RESENSI: “CYBER CRIME (AKAR MASALAH, SOLUSI, DAN PENANGGULANGANNYA)”

Peresensi: M. Jamil¹

Bagian Pertama: Akar Masalah *Cyber Crime*

Adanya penyalahgunaan teknologi informasi yang merugikan kepentingan pihak lain sudah menjadi realitas sosial dalam kehidupan masyarakat moderen sebagai dampak dari pada kemajuan iptek yang tidak dapat dihindarkan lagi bagi bangsa-bangsa yang telah mengenal budaya teknologi (*the culture of technology*). Teknologi telah menjadi bagian yang tidak terpisahkan dari kehidupan umat manusia dalam dunia yang semakin “sempit” ini. Semua ini dapat dipahami, karena teknologi memegang peran amat penting di dalam kemajuan suatu bangsa dan negara di dalam percaturan masyarakat internasional yang saat ini semakin global, kompetitif dan komparatif. Bangsa dan negara yang menguasai teknologi tinggi berarti akan menguasai “dunia”, baik secara ekonomi, politik, budaya, hukum internasional maupun teknologi persenjataan militer untuk pertahanan dan keamanan negara bahkan kebutuhan intelijen. Supaya masalah penyalahgunaan teknologi ini tidak menjadi keresahan sosial bagi masyarakat luas, seyogianya implementasi hukum di dalam kehidupan masyarakat moderen yang memakai teknologi tinggi harus mampu untuk mengurangi perilaku yang dapat merugikan kepentingan bagi orang atau pihak lain, meskipun adanya hak dan kebebasan individu dalam mengekspresikan ilmu atau teknologinya dalam kehidupan sosial yang semakin kompleks. Harus diingat, perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan, sedangkan kejahatan itu telah ada dan muncul sejak permulaan zaman sampai sekarang ini dan masa akan datang yang tidak mungkin untuk diberantas tuntas.

¹ Ketua Umum Pusat Studi Mahasiswa Pascasarjana (PUSMAJA) Mbojo-Yogyakarta Periode 2015-2017 | Ketua II Bagian Eksternal Dewan Pimpinan Cabang Perhimpunan Mahasiswa Hukum Indonesia Daerah Istimewa Yogyakarta (DPC PERMAHI DIY) Periode 2012-2014 | Email: jamilncera@gmail.com | FB/Youtube/IG/Twitter: @MJAMILSH | Website: <http://www.mjamil.my.id>.

Suatu hal yang patut diperhatikan adalah bahwa kejahatan sebagai gejala sosial sampai sekarang belum diperhitungkan dan diakui untuk menjadi suatu tradisi atau budaya yang selalu mengancam dalam setiap saat kehidupan masyarakat. Di sini perlu ada semacam batasan hukum yang tegas di dalam menanggulangi dampak sosial, ekonomi dan hukum dari kemajuan teknologi moderen yang tidak begitu mudah ditangani oleh aparat penegak hukum di negara berkembang seperti halnya Indonesia yang membutuhkan perangkat hukum yang jelas dan tepat dalam mengantisipasi setiap bentuk perkembangan teknologi dari waktu ke waktu. Kemampuan hukum pidana menghadapi perkembangan masyarakat moderen amat dibutuhkan mengingat pendapat Herbert L. Packer “*We live today in a state of hyper-consciousness about the real of fancied breakdown of social control over the most basic threats to person and proverty*”. Artinya, dewasa ini kita hidup dalam suatu negara dengan kecurigaan tinggi seputar kenyataan pengendalian sosial dari khayalan melebihi ancaman paling dasar terhadap orang dan harta benda. Roberto Mangabeira Unger pernah mengemukakan, “*the rule of law is intimately associated with individual freedom, even though it fails to resolve the problem of illegitimate personal dependency in social life*”. Artinya, aturan hukum merupakan lembaga pokok bagi kebebasan individu meskipun ia mengalami kegagalan untuk memecahkan masalah ketergantungan pribadi yang tidak disukai dalam kehidupan sosial. Wajar hukum harus mampu mengantisipasi setiap perkembangan pesat teknologi berikut dampak buruk yang ditimbulkannya, karena amat merugikan.

