ETIKA SIBER DAN SIGNIFIKANSI MORAL DUNIA MAYA

CYBER ETHICS AND MORAL SIGNIFICATION IN CYBERSPACE

Ahmad Rudy Fardiyan[1]

Abstract

Internet usage has been necessity and helpfull in daily modern activities. However, the benefits of using internet is equal to the risk of it own. The world of cyber created by internet, is borderless. This, allow the citizen of cyber (netizen) to do eithergoodthings or badthings that can not or impossible to achieve in the real world. Many cases in these terms across countries make this type of crime become more complex to anticipates. The differences of law and attention between countries about this phenomena, make it even worse. At this point, the moral become significant to control "life" in cyberspace. The unique characteristic of cyberworld doesn't change the view of values, ethics, and etiquette of life within. Cyberethics as a part of ethic studies, proposes guidelines of values so the opportunity and advantages that provided by internet can be use for good purpose on human being.

Keywords : Moral, Cyberethic, Cyberspace

I. PENDAHULUAN

Peradaban masyarakat modern seiring perkembangan ilmu pengetahuan dan teknologi telah menimbulkan persoalan baru tentang nilai. Jika melihat kondisi etis masyarakat modern, menurut Bertens (2011) ada tiga ciri yang menonjol. Pertama, adanya *pluralisme moral*. Hal ini dirasakan karena perkembangan teknologi komunikasi dan informasi menjadikan dunia ini seperti tidak mengenal lagi batas-batas yang konkret, baik dalam geografis maupun kebudayaan. Campur-aduknya manusia (yang secara geografis dan budaya terpisah jauh) ke dalam satu wadah yang bernama internet telah membuat kita berhadap-hadapan langsung dengan kemajemukan. Kemajemukan ini membawa pula nilai-nilai dan norma-norma yang menyangkut praktik bisnis, seksualitas, gaya hidup, atau perkawinan.

Ciri kedua yang menandai situasi etis di zaman modern adalah *munculnya persoalan etis baru* yang disebabkan perkembangan ilmu pengetahuan dan teknologi. Persoalan tentang hal ini misalnya tentang biomedis, terkait dengan manipulasi genetik; reproduksi artifisial, donor rahim, kloning, dan sebagainya. Persoalan lain misalnya tentang privasi atau *hacking* virus komputer. Ciri ketiga adalah *munculnya kepedulian etis* di seluruh dunia. Globalisasi juga berarti adanya gejala di bidang moral dimana gerakan kesadaran moral universal, baik yang terorganisasi maupun tidak, mulai bermunculan. Salah satunya adalah Deklarasi Universal tentang Hak-hak Asasi Manusia oleh PBB pada tahun 1948. (Bertens, 2011: 32-36).

[1]Dosen Program Studi Ilmu Komunikasi, FISIP Universitas Lampung;ahmad.rudy@unila.ac.id

Sebagai salah satu hasil perkembangan teknologi informasi, internet (*interconnected networking*) kini telah menjadi kebutuhan dasar masyarakat modern, terutama yang tinggal di daerah perkotaan. Bermacam-macam aktivitas yang dilakukan orang-orang di internet, membaca berita, menelusuri dokumen, bersosialisasi, saling tukar informasi data, hingga berdagang. Internet telah menjadi "dunia" yang baru, dimana di dalamnya terdapat "kehidupan" manusia dengan segala aktivitasnya.

Selain memberi keuntungan dalam akses dan transaksi informasi, internet juga dimanfaatkan untuk mendapatkan keuntungan pribadi dengan merugikan pihak lain. Sejumlah kasus seperti perdagangan senjata ilegal, *human trafficking*, pencurian data, pembobolan rekening, dan lain sebagainya, telah meresahkan siapa saja yang aktif menggunakan internet. Bentuk kejahatan ini biasa disebut kejahatan internet (*cyber crime*). Korban dari kejahatan internet ini tidak hanya individu, namun juga instansi, bahkan negara. Pada tahun 1999 seorang *hacker* berhasil menembus portal kemanan pada situs Kementrian Keuangan Rumania. *Hacker* asing tersebut mengganti nilai kurs mata uang Rumania sehingga banyak pembayar pajak *online* yang terkecoh dengan besaran nilai yang telah diganti tersebut. Akibat serangan ini pemerintah Rumania mengalami kerugian yang sangat besar[2]. Kasus ini tidak berlanjut ke ranah hukum karena tidak ada aturan tertulis yang mengatur tentang tindak kejahatan antar wilayah negara. Meskipun pada tanggal 4 Desember 2000 Sidang Umum Perserikatan Bangsa-Bangsa (PBB) telah menandatangai Resolusi PBB 55/63 untuk memerangi penyalahgunaan teknologi komunikasi dan informasi, namun perbedaan penafsiran tentang jenis kejahatan dan perbedaan kemampuan dari setiap negara dalam tata kelola internet di negaranya masing-masing, membuat kejahatan telematika masih terus menjadi momok yang menghantui setiap pengguna internet aktif.

