum) atas tindak pidana yang telah dilakukannya. Oleh karena itu, pertanggungjawaban pidana mengandung di dalamnya pencelaan/ pertangjawaban objektif dan subjektif. Artinya, secara objektif si pembuat telah melakukan tindak pidana menurut hukum yang berlaku (asas legalitas), dan secara subjektif si pembuat patut dicela atau dipersalahkan/dipertanggungjawabkan atas tindak pidana yang dilakukannya itu (asas *culpabilitas*/kesalahan) sehingga ia patut dipidana.

Persyaratan dan asas-asas pertanggungjawaban pidana tersebut merupakan hal-hal yang sudah diterima secara umum dan konvensional dalam doktrin/teori, maupun dalam peraturan perundang-undangan (hukum positif). Untuk adanya pertanggungjawaban pidana pertama-tama harus dipenuhi persyaratan objektif, yaitu perbuatannya harus telah merupakan tindak pidana menurut hukum yang berlaku (asas legalitas).

Berdasarkan persyaratan objektif yang konvensional, pertanggungjawaban *cyber crime* tentunya harus didasarkan pada sumber hukum perundang-undangan yang berlaku saat ini, baik didalam KUHP maupun dalam undang-undang khusus di luar KUHP. Namun kenyataannya dalam peraturan perundang-undangan yang ada dan berlaku sekarang di Indonesia, tidak semua kasus *cyber crime* dapat dijangkau. Selain itu dalam peraturan perundang-undangan yang ada sekarang (baik KUHP maupun UU khusus di luar KUHP) memiliki berbagai kelemahan dan kemampuan sangat terbatas dalam menghadapi berbagai masalah *cyber crime.* Berbagai masalah atau kelemahan tersebut antara lain:[9]

1. Di dalam UU No.32 Tahun 2002 tentang penyiaran, tidak ada penentuan kualifikasi delik (sebagai kejahatan atau pelanggaran) sehingga dapat menimbulkan masalah yuridis;
2. Dalam berbagai undang-undang, terdapat subjek hukum berupa korporasi namun tidak membuat aturan tentang pertanggungjawaban pidana untuk korporasi, misalnya dalam UU No.36 Tahun 1999 tentang Telekomunikasi;
3. Dalam undang-undang yang mengatur pertanggungjawaban pidana korporasi (seperti dalam undang-undang korupsi dan pencucian uang), tidak diatur ketentuan mengenai aturan pidana pengganti denda untuk korporasi apabila denda tidak dibayar;
4. Dalam undang-undang yang memuat ancaman pidana minimal khusus, tidak ada ketentuan mengenai aturan atau pedoman penerapan pidana minimal khusus;
5. Pengakuan yuridis terhadap *electronic record* sebagai alat bukti hanya ada pada Undang-undang Korupsi (UU No. 31 Tahun 1999 jo. UU No. 20 Tahun 2001, UU No. 30 Tahun 2002 tentang Pemberantasan Tindak Pidana Korupsi); dan Undang-Undang Tindak Pidana Pencucian Uang (UU No. 15 Tahun 2002), sehingga menjadi masalah apabila akan diterapkan untuk tindak pidana lainnya khususnya yang berkaitan dengan *cyber crime*.

Masih terbatasnya undang-undang yang ada khususnya yang mengatur *cyber crime*, berarti asas legalitas konvensional saat ini menghadapi tantangan serius dari perkembangan *cyber crime*. Hal ini dapat dimaklumi karena:[10]

a. *Cyber crime* berada di lingkungan elektronik dan dunia maya yang sulit diidentifikasi secara pasti, sedangkan asas legalitas konvensional bertolak dari perbuatan riel dan kepastian hukum;

---

[8] Widodo, *Aspek…*, hlm. 64-66.

[9] Barda Nawawi Arief, *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia*, Rajawali Press, PT RajaGrafindo Persada, Jakarta, 2006, hlm. 102-105.

[10] Barda Nawawi Arief, *Tindak...*, hlm. 78.

b. *Cyber crime* berkaitan erat dengan perkembangan teknologi canggih yang sangat cepat berubah, sedangkan asas legalitas konvensional bertolak dari sumber hukum formal (undang-undang) yang statis;
c. *Cyber crime* melampaui batas-batas negara, sedangkan perundang-undangan suatu negara pada dasarnya atau pada umumnya hanya berlaku di wilayah teritorialnya sendiri.