Penyalahgunaan teknologi informasi ini akan dapat menjadi masalah hukum, khususnya hukum pidana, karena adanya unsur merugikan orang, bangsa dan negara lain. Sarana yang dipakai dalam melakukan aksi kejahatan mayantara ini adalah seperangkat komputer yang memiliki fasilitas internet. Penggunaan teknologi moderen ini dapat dilakukan sendiri oleh hacker atau sekelompok cracker dari rumah atau tempat tertentu tanpa diketahui oleh pihak korban. Kerugian yang dialami korban dapat berupa kerugian moril, materil dan waktu seperti rusaknya data penting, domain *names* atau nama baik, kepentingan negara ataupun transaksi bisnis dari suatu korporasi atau badan hukum (perusahaan)

mengingat kejahatan mayantara atau teknologi informasi ini tidak akan mengenal batas wilayah negara yang jelas. Kejahatan teknologi informasi ini menurut pendapat penulis dapat digolongkan ke dalam supranational criminal law. Artinya, kejahatan yang korbannya adalah masyarakat lebih luas dan besar terdiri dari rakyat suatu negara bahkan beberapa negara sekaligus. Pada Kongres PBB ke X tahun 2000, pengertian atau definisi dari cybercrime dibagi dua, yaitu pengertian sempit, yakni *“any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them”*. Artinya, kejahatan ini merupakan perbuatan bertentangan dengan hukum yang langsung berkaitan dengan sarana elektronik dengan sasaran pada proses data dan sistem keamanan komputer. Di dalam pengertian luas, *cybercrime* didefinisikan sebagai : *“any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network”*. Artinya, perbuatan yang melawan hukum dengan menggunakan sarana atau berkaitan dengan sistem atau jaringan komputer termasuk kejahatan memiliki secara *illegal*, menawarkan atau mendistribusikan informasi melalui sarana sistem atau jaringan komputer. Selain itu, *cybercrime* dapat juga diartikan sebagai *“crime related to technology, computers, and the internet”*. Artinya, kejahatan yang berkaitan dengan teknologi, komputer dan internet.

Dari pengertian di atas memberikan gambaran betapa pengertian dan kriminalisasi terhadap *cybercrime* cukup luas yang dapat menjangkau setiap perbuatan ilegal dengan menggunakan sarana sistem dan jaringan komputer yang dapat merugikan orang lain. Oleh karena itu, supaya jelas dalam kriminalisasi terhadap cybercrime harus dibedakan antara harmonisasi materi/substansi yang dinamakan dengan tindak pidana atau kejahatan mayantara dengan harmonisasi kebijakan formulasi kejahatan tersebut. Perbedaan ini penting untuk menentukan, apakah jenis kejahatan ini akan berada di dalam atau di luar ketentuan Kitab Undang-undang Hukum Pidana (KUHP) ataupun undang-undang pidana khusus yang membutuhkan kerangka hukum baru untuk diberlakukan secara nasional. Saat ini telah ada konsep KUHP Baru yang dapat menambahkan pasal-pasal

sanksi ancaman terhadap pelaku dari kejahatan mayantara dan RUU tentang Teknologi Informasi antara lain mengatur soal yurisdiksi dan kewenangan pengadilan (Bab VIII), penyidikan (Bab X) dan ketentuan pidana (Bab XI). Pemberlakuan undang-undang ini tidak hanya untuk *ius constitutum* sebagai hukum positif, yakni hukum yang diberlakukan saat ini akan tetapi juga *ius constituendum* atau hukum masa depan.

Bagian Kedua: Tinjauan Teoritis Cyber Crime Dalam Perspektif Hukum Positif

Untuk memahami kejahatan dunia maya (*cyber crime*) perlu memahami internet. Internet adalah suatu jaringan komunikasi digital yang menghubungkan lebih dari 25.000 (dua puluh lima ribu) jaringan dari hampir seluruh Negara di dunia Berdasarkan catatan dari *National Criminal Intellengence Services* (NCIS) di Inggris terdapat 13 macam bentuk-bentuk cybercrime.

Pertama, *Recreational Hackers*, kejahatan ini dilakukan oleh netter tingkat pemula untuk iseng-iseng mencoba kekurangandalan dari sistem sekuritas atau keamanan data suatu perusahaan. lain.