Atas dasar inilah pembicaraan mengenai etika kembali mendesak dilakukan. Pembicaraan ini bukan hanya untuk merumuskan kembali sistem hukum yang tepat dan ampuh untuk mengatasi persoalan kejahatan ini secara retrospektif dan prospektif, tetapi juga untuk membangun kesadaran dalam memanfaatkan teknologi internet ini dengan cara yang bermoral dan bermartabat. Sekiranya telah ada kesadaran bahwa untuk menciptakan ketertiban dan kenyamanan, selain menempuh cara-cara represif (dengan menetapkan undang-undang dan aturan legal) juga dibutuhkan "pendisiplinan" melalui pengetahuan moral atau etika yang ditanamkan secara berkelanjutan. Etika yang secara khusus diterapkan dalam konteks penggunaan internet ini biasa dikenal sebagai etika internet atau etika siber (*cyberethics*).

II. PEMBAHASAN

Kata "moral" memiliki etimologi yang sama dengan "etika", hanya asal katanya yang berbeda. Oleh karena itu, berbicara tentang etika sama halnya berbicara tentang moral. Sedangkan kata "etis" merupakan bentuk kata sifat dari "etika". Selain itu, persoalan yang menyangkut etika seringkali dicampur maknanya dengan persoalan tentang "etiket". Padahal keduanya punya perbedaan yang mendasar. Perbedaan tersebut bisa dijelaskan sebagai berikut: 1) *etiket menyangkut cara suatu perbuatan harus dilakukan, sedangkan etika memberi norma tentang perbuatan tersebut*. Misalnya, untuk memberi sesuatu kepada orang lain, kita sebaiknya menggunakan tangan kanan. Namun, menyangkut etika, apakah mencuri itu sebaiknya menggunakan tangan kanan atau kiri? Etiket adalah cara suatu perbuatan

[2] "Hackers Alter Romanian Money Rate", New York Times on the web/ Breaking News from Associated Press, November 3, 1999, reported at_http://www.nytimes.com/aponline/i/AP-Romania-Hackers.html_.

dilakukan, sedangkan etika menyangkut perbuatan itu sendiri; 2) *etiket hanya berlaku di dalam pergaulan, yang berarti selalu melibatkan orang lain. Sedangkan etika tetap berlaku meskipun tidak ada saksi mata*; 3) *etiket bersifat lebih relatif sedangkan etika bersifat lebih absolut*. Meskipun etika juga mempunyai relativitas, namun tingkatannya tidak setinggi relativitas pada etiket; 4) *etiket hanya memandang manusia dari segi lahiriahnya saja, sedangkan etika menyangkut manusia dari segi dalam* (Bertens, 2011: 10-11).

Etika secara umum membahas sejumlah tema yaitu hati nurani, nilai dan norma, kebebasan dan tanggung jawab, serta hak dan kewajiban. Hati nurani merupakan "instansi" dalam diri manusia yang memberi penilaian moralitas terhadap tingkah lakunya. Hati nurani tidak membahas tentang situasi yang umum, melainkan tentang situasi yang konkret. Bisa dibilang, hati nurani merupakan kesadaran moral manusia, sehingga ia bisa merefleksi dan membimbing perbuatan-perbuatan manusia dalam bidang moral. Nilai memiliki beberapa karakteristik, yaitu: kehadiran subjek (yang menilai), tampil dalam konteks praktis (adanya kepentingan subjek), nilai menyangkut sifat yang ditambah oleh subjek terhadap objek. Sedangkan norma adalah kaidah yang digunakan manusia untuk menilai sesuatu.