Pertanggungjawaban pidana pelaku *cyber crime* juga harus mengandung makna pencelaan subjektif. Artinya secara subjektif si pelaku patut dicela atau dipersalahkan atau dipertanggungjawabkan atas tindak pidana yang dilakukannya sehingga ia patut dipidana. Secara singkat sering dinyatakan, tiada pidana (pertanggungjawaban pidana) tanpa kesalahan (asas *culpabilitas*). Asas *culpabilitas* ini pun tentunya harus diperhatikan dalam masalah pertanggungjawaban pidana *cyber crime*. Walaupun mungkin menghadapi tantangan sendiri dalam kasus-kasus *cyber crime* karena tidak mudah membuktikan adanya unsur kesalahan (*dolus/culpa*) dalam masalah *cyber crime*.

D. Jurisdiksi

Sisi lain dari persyaratan objektif untuk pertanggungjawaban *cyber crime* adalah masalah jurisdiksi, khususnya yang berkaitan dengan masalah ruang berlakunya hukum pidana menurut tempat. Dalam sistem hukum pidana yang sekarang berlaku, hukum pidana pada umumnya hanya berlaku di wilayah negaranya sendiri (asas territorial), dan untuk warga negaranya sendiri (asas personal/nasional aktif). Hanya untuk tindak pidana tertentu dapat digunakan asas nasional pasif dan asas universalitas.

Masalah jurisdiksi *cyber crime* termasuk masalah yang sangat serius, Barbara Etter mengidentifikasikan beberapa masalah kunci yang berkait atau yang menyebabkan timbulnya masalah jurisdiksi ini dalam konteks internasional, antara lain:[11]

1. Tidak adanya konsensus global mengenai jenis-jenis CRC (*computer related crime*) dan tindak pidana pada umumnya;
2. Kurangnya keahian aparat penegak hukum dan ketidakcukupan hukum untuk melakukan investigasi dan mengakses sistem komputer;
3. Adanya sifat transnasional dari *computer crime*;
4. Ketidakharmonisan hukum acara/prosedural di berbagai negara;
5. Kurangnya sinkronisasi mekanisme penegakan hukum, bantuan hukum, ekstradisi, dan kerja sama internasional dalam melakukan investigasi *cyber crime.*

Membicarakan masalah jurisdiksi di ruang maya (*cyber space*), Masaki Hamano mengemukakan terlebih dahulu adanya jurisdiksi yang didasarkan pada prinsip-prinsip tradisional. Menurutnya ada tiga kategori jurisdiksi tradisional, yaitu jurisdiksi legislatif (*legislative jurisdiction* atau *jurisdiction to prescribe*); jurisdiksi yudisial (*judicial jurisdiction* atau *jurisdiction to adjudicate*); dan jurisdiksi eksekutif (*executive jurisdiction* atau *jurisdiction to enforce*).[12]

Mengacu pada pengertian ketiga jurisdiksi di atas, maka dapat dikatakan bahwa jurisdiksi tradisional berkaitan dengan batas-batas kewenangan negara di tiga bidang penegakan hukum. *Pertama*, kewenangan pembuatan hukum substantif; *kedua*, kewenangan mengadili atau menerapkan hukum; *ketiga*, kewenangan melaksanakan/memaksakan kepatuhan terhadap hukum yang dibuatnya.[13]

Masaki Hamano membedakan pengertian *cyber jurisdiction* dari sudut pandang dunia *cyber*/virtual dan dari sudut hukum. Dari sudut dunia virtual, *cyber jurisdiction* sering diartikan sebagai kekuasaan sistem operator dan para pengguna (users) untuk menerapkan aturan dan melaksanakannya pada suatu masyarakat di ruang *cyber*/virtual. Dari sudut hukum, *cyber jurisdiction* atau *jurisdiction on cyber space* adalah kekuasaan fisik pemerintah dan kewenangan pengadilan terhadap pengguna internet atau terhadap aktivitas mereka di ruang *cyber*.[14]

---

[11] Barda Nawawi Arief…, hlm. 143-144.
[12] Barda Nawawi Arief, *Tindak...*, hlm. 27-28.
[13] Barda Nawawi Arief, *Tindak...*, hlm. 28.
[14] Barda Nawawi Arief, *Kapit...*, hlm. 247-248.