Kedua, *Crackers* atau *Criminal Minded Hackers*, yaitu pelaku kejahatan ini biasanya memiliki motivasi untuk mendapatkan keuntungan finansial, sabotase, dan penghancuran data pihak korban. Ketiga, *Political Hackers*, yakni aktivis politik atau *hactivist* melakukan perusakan terhadap ratusan situs web untuk mengkampanyekan program-program tertentu bahkan tidak jarang digunakan untuk menempelkan pesan untuk mendiskreditkan lawan politiknya. Keempat, *Denial of Service Attack*. Serangan tujuan ini adalah untuk memacetkan sistem dengan mengganggu akses dari pengguna jasa internet yang sah. Kelima, *Insiders (Internal) Hackers* yang biasanya dilakukan oleh orang dalam perusahaan sendiri. Modus operandinya adalah karyawan yang kecewa atau bermasalah dengan pimpinan korporasi dengan merusak data atau akses data dalam transaksi bisnis. Keenam, *viruses*. Program pengganggu (*malicious*) perangkat lunak dengan melakukan penyebaran virus yang dapat menular melalui aplikasi internet, ketika akan diakses oleh pemakai. Ketujuh, *piracy*. Pembajakan software atau

perangkat lunak komputer merupakan trend atau kecenderungan yang terjadi dewasa ini, karena dianggap lebih mudah dan murah untuk dilakukan para pembajak dengan meraup keuntungan berlipat ganda. Kedelapan, fraud adalah sejenis manipulasi informasi keuangan dengan tujuan untuk mengeruk keuntungan sebesar-besarnya. Kesepuluh, pornography and paedophilia. Perkembangan dunia maya selain mendatangkan berbagai kemaslahatan bagi umat manusia dengan mengatasi kendala ruang dan waktu, juga telah melahirkan dampak negatif berupa “dunia pornografi” yang mengkhawatirkan berbagai kalangan terhadap nilai-nilai etika, moral dan estetika. Kesebelas, *cyber stalking* adalah segala bentuk kiriman e-mail yang tidak dikehendaki oleh user atau junk e-mail yang sering memakai folder serta tidak jarang dengan pemaksaan..

Duabelas, hate sites. Situs ini sering digunakan oleh hackers untuk saling menyerang dan melontarkan komentar-komentar yang tidak sopan dan vulgar yang dikelola oleh para “ekstrimis” untuk menyerang pihak-pihak yang tidak disenanginya. Ketigabelas, *criminal communications*. NCIS telah mendeteksi bahwa internet dijadikan sebagai alat yang andal dan moderen untuk melakukan kegiatan komunikasi antar gangster, anggota sindikat obat bius dan bahkan komunikasi antar “hooligan” di dunia sepakbola Inggris.

Merujuk pada sistematika Draft *Convention on Cybercrime* dari Dewan Eropa (Council of Europe) yaitu Draft No. 25, Desember 2000 dimana konvensi ini ditandatangani oleh 30 negara pada bulan November 2001 di Budapest, Bulgaria, maka Barda Nanawi Arief memberikan kategori *cybercrime* sebagai delik dalam empat hal sebagai berikut. Pertama, delik-delik terhadap kerahasiaan, integritas, dan ketersediaan data dan sistem komputer termasuk di dalamnya (a) mengakses sistem komputer tanpa hak (illegal acces), (b) tanpa hak menangkap/mendengar pengiriman dan pemancaran (illegal interception), (c) tanpa hak merusak data (data interference), (d) tanpa hak mengganggu sistem (*system interference*), (e) menyalahgunakan perlengkapan (*misuse of devices*). Kedua, delik-delik yang berhubungan dengan komputer berupa pemalsuan dan penipuan dengan komputer (*computer related offences : forgery and fraud*). Ketiga, delik-delik yang bermuatan tentang pornografi anak (*content-related*

offences, child pornography). Keempat, delik-delik yang berhubungan dengan masalah hak cipta (*offences related to infringements of copyright*).