Kebebasan (bebas) bukanlah hal yang mudah untuk didefinisikan, karena ia mempunyai banyak aspek dan karakteristik, sehingga "bebas" menjadi sebuah realitas yang kompleks. Namun pada prinsipnya kebebasan dapat dibedakan antara kebebasan sosial-politik dan kebebasan individual. Kebebasan sosial-politik mencakup kebebasan kolektif. Di sini, yang menjadi subjeknya adalah bangsa atau rakyat. Secara sederhana, dapat diterjemahkan bahwa kebebasan sosial-politik merupakan bentuk kedaulatan rakyat terhadap kekuasaan absolut (penguasa otoriter, raja) maupun kekuasaan imperialis (kolonialisme). Sedangkan kebebasan individual menempati posisi yang lebih umum dan penting. Di sini yang menjadi subjeknya adalah manusia perorangan. Beberapa bentuk kebebasan individual yaitu kesewenang-wenangan, kebebasan fisik, kebebasan yuridis, kebebasan psikologis (*free will*), kebebasan moral, dan kebebasan eksistensial (Bertens, 2011: 107-123).Secara umum, kebebasan lebih mudah dipahami sebagai kebebasan negatif. Yaitu kebebasan dengan pengertian "bebas dari...". Dari aspek ini, kebebasan bisa dimengerti sebagai bebas dari paksaan fisik, perampasan hak-hak, tekanan bathin, paksaan moral, serta keterasingan (alienasi) atau inotentisitas. Namun yang lebih sulit adalah memahami kebebasan dalam aspek positifnya, yang dimengerti sebagai "bebas untuk..." Dalam hal ini maka dapat dikatakan bahwa kebebasan mempunyai batasan. Batasan kebebasan yaitu faktor dari dalam (*nature* dan *nurture*), lingkungan (geografis dan sosial), kebebasan orang lain, dan generasi yang akan datang.

Tanggung jawab selalu mengandaikan kebebasan karena disana ada tindakan bebas yang dilakukan, maka perlu ada 'jawaban' atas apa yang dilakukannya itu. Bisa dikatakan bahwa tindakan yang dilakukan secara bebas adalah penyebab. Orang bertanggung jawab atas sesuatu yang disebabkan olehnya. Ada dua jenis tanggung jawab, yaitu tanggung jawab prospektif dan tanggung jawab retrospektif. *Tanggung jawab prospektif* merupakan tanggung jawab atas apa-apa yang belum dan mungkin akan terjadi. Sedangkan *tanggung jawab retrospektif* adalah tanggung jawab atas apa-apa yang sudah terjadi (konsekuensi).

Hak adalah klaim yang dapat dibenarkan atau klaim yang sah. Karena itu, hak mempunyai korelasi dengan kewajiban, dimana hak seseorang atas orang lain merupakan kewajiban bagi orang lain tersebut. Meski demikian, ada perbedaan antara hak dengan kewajiban menyangkut pihak yang terlibat. Tidak ada hak untuk diri sendiri. Hak selalu mengandung hubungan dengan orang lain. Namun kewajiban berkaitan, baik terhadap orang lain maupun diri sendiri. Kewajiban terhadap diri sendiri ini juga dapat dimengerti sebagai

kewajiban terhadap Tuhan. Hal ini sesuai dengan kajian etika dimana etika berhubungan dengan pula dengan agama dan hukum.

Etika Siber (*Cyberethics*) termasuk dalam kajian etika terapan atau etika khusus. Menurut Richard A. Spinello (2004), etika siber di definisikan sebagai penerapan etika yang menjelaskan tentang moral, hukum, dan isu sosial dalam pengembangan dan penggunaan teknologi siber. Yang mana teknologi siber itu ia definisikan pula sebagai sebuah spektrum besar yang membentang dari perangkat komputer hingga sekelompok jaringan komputasi informasi dan komunikasi.

