PERTEMUAN VII

CYBERLAW

7.1 Asas Hukum Untuk Dunia *Cyber*

Terdapat tiga pendekatan untuk mempertahankan keamanan di *Cyberspace* (ruang maya), yaitu : pendekatan teknologi, pendekatan sosial budaya-etika, dan pendekatan hukum. Untuk mengatasi gangguan keamanan pendekatan teknologi sifatnya mutlak dilakukan, sebab tanpa suatu pengamanan jaringan akan sangat mudah disusupi, dintersepsi, atau diakses secara ilegal dan tanpa hak.

Dalam ruang *Cyber* pelaku pelanggaran seringkali menjadi sulit dijerat karena hukum dan pengadilan Indonesia tidak memiliki yurisdiksi terhadap pelaku dan perbuatan hukum yang terjadi, mengingat pelanggaran hukum bersifat transnasional tetapi akibatnya justru memiliki implikasi hukum di Indonesia.

Dalam hukum internasional, dikenal tiga jenis yurisdiksi, yakni

1. jurisdiksi untuk menetapkan undang-undang *(the jurisdiction to prescribe)*
2. jurisdiksi untuk penegakan hukum *(the jurisdiction to enforce)*
3. jurisdiksi untuk menuntut *(the jurisdiction to adjudicate).*

Dalam kaitannya dengan penentuan hukum yang berlaku dikenal beberapa asas yang biasa digunakan, yaitu :

1. *subjective territoriality,* yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan di negara lain.
2. *objective territoriality,* yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi negara yang bersangkutan.
3. *nationality* yang menentukan bahwa negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku.

4. *passive nationality* yang menekankan jurisdiksi berdasarkan kewarganegaraan korban.
5. *protective principle* yang menyatakan berlakunya hukum didasarkan atas keinginan negara untuk melindungi kepentingan negara dari kejahatan yang dilakukan di luar wilayahnya, yang umumnya digunakan apabila korban adalah negara atau pemerintah.
6. asas *Universality.* Asas *Universality* selayaknya memperoleh perhatian khusus terkait dengan penanganan hukum kasus-kasus *Cyber*. Asas ini disebut juga sebagai *"universal interest jurisdiction"*. Pada mulanya asas ini menentukan bahwa setiap negara berhak untuk menangkap dan menghukum para pelaku pembajakan. Asas ini kemudian diperluas sehingga mencakup pula kejahatan terhadap kemanusiaan *(crimes against humanity)*, misalnya penyiksaan, genosida, pembajakan udara dan lain-lain.

Meskipun di masa mendatang asas jurisdiksi universal ini mungkin dikembangkan untuk *internet piracy*, seperti *computer, cracking, carding, hacking and viruses,* namun perlu dipertimbangkan bahwa penggunaan asas ini hanya diberlakukan untuk kejahatan sangat serius berdasarkan perkembangan dalam hukum internasional. Oleh karena itu, untuk ruang *Cyber* dibutuhkan suatu hukum baru yang menggunakan pendekatan yang berbeda dengan hukum yang dibuat berdasarkan batas-batas wilayah

7.1.1 Pengertian *Cyber*law

Secara akademis, terminologi "*Cyber* law" tampaknya belum menjadi terminologi yang sepenuhnya dapat diterima. Hal ini terbukti dengan dipakainya terminologi lain untuk tujuan yang sama seperti The law of the Internet, Law and the Information Superhighway, Information Technology Law, The Law of Information, dan sebagainya. Di Indonesia sendiri tampaknya belum ada satu istilah yang disepakati atau paling tidak hanya sekedar terjemahan atas terminologi "*Cyber* law". Sampai saat ini ada beberapa istilah yang dimaksudkan sebagai terjemahan dari "*Cyber* law", misalnya, Hukum Sistem Informasi, Hukum Informasi, dan Hukum Telematika (Telekomunikasi dan Informatika).

Cyber Law adalah aspek hukum yang artinya berasal dari kata "*Cyber*space Law" yang ruang lingkupnya meliputi aspek-aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai "online" dan memasuki dunia *Cyber* atau maya.

7.1.2 Ruang Lingkup *Cyber* Law

Pembahasan mengenai ruang lingkup ”*Cyber* law” dimaksudkan sebagai inventarisasi atas persoalan-persoalan atau aspek-aspek hukum yang diperkirakan berkaitan dengan pemanfaatan Internet. Secara garis besar ruang lingkup ”*Cyber* law” ini berkaitan dengan persoalan-persoalan atau aspek hukum.