Sementara Mardjono Reksodiputro dengan mengutip pendapat Eric J. Sinrod dan William P. Reilly melihat kebijakan formulasi *cybercrime* dapat dilakukan dalam dua pendekatan. Pertama, menganggapnya sebagai kejahatan biasa (*ordinary crime*) yang dilakukan dengan pemakaian teknologi tinggi (*high-tech*) dan KUHP dapat dipergunakan untuk menanggulanginya dengan penambahan pasal tertentu dalam konsep RUU KUHP Baru. Kedua, menganggapnya sebagai kejahatan baru (*new category of crime*) yang amat membutuhkan suatu kerangka hukum baru (*new legal framework*) dan komprehensif untuk mengatasi sifat khusus teknologi yang sedang berkembang dan tantangan baru yang tidak ada pada kejahatan biasa (misalnya masalah yurisdiksi) dan karena itu perlu diatur secara tersendiri di luar KUHP.

Kendati ketentuan dalam KUHP belum bisa menjangkau atau memidana para pelaku kejahatan ini dengan tepat dan undang-undang teknologi informasi belum ada yang dapat mengatur masalah penyalahgunaan teknologi, akan tetapi kejahatan mayantara harus tetap menjadi prioritas utama penegak hukum kepolisian untuk menanggulanginya. Dampak buruk teknologi menjadi masalah serius bagi umat manusia pada masa depan, apabila disalahgunakan oleh orang-orang yang tidak bertanggungjawab dengan maksud untuk menarik keuntungan ataupun mengacaukan data penting pihak lain bahkan negara bisa menjadi korbannya.

Keadaan ini tidak dapat dihindarkan mengingat salah satu ciri dari masyarakat moderen adalah kecenderungan untuk menggunakan teknologi dalam segenap aspek kehidupannya. Perkembangan teknologi digital tidak dapat dihentikan oleh siapa pun sebagai wujud dari hasil kebudayaan. Di sini menjadi tugas dari pihak pemerintah, penegak hukum kepolisian dan warga masyarakat untuk mampu mengantisipasi setiap bentuk kemajuan teknologi digital yang pesat sehingga dampak buruk perkembangan yang merugikan dapat ditanggulangi lebih dini. Munculnya revolusi teknologi informasi dewasa ini dan masa depan tidak hanya membawa dampak pada perkembangan teknologi itu sendiri, akan tetapi

juga akan mempengaruhi aspek kehidupan lain seperti agama, kebudayaan, sosial, politik, kehidupan pribadi, masyarakat bahkan bangsa dan negara. Jaringan informasi global atau internet saat ini telah menjadi salah satu sarana untuk melakukan kejahatan baik domestik maupun internasional. Internet menjadi medium bagi pelaku kejahatan untuk melakukan kejahatan dengan sifatnya yang mondial, internasional dan melampaui batas ataupun kedaulatan suatu negara. Semua ini menjadi motif dan modus operandi yang amat menarik bagi para penjahat digital.

Manifestasi kejahatan mayantara yang terjadi selama ini dapat muncul dalam berbagai macam bentuk atau varian yang amat merugikan bagi kehidupan masyarakat ataupun kepentingan suatu bangsa dan negara pada hubungan internasional. Kejahatan mayantara dewasa ini mengalami perkembangan pesat tanpa mengenal batas wilayah negara lagi (*borderless state*), karena kemajuan teknologi yang digunakan para pelaku cukup canggih dalam aksi kejahatannya. Para hacker dan cracker bisa melakukannya lewat lintas negara (*cross boundaries countries*) bahkan di negara-negara berkembang (*developing countries*) aparat penegak hukum, khususnya kepolisian tidak mampu untuk menangkal dan menanggulangi disebabkan keterbatasan sumber daya manusia, sarana dan prasarana teknologi yang dimiliki.

Meskipun hukum pidana merupakan sarana terakhir (*ultimum remedium*), tetapi hukum pidana bukanlah alat yang cukup ampuh untuk menanggulangi kejahatan mayantara karena penanggulangan kejahatan dengan hukum pidana hanya pengobatan simptomatik sehingga dibutuhkan sarana lain yang bersifat non penal. Sarana non penal ini dapat dilakukan melalui saluran teknologi (*techno-prevention*) pada pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan itu sendiri yang dapat digunakan manusia, baik untuk tujuan baik maupun jahat. Pendekatan budaya ini dilakukan untuk membangun atau membangkitkan kepekaan tinggi warga masyarakat dan aparat penegak hukum terhadap setiap masalah cybercrime dan menyebarluaskan atau mengajarkan etika penggunaan komputer yang baik melalui media pendidikan. Pentingnya pendekatan ini adalah dalam upaya mengembangkan kode etik dan perilaku (*code*

of behaviour and ethics) dalam pemakaian teknologi internet. Pendekatan non penal ini diharapkan dapat mengurangi pelanggaran hukum yang menggunakan sarana teknologi sebagai bentuk pencegahan kejahatan.