> *"...the field of applied ethics that examines moral, legal, and social issues in the development and use of cybertechnology. Cybertechnology in turn, refers to abroad spectrum of technologies that range from stand alone computer to the cluster of networked computing information and communication".* (Spinello, 2004)

Dengan demikian etika siber atau etika internet tidak sekedar membahas tentang tata cara penggunaan internet yang baik, aman, dan santun – yang mana hal tersebut tergolong ke dalam etiket internet – namun lebih jauh lagi, etika internet mengkaji permasalahan-permasalahan moral, hukum, dan isu-isu sosial yang berhubungan dengan penggunaan komputer dan jaringan internet sebagai penunjang interaksi antar manusia.

Bilamana suatu tindakan merupakan pelanggaran etika atau bukan, melibatkan penilaian normatif dan penafsiran terhadap aturan tertulis. Telah diketahui pula bahwa teknologi siber menciptakan sebuah "dunia" tersendiri yang terpisah dari dunia riil; sebuah dunia siber (dunia maya/dunia virtual) yang hanya bisa diakses melalui sambungan internet pada komputer. Dunia siber ini mempunyai karakteristik yang berbeda dengan dunia riil. Karekteristik tersebut dijelaskan oleh Dysson (1994)[3] sebagai berikut:

1. Beroperasi secara virtual
2. Dunia siber (dunia maya) selalu berubah dengan cepat
3. Dunia siber tidak mengenal batas teritorial (*borderless*)
4. Orang yang hidup dalam dunia siber dapat melakukan aktivitasnya tanpa harus menunjukkan identitas aslinya (anonim).
5. Informasi di dalamnya bersifat publik.

Karakteristik dunia siber yang khas ini memberi peluang terhadap munculnya perilaku atau tindakan yang pada dunia riil tidak atau sulit bisa terwujud. Hal ini bisa disebabkan adanya batas-batas fisik (geografis, bangunan, dan lain-lain) dan situasi perjumpaan yang konkret (*face to face* dan/atau kehadiran orang lain secara riil).

Dunia siber menyediakan ruang fantasi yang luas untuk ekspresi ego individu. Dalam ruang imajiner tersebut, identitas menjadi abstrak dan bisa berganda. Pengguna bisa menjadi "hantu" yang bergentayangan di ruang privat pengguna lain. "Fasilitas" yang ditawarkan dunia siber ini tentu saja memberi peluang bagi siapa saja yang oportunis dan ingin mendapatkan keuntungan pribadi meskipun dicapai dengan mengorbankan prinsip-prinsip etis. Selain itu, kemajemukan pengguna internet yang berasal dari seluruh dunia juga berpotensi menimbulkan permasalahan nilai dan norma. Kondisi ini tidak berbeda dengan apa yang biasa terjadi di dunia nyata. Oleh karena itu praktik pelanggaran etika dan hukum pada teknologi siber merupakan adopsi dari apa yang terjadi di dunia nyata ke dalam dunia siber.

[3] Kejahatan Telematika Sebagai Kejahatan Transnasiona, jurnal dari http://www.academia.edu

Maka menjadi jelas bagi kita bahwa penggunaan komputer tidak menimbulkan isu tentang etika internet tanpa adanya teknologi siber.

Penguasaan dan penggunaan teknologi ICT komputer yang dibarengi dengan niat jahat berpotensi menimbulkan kejahatan siber. Ada banyak sekali bentuk kejahatan yang memanfaatkan komputer dan jaringan internet sebagai mediumnya. *Convention on Cybercrime* di Budapest, Hungaria pada tahun 2001 mengklasifikasikan kejahatan siber itu sebagai berikut:

1. *Illegal acces*; yaitu sengaja dan tanpa hak memasuki atau mengakses komputer pihak lain
2. *Illegal interception*; yaitu dengan sengaja dan tanpa hak mendengar atau menangkap secara diam-diam pengiriman dan pemancaran data komputer yang tidak bersifat publik, dari atau di dalam sistem komputer dengan menggunakan alat bantu teknis
3. *Data interference*; yaitu sengaja dan tanpa hak melakukan pengrusakan, penghapusan atau perubahan data komputer pihak lain
4. *System interference*; yaitu sengaja dan tanpa hak melakukan gangguan atau rintangan terhadap berfungsinya sistem komputer
5. *Misuses of Devices*; yaitu penyalahgunaan perlengkapan komputer, termasuk program komputer seperti *code access* dan sebagainya.
6. *Computer related forgery*; yaitu sengaja dan tanpa hak mengubah dan/atau menghapus data otentik menjadi tidak otentik atau digunakan sebagai data otentik untuk kepentingan pribadi (pemalsuan)
7. *Computer related fraud*; yaitu dengan sengaja menyebabkan hilangnya barang/kekayaan orang lain dengan cara memasukkan, mengubah, menghapus data komputer atau dengan mengganggu fungsi sistem komputer dengan tujuan untuk memperoleh keuntungan bagi diri sendiri atau orang lain (penipuan).
8. *Content-related offences*; yaitu delik-delik yang berhubungan dengan pornografi anak
9. *Offences related to infringements of copyright and related rights*; yaitu delik-delik yang terkait dengan pelanggaran hak cipta.