Jonathan Rosenoer dalam *Cyber*law, the law of internet mengingatkan tentang ruang lingkup dari *Cyber* law, yaitu :

1. Copyright (hak cipta)
2. Trademark (hak Merk)
3. Defamation (pencemaran nama baik)
4. Hate Speech (fitnah, penghinaan, penistaan)
5. Hacking, Viruses, Illegal Acces (Serangan terhadap fasilitas komputer)
6. Duty Care (prinsip kehati – hatian)
7. Tindakan kriminal yang biasa menggunakan IT sebagai alat
8. Isu prosedural seperti yuridiksi, penyelidikan
9. Transaksi elektronik dan tanda tangan digital
10. Pornografi
11. Pencurian melalui internet
12. Perlindungan konsumen
13. Pemanfaatan internet dalam aktivitas sehari – hari seperti e-commerce, e-goverment, e-education

7.1.3 Perangkat hukum *Cyber* Law

Agar pembentukan perangkat perundang – undangan tentang teknologi informasi mampu mengarahkan segala aktivitas dan transaksi didunia maya/ *Cyber* sesuai dengan standar etik dan hukum yang disepakati maka proses pembuatanya diupayakan sebagai berikut :

a. Menerapkan pinsip – prinsip dan pengembangan teknologi informasi antara lain :
    1. Melibatkan unsur yang terkait (pemerintah, swasta dan profesional)
    2. Menggunakan pendekatan moderat untuk mensintesiskan prinsip hukum konvensional dan norma hukum baru yang akan terbentuk
    3. Memperhatikan keunikan dari dunia maya

4. Mendorong adanya kerjasama internasional mengingat sifat internet yang global
5. Menempatkan sektor swasta sebagai leader persoalan yang menyangkut industri dan perdagangan
6. Pemerintah harus mengambil peran dan tanggung jawab yang jelas untuk persoalan yang menyangkut kepentingan publik
7. Aturan hukum yang akan dibentuk tidak bersifat restriktif melainkan harus direktif dan futuristik

b. Melakukan pengkajian terhadap perundang – undangan nasional yang memiliki kaitan langsung maupun tidak langsung dengan munculnya persoalan hukum akibat transaksi di internet seperti UU hak cipta, UU Merk, UU Perseroan Terbatas, UU Penanaman Modal Asing, UU Perpajakan, UU pidana dll

7.1.4 Perangkat Hukum Internasional

Dalam rangka upaya menanggulangi dan menangani *Cyber* crime dewan keamanan PBB dalam resolusi kongres PBB VII/1990 mengenai "Computer related crime"mengajukan beberapa kebijakan antara lain :

- Menghimbau kepada negara anggota untuk mengintensifkan upaya – upaya penanggulangan penyalahgunaan komputer yang lebih efektif dengan mempertimbangkan langkah – langkah berikut :
  a. Melakukan modernisasi hukum pidana material dan hukum pidana acara
  b. Mengembangkan tindakan pencegahan dan pengamanan komputer
  c. Melakukan langkah untuk membuat peka warga masyarakat, aparat, terhadap pentingnya pencegahan kejahatan
  d. Melakukan training bagi hakim, pejabat dan aprat hukum tentang *Cyber* crime
  e. Memperluas rules of ethics dalam penggunaankomputer melalui kurikulum informasi
  f. Mengadopsi kebijakan perlindungan korban *Cyber* crime sesuai dengan deklarasi PBB
- Menhimbau negara anggota meningkatkan upaya penanggulangan *Cyber* crime
- Merekomendasikan kepada komite pengendalian dan pencegahan kejahatan PBB (***commitee on Crime Prevention and Control***) untuk menyebarluaskan pedoman dan standar untuk membantu negara anggota menghadapi *Cyber* crime, mengembangkan penelitian dan analisis untuk menemukan cara baru menghadapi *Cyber* crime di masa datang

Perangkat hukum internasional di bidang kejahatan *Cyber (Cyber Crime*) merupakan sebuah fenomena baru dalam tatanan Hukum Internasional modern mengingat kejahatan *Cyber* sebelumnya tidak mendapat perhatian negara-negara sebagai subjek Hukum Internasional. Munculnya bentuk kejahatan baru yang tidak saja bersifat lintas batas (transnasional) tetapi juga berwujud dalam tindakan-tindakan virtual telah menyadarkan masyarakat internasional tentang perlunya perangkat Hukum Internasional baru yang dapat digunakan sebagai kaidah hukum internasional dalam mengatasi kasus-kasus *Cybercrime*.