Jadi membicarakan jurisdiksi *cyber* pada hakikatnya berkaitan dengan masalah kekuasaan atau kewenangan, yaitu siapa yang berkuasa atau berwenang mengatur dunia internet. Mengenai masalah ini, David R. Johnson dan David G. Post mengemukakan empat model yang bersaing, yaitu:[15]

a. Pelaksanaan kontrol dilakukan oleh badan-badan pengadilan yang saat ini ada (*the exesiting judicial forums*);
b. Penguasa nasional melakukan kesepakatan internasional mengenai *the governance of cyber space*;
c. Pembentukan suatu organisasi internasional baru (*a new international organization*) yang secara khusus menangani masalah-masalah di dunia internet; dan
d. Pemerintahan/pengaturan sendiri (*self governance*) oleh para pengguna internet.

Berkaitan dengan *cyber jurisdiction* ini, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Pasal 2 menyatakan bahwa undang-undang ini berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam undang-undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Penjelasan Pasal 2 UU-ITE menjelasakan bahwa undang-undang ini memiliki jangkauan yurisdiksi tidak semata-mata untuk perbuatan hukum yang berlaku di Indonesia dan/atau dilakukan oleh warga negara Indonesia, tetapi juga berlaku untuk perbuatan hukum yang dilakukan di luar wilayah hukum (yurisdiksi) Indonesia baik oleh warga negara Indonesia maupun warga negara asing atau badan hukum Indonesia maupun badan hukum asing yang memiliki akibat hukum di Indonesia, mengingat pemanfaatan teknologi informasi untuk informasi elektronik dan transaksi elektronik dapat bersifat lintas teritorial atau universal. Sedangkan yang dimaksud dengan “merugikan kepentingan Indonesia” adalah meliputi tetapi tidak terbatas pada merugikan kepentingan ekonomi nasional, perlindungan data strategis, harkat dan martabat bangsa, pertahanan dan keamanan negara, kedaulatan negara, warga negara, serta badan hukum Indonesia.

E. Hukum Acara dan Penyidikan

Pasal 42 UU ITE menyatakan penyidikan terhadap tindak pidana sebagaimana dimaksud dalam undang-undang ini, dilakukan berdasarkan ketentuan dalam hukum acara pidana dan ketentuan dalam undang-undang ini. Hal ini berarti segala ketentuan dalam KUHAP dan undang-undang lainnya yang berkaitan dengan hukum acara pidana, berlaku dalam rangka penyidikan dalam upaya mengungkap tindak pidana yang terjadi dalam dunia *cyber*.

Selain penyidik pejabat Polisi Negara Republik Indonesia (Polri), Pejabat Pegawai Negeri Sipil tertentu di lingkungan pemerintah yang lingkup tugas dan tanggung jawabnya di bidang teknologi informasi dan transaksi elektronik diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam undang-undang hukum acara pidana untuk melakukan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik. Penyidik Pegawai Negeri Sipil, berwenang:

a. Menerima laporan atau pengaduan;
b. Memanggil setiap orang atau pihak lainnya untuk didengar dan/atau diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana;
c. Melakukan pemeriksaan atas kebenaran laporan atau keterangan;
d. Melakukan pemeriksaan terhadap orang dan/atau badan usaha yang patut diduga melakukan tindak pidana;
e. Melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan teknologi informasi yang diduga digunakan untuk melakukan tindak pidana;
f. Melakukan penggeledahan terhadap tempat tertentu;
g. Melakukan penyegelan dan penyitaan;
h. Meminta bantuan ahli guna kepentingan penyidikan;
i. Mengadakan penghentian penyidikan.

[15] Barda Nawawi Arief, *Kapita...*, hlm. 248.

UU-ITE mengatur bahwa tindakan penyidikan tindak pidana di bidang teknologi informasi dan transaksi elektronik, harus dilakukan dengan memperhatikan perlindungan terhadap privasi, kerahasiaan, kelancaran pelayanan publik (masyarakat), integritas data, atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

Penggeledahan dan/atau penyitaan terhadap sistem elektronik yang terkait dengan dugaan tindak pidana harus dilakukan atas izin Ketua Pengadilan Negeri setempat. Dalam melakukan penggeledahan dan/atau penyitaan, penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum. Dalam melakukan penangkapan dan penahanan, penyidik melalui penuntut umum wajib meminta penetapan Ketua Pengadilan Negeri setempat dalam waktu satu kali dua puluh empat jam.