Dengan klasifikasi tersebut, maka bentuk-bentuk aktivitas di dunia siber berikut ini dapat dikategorikan sebagai kejahatan siber: 1) *Carding*, yaitu berbelanja dengan menggunakan nomor dan identitas kartu kredit orang lain yang diperoleh secara ilegal melalui internet; 2) *Hacking dan Cracking*, Kedua istilah ini merujuk pada kegiatan menerobos sistem keamanan komputer pihak lain. Bedanya, para *hacker* umumnya hanya senang pada proses "menerobos" tersebut sementara *cracker* memang mempunyai tujuan dan kepetingan tertentu; 3) *Defacing*, yaitu kegiatan mengubah laman situs tertentu. Motifnya bisa sekedar iseng, unjuk kebolehan, namun ada juga yang mencuri data untuk dijual pada pihak lain; 4) *Phising*; yaitu kegiatan memancing para pengguna internet (*user*) untuk memberikan data personal (*username* dan *password*) mereka pada situs yang telah di *deface*; 5) *Spaming*; yaitu pengiriman informasi yang tidak dikehendaki melalui e-mail sehingga sering juga disebut *bulk e-mail* atau *junk e-mail*. Spam seringkali dibarengi dengan *phising* untuk memperoleh keuntungan pribadi; 6) *Malware*; yaitu merupakan program komputer yang dibuat untuk merusak *software* atau *operating system*. Jenisnya beraneka ragam seperti *virus, worm,* atau *browser hijacker*; 7) Melakukan *copy paste* sebagian atau keseluruhan tulisan karya orang lain tanpa hak atau tidak mencantumkan sumbernya. Ini merupakan pelanggaran terhadap Hak Atas Kekayaan Intelektual (HAKI). Mengenai hal ini pemerintah RI telah memperbarui UU Hak Cipta yang lama yaitu UUHC No.6 Tahun1982 dan UUHC No.12 tahun 1997 dengan UUHC No.19 Tahun 2002 untuk melindungi hasil karya seseorang dan menegakkan etika dalam penggunaan komputer dan internet.

Bentuk-bentuk kejahatan siber tersebut masih bisa bertambah lagi menyesuaikan dengan perkembangan teknologi dan modus operandi yang bisa dilakukan untuk menghindari sistem proteksi komputer yang juga terus berkembang.

Maraknya kasus kejahatan siber ini menuntut diterapkannya regulasi yang khusus mengatur tentang hal ini. Sekarang, negara-negara di dunia sudah mempunyai perangkat hukum untuk memerangi kejahatan siber. Di Indonesia sendiri saat ini ada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) yang disahkan pada tanggal 25 Maret 2008 oleh DPR RI. UU ITE ini mengatur berbagai perlindungan hukum atas penyalahgunaan internet. UU semacam ini telah lebih dulu ada dan diterapkan di sejumlah negara-negara Eropa dan Amerika Serikat.