7.2 *Cyber*law Di Berbagai Negara

7.2.1 *Council of Europe Convention on Cyber crime*

Instrumen Hukum Internasional publik yang mengatur masalah Kejahatan *Cyber* yang saat ini paling mendapat perhatian adalah Konvensi tentang Kejahatan *Cyber (Convention on Cyber Crime*) 2001 yang digagas oleh Uni Eropa. Konvensi ini meskipun pada awalnya dibuat oleh organisasi Regional Eropa, tetapi dalam perkembangannya dimungkinkan untuk diratifikasi dan diakses oleh negara manapun di dunia yang memiliki komitmen dalam upaya mengatasi kejahatan *Cyber*.

Negara-negara yang tergabung dalam Uni Eropa *(Council of Europe)* pada tanggal 23 November 2001 di kota Budapest, Hongaria telah membuat dan menyepakati *Convention on Cybercrime* yang kemudian dimasukkan dalam *European Treaty Series* dengan Nomor 185. Konvensi ini akan berlaku secara efektif setelah diratifikasi oleh minimal 5 (lima) negara, termasuk paling tidak ratifikasi yang dilakukan oleh 3 (tiga) negara anggota *Council of Europe.* Substansi konvensi mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal *(criminalpolicy)* yang bertujuan untuk melindungi masyarakat dari *Cyber crime,* baik melalui undang-undang maupun kerjasama internasional.

Hal ini dilakukan dengan penuh kesadaran sehubungan dengan semakin meningkatnya intensitas digitalisasi, konvergensi, dan globalisasi yang berkelanjutan dari teknologi informasi, yang menurut pengalaman dapat juga digunakan untuk melakukan tindak pidana. Konvensi ini dibentuk dengan pertimbangan-pertimbangan antara lain sebagai berikut :

1. bahwa masyarakat internasional menyadari perlunya kerjasama antar Negara dan Industri dalam memerangi kejahatan *Cyber* dan adanya kebutuhan untuk melindungi kepentingan yang sah dalam penggunaan dan pengembangan teknologi informasi.
2. Konvensi saat ini diperlukan untuk meredam penyalahgunaan sistem, jaringan dan data komputer untuk melakukan perbuatan kriminal. Hal lain yang diperlukan adalah adanya kepastian dalam proses penyelidikan dan penuntutan pada tingkat internasional dan domestik melalui suatu mekanisme kerjasama internasional yang dapat dipercaya dan cepat.
3. saat ini sudah semakin nyata adanya kebutuhan untuk memastikan suatu kesesuaian antara pelaksanaan penegakan hukum dan hak azasi manusia sejalan dengan Konvensi Dewan Eropa untuk Perlindungan Hak Azasi Manusia dan Kovenan Perserikatan Bangsa-Bangsa 1966 tentang Hak Politik Dan sipil yang memberikan perlindungan kebebasan berpendapat seperti hak berekspresi, yang mencakup kebebasan untuk mencari, menerima, dan menyebarkan informasi/pendapat.

Konvensi ini telah disepakati oleh Masyarakat Uni Eropa sebagai konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen Hukum Internasional dalam mengatasi kejahatan *Cyber*, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi.

US Department of Justice (DOJ) menyatakan bahwa konvensi membuat kemajuan di bidang teknologi informasi dengan langkah – langkah diantaranya :

1. mewajibkan negara-negara penandatangan untuk mendirikan substantif tertentu pelanggaran di bidang kejahatan komputer
2. Pihak-pihak yang membutuhkan untuk mengadopsi hukum-hukum prosedural domestik untuk menyelidiki kejahatan komputer
3. memberikan dasar yang kokoh bagi penegakan hukum internasional kerjasama dalam memerangi kejahatan yang dilakukan melalui sistem komputer.

7.2.2 *Cyberlaw Malaysia*

Digital Signature Act 1997 merupakan *Cyber*law pertama yang disahkan oleh parlemen Malaysia. Tujuan *Cyber*law ini, adalah untuk memungkinkan perusahaan dan konsumen untuk

menggunakan tanda tangan elektronik (bukan tanda tangan tulisan tangan) dalam hukum dan transaksi bisnis.