Bagian Ketiga: Problematika Cyber Crime, Solusi, dan Penangannya

A. Kebijakan Non-Penal Instansi Pemerintah dalam Penanggungan Cyber Crime

Thomas L. Friedman seorang columnist asing *The New York Times* dalam bukunya ”*World is Flat: A Brief History of the Twenty-first Century*” menggambarkan bagaimana peradaban dunia saat ini. Friedman menggambarkan bahwa globalisasi merupakan hal yang tidak bisa di tolak lagi oleh setiap bangsa. Friedman memaparkan tiap tahapan-tahapan globalisasi secara rinci. Globalisasi menurut Friedman terjadi pada hampir di seluruh negara di dunia. Globalisasi yang dijabarkan termasuk didalamnya juga pengaruh besar teknologi informasi dalam aktifitas manusia . Perkembangan teknologi informasi yang terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara (*borderless*). Negara yang sudah mempunyai infrastruktur jaringan informasi yang lebih memadai tentu telah menikmati hasil pengembangan teknologi informasinya, negara yang sedang berkembang dalam pengembangannya akan merasakan kecenderungan timbulnya neo-kolonialisme . Hal tersebut menunjukan adanya pergeseran paradigma dimana jaringan informasi merupakan infrastruktur bagi perkembangan suatu negara. Tanpa penguasaan dan pemahaman akan teknologi informasi ini, tantangan globalisasi akan menyebabkan ketergantungan yang tinggi terhadap pihak lain dan hilangnya kesempatan untuk bersaing karena minimnya pemanfaatan teknologi informasi. Disadari betul bahwa perkembangan teknologi informasi yang berwujud internet, telah mengubah pola interaksi masyarakat, seperti interaksi bisnis, ekonomi, sosial, dan budaya. Internet telah memberikan kontribusi yang demikian besar bagi masyarakat, perusahaan / industri maupun pemerintah. Hadirnya Internet telah menunjang efektifitas dan efisiensi operasional setiap aktifitas manusia. Upaya yang sedang dilakukan pemerintah saat ini dalam rangka menyusun

payung hukum ruang cyber melalui usulan Rancangan Undang-undang Informasi dan Transaksi Elektronik (RUU ITE) memang patut dihargai. Rancangan Undang-undang Informasi dan Transaksi Elektronik memuat beberapa hal yakni; masalah yurisdiksi, perlindungan hak pribadi, azas perdagangan secara e-commerce, azas persaingan usaha usaha tidak sehat dan perlindungan konsumen, azas-azas hak atas kekayaan intelektual (HaKI) dan hukum Internasional serta azas *Cyber Crime*. Kendati Rancangan Undang-undang Informasi dan Transaksi Elektronik telah diusulkan dan di bahas oleh Pemerintah (melalui Depkominfo) dan DPR, namun hasil riil berupa disahkannya RUU tersebut menjadi Undang-undang belum tercapai. Menurut pemerintah, masih ada beberapa Daftar Inventaris Masalah (DIM) yang perlu dilakukan pembahasan lagi. Usaha yang dilakukan di atas adalah melalui regulasi undang-undang dengan menggunakan sarana penal, yakni memperluas pengaturan cyberspace dalam Konsep KUHP Baru dan membuat suatu RUU Teknologi Informasi dan RUU Telematika yang berkaitan dengan kegiatan di cyberspace. Akan tetapi yang perlu diperhatikan adalah pengkajian lebih intensif terhadap masalah yang hendak dikriminalisasikan sebagai upaya penanggulangan kejahatan mayantara. Persyaratan pokok adalah kerugian korban yang signifikan dengan perbuatan pelaku. Ketentuan pidana harus dapat dioperasionalkan dan keyakinan bahwa tidak ada sarana lain yang betul-betul dapat mengatasinya.