Namun begitu, karakter *borderless* dunia siber menjadi faktor yang menyulitkan upaya membangun aturan hukum yang jelas untuk menertibkan pengguna internet. Tidak adanya batas teritorial berarti memungkinkan kejahatan siber ini dilakukan lintas negara. Namun tidak adanya keseragaman dalam membuat regulasi dan aturan internal domestik membuat kejahatan semacam ini sulit diberantas. Kasus penyebaran *virus melissa* di sejumlah negara pada akhir dekade 90-an adalah contoh tentang hal ini. Virus yang dibuat oleh seorang programmer dari New Jersey bernama David L. Smith tersebut disebarluaskan melalui situs X-rate atau e-mail dan telah merugikan beberapa perusahaan hingga senilai US$ 80 milyar.[4] Setelah munculnya Resolusi PBB 55/63 pada tahun 2000 tentang anjuran bagi negara-negara anggota untuk memerangi tindak kejahatan siber, negara-negara yang tergabung dalam organisasi Kerjasama Ekonomi Asia Pasifik (APEC) sepakat membentuk *APEC Cyber Crime Strategy* yang bertujuan mengupayakan sistem keamanan internet bersama, dan mencegah serta menghukum pelaku kejahatan siber. Bahkan negara-negara ASEAN pernah pula menghasilkan deklarasi tentang pencegahan dan pengawasan kejahatan antar negara (*Manila Declaration on Prevention and Control of Transnational Crime*), termasuk di dalamnya kejahatan yang menggunakan teknologi ICT atau kejahatan siber. Akan tetapi upaya-upaya yang telah ditempuh tersebut hanya berupa kesepakatan moral dan politis saja, sedangkan pelaksanaannya diserahkan sepenuhnya pada kemauan dan kemampuan dari masing-masing negara anggota.

III. PENUTUP

Etika internet atau etika siber (*cyberethics*) merupakan adopsi dari konsep etika tradisional yang di terapkan pada konteks penggunaan dan pengembangan teknologi komputer dan jaringan internet. Penggunaan komputer tidak akan menimbulkan pelanggaran etika internet tanpa adanya teknologi siber. Teknologi siber ini menciptakan sebuah "dunia" baru yang di dalamnya manusia bisa berinteraksi, berserikat, berbisnis, dan banyak lagi aktivitas lainnya. Simulasi kehidupan dunia siber yang mirip dengan kehidupan riil, di tambah dengan karakteristik yang khas dari dunia siber itu sendiri, membuka peluang yang sangat besar untuk terjadinya tindak kejahatan siber. Kejahatan siber ini merupakan hal yang baru, dimana bentuk kejahatannya sangat beragam dan bisa terus bertambah mengingat teknologi komputer, komunikasi, dan informasi masih terus berkembang.

Di sinilah etika memegang peranan penting untuk menjaga supaya aktivitas di dunia siber dapat berjalan dengan tertib, aman, dan nyaman. Aturan dan undang-undang telah

[4]"Melissa Virus Exposes Computer Users' Vulnerability,"*Japan Computer Industry Scan*, April 12, 1999, available at 1999 WL 9642279;dalam http://media.hoover.org/documents/0817999825

dibuat untuk memerangi kejahatan siber. Namun pembuatan regulasi ini masih banyak dilakukan secara parsial, sesuai dengan kemampuan dan kemauan dari setiap negara untuk memerangi kejahatan siber. Perlu ada perhatian yang lebih serius terhadap kerjasama regional bahkan internasional dalam upaya melindungi dan mencegah terjadinya kejahatan siber. UU ITE Tahun 2008 yang menjadi acuan negara untuk menangani masalah kejahatan siber di Indonesia harus terbuka untuk pembaharuan dan penyesuaian. Selain itu, perlu ada upaya yang berkelanjutan dalam menyosialisasikan etika internet karena pengguna internet yang terus bertambah. Hal ini penting untuk menjaga etika dari pengguna internet pada tingkat individu.

REFERENSI

Bertens, K. 2011. *Etika.* Jakarta: PT Gramedia Pustaka Utama

Spinello, R.A. & Tavani, H.T. 2004. *Reading In Cyberethics 2nd Edition*. USA: Jone & Barlett Publisher, Inc.

Sumber Internet :

Associated Press. 1999, *Hackers Alter Romanian Money Rate*, dilihat pada Februari 2014. http://nytimes.com/aponline/i/AP-Romania-Hackers

Japan Computer Industry Scan. 1999. *Melissa Vyrus Exposes Computer Users Vulnerability.* 12 April, dilihat Februari 2014 dalam http://media.hoover.org/documents/0817999825

Soeparna, Intan. *Kejahatan Telematika Sebagai Kejahatan Internasional*, dilihat pada Februari 2014. http://academia.edu/208360