Guna mengungkap tindak pidana informasi elektronik dan transaksi elektronik, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti. Alat bukti penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan, berupa: (1) alat bukti sebagaimana dimaksud dalam ketentuan perundang-undangan, (2) alat bukti berupa informasi elektronik dan/atau dokumen elektronik.

Alat bukti berupa informasi elektronik dan/atau dokumen elektronik dalam rangka penyidikan, penuntutan, dan pemeriksaan persidangan tindak pidana *cyber crime* dalam UU-ITE, adalah:

a. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (*EDI*), surat elektronik (*electronic mail)*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya;
b. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya;
c. Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah. Merupakan perluasan dari alat bukti yang sah sesuai dengan hukum acara yang berlaku di Indonesia, yang dinyatakan sah apabila menggunakan sistem elektronik sesuai dengan ketentuan yang diatur dalam undang-undang ini. Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagai alat bukti hukum yang sah tidak berlaku untuk: (a) surat yang menurut undang-undang harus dibuat dalam bentuk tertulis; dan (b) surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta. Dimaksud dengan surat yang menurut undang-undang harus dibuat tertulis meliputi tetapi tidak terbatas pada surat berharga, surat yang berharga, dan surat yang digunakan dalam proses penegakan hukum acara perdata, pidana, dan administrasi negara.

F. Penutup

Dalam upaya penanggulangan *cyber crime*, Resolusi Kongres PBB VIII tahun 1990 mengenai CRC (*computer related crime*) mengajukan beberapa kebijakan antara lain:[16]

1. Mengimbau negara anggota untuk mengintensifkan upaya-upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah-langkah diantaranya:
   a. Melakukan modernisasi hukum pidana materiil dan hukum acara pidana;
   b. Mengembangkan tindakan-tindakan pencegahan dan pengamanan komputer;
   c. Melakukan langkah-langkah untuk membuat peka (sensitif) warga masyarakat, aparat pengadilan, dan penegak hukum, terhadap pentingnya pencegahan kejahatan yang berhubungan dengan komputer;

[16] Barda Nawawi Arief, *Tindak*..., hlm. 3-4.

d. Melakukan upaya-upaya pelatihan (training) bagi para hakim, pejabat, dan aparat penegak hukum mengenai kejahatan ekonomi dan *cyber crime*;
e. Memperluas *rule of ethics* dalam penggunaan komputer dan mengajarkannya melalui kurikulum informatika;
f. Mengadopsi kebijakan perlindungan korban *cyber crime* sesuai dengan Deklarasi PBB mengenai korban, dan mengambil langkah-langkah untuk mendorong korban melaporkan adanya *cyber crime*.

2. Mengimbau negara anggota meningkatkan kegiatan internasional dalam upaya penanggulangan *cyber crime*;
3. Merekomendasikan kepada Komite pengendalian dan Pencegahan Kejahatan (*Committee on Crime Prevention and Control*) PBB untuk:
   a. Menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *cyber crime* di tingkat nasional, regional, dan internasional;
   b. Mengembangkan penelitian dan analisis lebih lanjut guna menemukan cara-cara baru menghadapi problem *cyber crime* di masa yang akan dating;
   c. Mempertimbangkan *cyber crime* sewaktu mengimplementasikan perjanjian ekstradisi dan bantuan kerja sama di bidang penanggulangan kejahatan.

DAFTAR PUSTAKA

Bambang Poernomo. 1988. *Kapita Selekta Hukum Pidana*. Liberty. Yogyakarta.

Barda Nawawi Arief. 2002. *Bunga Rampai KebijakanHukum Pidana*. Citra Aditya Bakti. Bandung.

_____. 2003. *Kapita Selekta Hukum Pidana*. Citra Aditya Bakti. Bandung.

_____. 2005. *Pembaharuan Hukum Pidana dalam Perspektif Kajian Perbandingan.* Citra Aditya Bakti. Bandung.

_____. 2006. *Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia.* PT RajaGrafindo Persada. Jakarta.

Leden Marpaung. 2008. *Asas Teori Praktik Hukum Pidana.* Sinar Grafika. Jakarta.

Sudarto. 1981. *Hukum dan Hukum Pidana.* Alumni. Bandung.

Widodo. 2013. *Aspek Hukum Pidana Kejahatan Mayantara*. Aswaja Pressindo. Yogyakarta.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transfer Elektronik. 2009. Pustaka Fahima. Yogyakarta.