Meskipun hukum pidana merupakan sarana terakhir (ultimum remedium), tetapi hukum pidana bukanlah alat yang cukup ampuh untuk menanggulangi kejahatan mayantara karena penanggulangan kejahatan dengan hukum pidana hanya pengobatan simptomatik sehingga dibutuhkan sarana lain yang bersifat non penal. Sarana non penal ini dapat dilakukan melalui saluran teknologi (techno-prevention) pada pendekatan budaya, karena teknologi merupakan hasil dari kebudayaan itu sendiri yang dapat digunakan manusia, baik untuk tujuan baik maupun jahat. Pendekatan budaya ini dilakukan untuk membangun atau membangkitkan kepekaan tinggi warga masyarakat dan aparat penegak hukum terhadap setiap masalah cybercrime dan menyebarluaskan atau mengajarkan etika penggunaan komputer yang baik melalui media pendidikan.

Pentingnya pendekatan ini adalah dalam upaya mengembangkan kode etik dan perilaku (*code of behaviour and ethics*) dalam pemakaian teknologi internet. Pendekatan non penal ini diharapkan dapat mengurangi pelanggaran hukum yang menggunakan sarana teknologi sebagai bentuk pencegahan kejahatan.

Kritisi Resensi Buku Cyber Crime Melalui Perspektif Filsafat Hukum

Perkembangan teknologi informasi termasuk internet di dalamnya juga memberikan tantangan tersendiri bagi perkembangan hukum di Indonesia. Hukum di Indonesia diuntut untuk dapat menyesuaikan dengan perubahan sosial yang terjadi. Soerjono Soekanto mengemukakan bahwa perubahan-perubahan sosial dan perubahan hukum atau sebaliknya tidak selalu berlangsung bersama-sama. Artinya pada keadaan tertentu perkembangan hukum mungkin tertinggal oleh perkembangan unsur-unsur lainnya dari masyarakat serta kebudahaannya atau mungkin hal yang sebaliknya.

Penulis berpendapat bahwa perkembangan teknologi informasi yang begitu cepat menimbulkan akibat yang menguntungkan dan akibat yang merugikan bagi masyarakat. Menguntungkan masyarakat karena antara lain komunikasi yang mudah dengan menggunakan informasi elektronik. Merugikan karena hukum terkait belum cukup mampu memfungsikan dirinya sebagai sarana ketertiban.

Pesatnya perkembangan di bidang teknologi informasi saat ini merupakan dampak dari semakin kompleksnya kebutuhan manusia akan informasi itu sendiri. Dekatnya hubungan antara informasi dan teknologi jaringan komunikasi telah menghasilkan dunia maya yang amat luas yang biasa disebut dengan teknologi *cyberspace*. Teknologi ini berisikan kumpulan informasi yang dapat diakses oleh semua orang dalam bentuk jaringan-jaringan komputer yang disebut jaringan internet.

Disinilah tampak jelas bahwa hukum di Indonesia masih tertinggal (bahkan tertinggal jauh) dengan perubahan yang ada di masyarakat. Hukum di Indonesia belum mengenal istilah internet, carding, e-commerce atau istilah

lainnya di bidang Teknologi Informasi. Dengan kata lain *cyber law* di Indonesia belum benar-benar terwujud seperti yang diharapkan masyarakat.

Cyber law mungkin dapat diklasifikasikan sebagai rejim hukum tersendiri, karena memiliki multi aspek; seperti aspek pidana, perdata, internasional, administrasi, dan aspek Hak Kekayaan Intelektual.

Penulis mendefinisikan *cyber law* atau kata lain dari cyberspace law sebagai aspek hukum yang berkaitan dengan penggunaan teknologi informasi pada ruang maya (*cyber space*). Guru Besar Fakultas Hukum Universitas Diponegoro Barda Nawawi Arief menyebut istilah cyber dengan ”mayantara”. Berbeda dengan Barda Nawawi Arief, Edmon Makarim dari Lembaga Kajian Hukum dan Teknologi Universitas Indonesia enggan menyebut *cyber law* dengan kata maya. Karena menurut Edmon Makarim, istilah maya lebih tepat diartikan sebagai bias, bukan *cyber*. Namun apapun istilahnya, sampai saat ini belum ada satupun regulasi di Indonesia yang menyebut atau mendefinisikan istilah *cyber* atau mayantara. Karena pada dasarnya istilah *cyber* di Indonesia saat ini bukan merupakan istilah hukum.