Computer Crimes Act 1997 menyediakan penegakan hukum dengan kerangka hukum yang mencakup akses yang tidak sah dan penggunaan komputer dan informasi dan menyatakan berbagai hukuman untuk pelanggaran yang berbeda komitmen. *Cyber*law berikutnya yang akan berlaku adalah Telemedicine Act 1997. *Cyber*law ini diperuntukan bagi praktisi medis untuk memberdayakan dan memberikan pelayanan medis / konsultasi dari lokasi jauh melalui menggunakan fasilitas komunikasi elektronik seperti konferensi video.

Undang-Undang Komunikasi dan Multimedia 1998 yang mengatur konvergensi komunikasi dan industri multimedia dan untuk mendukung kebijakan nasional ditetapkan untuk tujuan komunikasi dan multimedia industri. Undang-Undang Komunikasi dan Multimedia 1998 kemudian disahkan oleh parlemen untuk membentuk Komisi Komunikasi dan Multimedia Malaysia yang merupakan peraturan dan badan pengawas untuk mengawasi pembangunan dan hal-hal terkait dengan komunikasi dan industri multimedia.

Departemen Energi, Komunikasi dan Multimedia sedang dalam proses penyusunan baru undang-undang tentang Perlindungan Data Pribadi untuk mengatur pengumpulan, kepemilikan, pengolahan dan penggunaan data pribadi oleh organisasi apapun untuk memberikan perlindungan untuk data pribadi seseorang dan dengan demikian melindungi hak-hak privasinya. Undang -undang yang berlaku didasarkan pada sembilan prinsip perlindungan data yaitu :

1. Cara pengumpulan data pribadi
2. Tujuan pengumpulan data pribadi
3. Penggunaan data pribadi
4. Pengungkapan data pribadi
5. Akurasi dari data pribadi
6. Jangka waktu penyimpanan data pribadi
7. Akses ke dan koreksi data pribadi
8. Keamanan data pribadi
9. Informasi yang tersedia secara umum.

7.2.3 *Cyberlaw* Indonesia

Untuk Indonesia, regulasi hukum *Cyber* menjadi bagian penting dalam sistem hukum positif secara keseluruhan. Pemerintah dan Dewan Perwakilan Rakyat perlu segera menuntaskan Rancangan Undang-undang Informasi dan Transaksi Elektronik (RUU ITE) untuk dijadikan hukum positif, mengingat aktivitas penggunaan dan pelanggarannya telah demikian tinggi. Regulasi ini merupakan hal yang sangat ditunggu-tunggu masyarakat demi terciptanya kepastian hukum. RUU ITE sendiri dalam hal materi dan muatannya telah dapat menjawab persoalan kepastian hukum menyangkut tindak pidana carding, hacking dan cracking, dalam sebuah bab tentang perbuatan yang dilarang dimuat ketentuan yang terkait dengan penyalahgunaan teknologi informasi, yang diikuti dengan sanksi pidananya. Demikian juga tindak pidana dalam RUU ITE ini diformulasikan dalam bentuk delik formil, sehingga tanpa adanya laporan kerugian dari korban aparat sudah dapat melakukan tindakan hukum. Hal ini berbeda dengan delik materil yang perlu terlebih dulu adanya unsur kerugian dari korban.

RUU ITE merupakan satu upaya penting dalam setidaknya dua hal:

1. Pengakuan transaksi elektronik dan dokumen elektronik dalam kerangka hukum perikatan dan hukum pembuktian, sehingga kepastian hukum transaksi elektronik dapat terjamin.
2. Diklasifikasikannya tindakan-tindakan yang termasuk kualifikasi pelanggaran hukum terkait penyalahgunaan TI disertai sanksi pidananya termasuk untuk tindakan carding, hacking dan cracking.

Untuk selanjutnya setelah RUU ITE diundangkan, pemerintah perlu pula untuk memulai penyusunan regulasi terkait dengan tindak pidana *Cyber (Cyber Crime),* mengingat masih ada tindak-tindak pidana yang tidak tercakup dalam RUU ITE tetapi dicakup dalam instrumen Hukum Internasional di bidang tindak pidana *Cyber*, misalnya menyangkut tindak pidana pornografi, deufamation, dan perjudian maya. Untuk hal yang terakhir ini perlu untuk mengkaji lebih jauh *Convention on Cyber Crime* 2000, sebagai instrumen tindak pidana *Cyber* internasional, sehingga regulasi yang dibuat akan sejalan dengan kaidah-kaidah internasional, atau lebih jauh akan merupakan implementasi *(implementing legislation*) dari konvensi yang saat ini mendapat perhatian begitu besar dari masyarakat internasional.