Menurut pandangan penulis ada beberapa ruang lingkup cyberlaw yang memerlukan perhatian serius di Indonesia saat ini yakni;

1. Kriminalisasi *Cyber Crime* atau kejahatan di dunia maya. Dampak negatif dari kejahatan di dunia maya ini telah banyak terjadi di Indonesia. Namun karena perangkat aturan yang ada saat ini masih belum cukup kuat menjerat pelaku dengan sanksi tegas, kejahatan ini semakin berkembang seiring perkembangan teknologi informasi. Kejahatan sebenarnya tumbuh dan berkembang dalam masyarakat, tidak ada kejahatan tanpa masyarakat. Benar yang diucapkan Lacassagne bahwa masyarakat mempunyai penjahat sesuai dengan jasanya . Betapapun kita mengetahui banyak tentang berbagai faktor kejahatan yang ada dalam masyarakat, namun yang pasti adalah bahwa kejahatan merupakan salah satu bentuk perilaku manusia yang terus mengalami perkembangan sejajar dengan perkembangan masyarakat itu sendiri.

2. Aspek Pembuktian. Saat ini sistem pembuktian hukum di Indonesia (khususnya dalam pasal 184 KUHP) belum mengenal istilah bukti elektronik/digital (*digital evidence*) sebagai bukti yang sah menurut undang-undang. Masih banyak perdebatan khususnya antara akademisi dan praktisi mengenai hal ini. Untuk aspek perdata, pada dasarnya hakim dapat bahkan dituntun untuk melakukan *rechtsvinding* (penemuan hukum). Tapi untuk aspek pidana tidak demikian. Asas legalitas menetapkan bahwa tidak ada suatu perbuatan dapat dipidana jika tidak ada aturan hukum yang mengaturnya (*nullum delictum nulla poena sine previa lege poenali*). Untuk itulah dibutuhkan adanya dalil yang cukup kuat sehingga perdebatan akademisi dan praktisi mengenai hal ini tidak perlu terjadi lagi.
3. Aspek Hak Atas Kekayaan Intelektual di *cyber space*, termasuk didalamnya hak Cipta dan Hak Milik Industrial yang mencakup paten, merek, desain industri, rahasia dagang, sirkuit terpadu, dan lain-lain.
4. Standardisasi di bidang telematika. Penetapan standardisasi bidang telematika akan membantu masyarakat untuk mendapatkan keamanan dan kenyamanan dalam menggunakan teknologi informasi.
5. Aturan-aturan di bidang E-Business termasuk didalamnya perlindungan konsumen dan pelaku bisnis.
6. Aturan-aturan di bidang E-Government. Apabila E-Government di Indonesia telah terintegrasi dengan baik, maka efeknya adalah pelayanan kepada masyarakat menjadi lebih baik.
7. Aturan tentang jaminan keamanan dan kerahasiaan Informasi dalam menggunakan teknologi informasi.
8. Yurisdiksi hukum, cyberlaw tidak akan berhasil jika aspek ini diabaikan. Karena pemetaan yang mengatur *cyber space* menyangkut juga hubungan antar kawasan, antar wilayah, dan antar negara. Sehingga penetapan yurisdiksi yang jelas mutlak diperlukan.

Indonesia masih tertinggal jauh jika dibandingkan dengan Negara-negara Asia lainnya apalagi jika dibandingkan dengan negara-negara Uni Eropa yang telah memiliki perangkat hukum lengkap di bidang *cyber law*. Ketiadaan

perangkat hukum di bidang cyberlaw di Indonesia mengakibatkan terjadinya kesenjangan hukum di masyarakat. Namun demikian Satjipto Rahardjo berpendapat bahwa apabila timbul kesenjangan antara hukum dengan perubahan dalam masyarakat, maka kesenjangan itu termasuk hal yang normal. Karena hukum sebetulnya sudah diperlengkapi dengan peralatan teknik untuk bisa mengatasi kesenjangan tersebut. Dalam keadaan demikian hukum tidak selalu harus di ubah secara tegas. Namun dapat dilakukan adaptasi hukum terhadap perubahan masyarakat .

Untuk membangun pijakan hukum yang kuat dalam mengatur masalah-masalah hukum di ruang *cyber* (internet) diperlukan komitmen kuat pemerintah dan DPR. Namun yang lebih penting lagi selain komitmen adalah bahwa aturan yang dibuat nantinya merupakan produk hukum yang adaptable terhadap berbagai perubahan khususnya di bidang teknologi informasi. Kunci dari keberhasilan pengaturan cyberlaw adalah riset yang komprehensif yang mampu melihat masalah *cyber space* dari aspek konvergensi hukum dan teknologi. Kongkretnya pemerintah dapat membuat laboratorium dan pusat studi *cyber law* di perguruan-perguruan tinggi dan instansi-instansi pemerintah yang dianggap capable di bidang tersebut. Laboratorium dan pusat studi *cyber law* kemudian bekerjasama dengan Badan Litbang Instansi atau Perguruan Tinggi membuat riset komprehensif tentang cyberlaw dan teknologi informasi. Riset ini tentu saja harus mengkombinasikan para ahli hukum dan ahli teknologi informasi. Hasil dari riset inilah yang kemudian dijadikan masukan dalam menyusun produk-produk cyberlaw yang berkualitas selain tentunya masukan dari pihak-pihak lain seperti swasta, masyarakat, dan komunitas *cyber*. Selain hal tersebut hal paling penting lainnya adalah peningkatan kemampuan SDM aparatur hukum di bidang Teknologi Informasi mulai dari polisi, jaksa, hakim bahkan advokat khususnya yang menangani masalah-masalah ini. Penegakan hukum di bidang *cyber law* mustahil bisa terlaksana dengan baik tanpa didukung SDM aparatur yang berkualitas dan ahli di bidangnya.

Perkembangan teknologi informasi terjadi pada hampir setiap negara sudah merupakan ciri global yang mengakibatkan hilangnya batas-batas negara

“RESENSI: Cyber Crime (Akar Masalah, Solusi, dan Penanggulangannya)”

(*borderless*). Negara yang sudah mempunyai infrastruktur jaringan. Pihak kepolisian Indonesia telah membentuk suatu unit penanggulangan kejahatan mayantara dengan nama Cybercrime Unit yang berada di bawah kendali Direktorat Reserse Kriminal Polri. Pembentukan unit kepolisian ini patut dipuji, namun amat disayangkan apabila unit ini bekerja tidak dilengkapi dengan perangkat legislasi anti cybercrime. Model yang digunakan adalah Umbrella Provision atau “undang-undang payung”, artinya ketentuan *cybercrime* tidak dibuat dalam bentuk perundang-undangan tersendiri (khusus), akan tetapi diatur secara umum dalam RUU Teknologi Informasi dan RUU Telematika.

Judul Buku : CYBER CRIME (Akar Masalah, Solusi, dan Penanggulangannya)

Penulis : Ach. Tahir

Penerbit : SUKA-Press

Tahun Terbit: April 2010

Peresensi : **M. Jamil, S.H. ***

* Ketua Umum Pusat Studi Mahasiswa Pascasarjana (PUSMAJA) Mbojo-Yogyakarta Periode 2015-2017 | Ketua II Bagian Eksternal Dewan Pimpinan Cabang Perhimpunan Mahasiswa Hukum Indonesia Daerah Istimewa Yogyakarta (DPC PERMAHI DIY) Periode 2012-2014 | Ketua Ikatan Keluarga Alumni Prodi Ilmu Hukum Fakultas Syariah dan Hukum UIN SunanKalijaga Yogyakarta (IKASUKA Ilmu Hukum) Periode 2018-2023.

Ful Sumber Tulisan:

M. Jamil, “RESENSI: Cyber Crime (Akar Masalah, Solusi, dan Penanggulangannya)”, dimuat di <http://ikasukaih.uin-suka.ac.id/id/kolom/detail/171/resensi-cyber-crime-akar-masalah-solusi-dan-penanggulangannya>, pada 15 April 2010.