 ISBN 978-602-52451-0-7

PENGARUH NEGATIF ETIKA DAN MORALITAS PERETAS ATAU HACKER DALAM UPAYA MEMBANGUN SUMBERDAYA MANUSIA YANG BERBASIS SCIENCE DAN TEKNOLOGI DI EXPLOID ID HACKER FORUM

M Asmar Maheri

Program Studi Magister Pendidikan Bahasa Inggris
Universitas PGRI Palembang
E-mail: eririn776@gmail.com

Abstract-*Education and Technology is one of the pillars of human development and nation. Therefore, the government of Indonesia made education and technology as one of the needs for the whole society, but along with the high influence of technology in today's many who abuse technology tersebut.Internet is one technology that can not be separated in the present, any information can be searched and which usually misuses the Internet is called Peretas. Hackers or hackers are people who study, analyze, modify, break into computers and computer networks, either for profit or motivated by challenges. On the other hand the academics are required to better in building competence and technology-based innovation. Of course, the implementation must also promote moral and ethics. It is intended that all can run in accordance with the norms that have been embedded in the people of Indonesia. This is in line with what Kemenristekdikti, Syahril Caniago delivered in a technology seminar entitled 'Application of Technology to Preparing Young Generation in National' held in Hall Hall of Tangerang Regency Regent on Saturday (7/1/17). "As Students must continue to think positively in the face of competition challenges in the future, "he explained. In this article I as a researcher will use qualitative methods epistimologi based on the phenomenon of the rise of hackers or hackers in Indonesia.*

Keywords— Education, Internet, Hacker, Morality and Ethics

Abstrak-*Pendidikan dan Teknologi merupakan salah satu pilar dari pembangunan manusia dan bangsa. Oleh karena itu, pemerintah Indonesia menjadikan pendidikan dan teknologi sebagai salah satu kebutuhan bagi seluruh masyarakat, tetapi seiring tingginya pengaruh teknologi pada zaman sekarang banyak yang menyalahgunakan teknologi tersebut.Internet adalah salah satu teknologi yang tidak dapat dipisahkan pada zaman sekarang, informasi apapun dapat dicari dan yang biasanya menyalahgunakan internet disebut Peretas.Peretas atau hacker adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan. Disisi lain pihak akademisi dituntut untuk lebih baik dalam membangun kompetensi serta inovasi berbasis teknologi. Tentu, pelaksanaannya juga harus mengedepankan moral dan etika. Hal itu bertujuan agar semua dapat berjalan sesuai dengan Norma yang telah tertanam pada masyarakat Indonesia. Itu sejalan dengan apa yang disampaikan oleh Kemenristekdikti, Syahril Caniago dalam seminar teknologi bertajuk 'Penerapan Teknologi Untuk Menyiapakan Generasi Muda Dalam Nasional' yang diselenggarakan di Aula Pendopo Bupati Kabupaten Tangerang, Sabtu (7/1/17)."Sebagai Mahasiswa harus terus berfikir positif dalam menghadapi kompetisi tantangan di masa yang akan datang," paparnya. dalam artikel ini saya sebagai peneliti akan menggunakan metode kualitatif epistimologi berdasarkan fenomena maraknya hacker atau peretas di indonesia.*

Kata Kunci— Pendidikan, Internet, Hacker, Moralitas Dan Etika

PENDAHULUAN

Penelitian ini berawal dari banyaknya tuntutan bagi Pihak akademisi untuk lebih baik dalam membangun kompetensi serta inovasi berbasis teknologi. Tentu, pelaksanaannya juga harus mengedepankan moral dan etika. Hal itu bertujuan agar semua dapat berjalan sesuai dengan norma

yang telah tertanam pada masyarakat Indonesia.

Itu disampaikan oleh Direktorat Jendral Pembelajaran dan Kemahasiswaan pada Kementerian Riset Teknologi dan Pendidikan Tinggi (Kemenristekdikti), Syahril Caniago dalam seminar teknologi bertajuk 'Penerapan Teknologi Untuk Menyiapakan Generasi Muda Dalam Nasional' yang diselenggarakan pihak Badan Esekutif Mahasiswa (BEM) Fakultas Teknik Unversitas Muhamadiyah Tangerang (UMT), di Aula Pendopo Bupati Kabupaten Tangerang, Sabtu (7/1/17).

"Jadi kita mulai dari kampus, kami menyampaikan moral dan etika tujuannya itu. Menggunakan teknologi harus sesuai dengan fakta data, tidak bisa sembarangan mengupload informasi yang tidak bertanggungjawab. Kalau kita mau maju ya harus punya etika dan bertanggungjawab," tegas Syahril.

Untuk itu, seiring dengan perkembangan Informasi Teknologi (IT), kedepan pemerintah melalui Kemristekdikti sedianya telah melakukan upaya agar pengguna teknologi di jadikan ke hal yang positif, yakni dengan memberikan kuliah umum kepada mahasiswa diseluruh tanah air.

"Kedepan Kemendikti akan memberikan kuliah umum secara video konpren. Nanti kita akan fasilitasi itu.untuk mengambil contoh ke hal-hal yang lebih baik lagi," tandasnya.

Sementara, Ketua Panitia pelaksana Bem Fakultas Teknik UMT Trisana Anggoro mengatakan, ada sebayak 250 peserta dari berbagai universitas yang ada di Kota Tangerang, yang mengikuti seminar tersebut. Dimana, tujuannya adalah untuk membangun karakter mahasiswa dalam bidang teknologi.

"Kalau kita lihat dari sisi persentasinya, teknologi dipakai untuk medsos sekitar 20 persen dan dipakai untuk pembelajaran buku hanya 20 persen. Sedangkan, sisanya itu di gunkan kearah kurang baik, kita berharap,dengan seminar ini," katanya.

Dia berharap kedepan instansi pendidikan ikut mendorongnya. Karena saat ini dia menilai seperti ada pembiaran. "Saya yakin anak muda sekarang ini sebenarnya memiliki gagasan dan ide-ide cemerlang bagi kemajuan bangsa ini," tandasnya.

Pada zaman sekarang semua sistem tidak terlepas dari teknologi oleh karena sebagai seseorang yang berpendidikan haruslah bijak dalam menggunakan teknologi. Teknologi dan internet memfasilitasi kelahiran dan pertumbuhan kejahatan jaringan seperti virus, anti-virus, hacking. Hacking adalah praktek modifikasi perangkat keras komputer dan perangkat lunak sistem. Melanggar ilegal dari sebuah sistem komputer merupakan tindak pidana. Dan yang menyalagunakan teknologi ini biasanya disebut peretas.

Terminologi peretas muncul pada awal tahun 1960-di antara para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT). Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkutat dengan sejumlah komputer *mainframe*. Kata bahasa Inggris "hacker" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama.

Kemudian pada tahun 1983, istilah *hacker* mulai berkonotasi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer "The 414s" yang berbasis di Milwaukee, Amerika Serikat. 414 merupakan kode area lokal mereka.

Kelompok yang kemudian disebut *hacker* tersebut dinyatakan bersalah atas pembobolan 60 buah komputer, dari komputer milik Pusat Kanker Memorial Sloan-Kettering hingga komputer milik Laboratorium Nasional Los Alamos. Satu dari pelaku tersebut mendapatkan kekebalan karena testimonialnya, sedangkan 5 pelaku lainnya mendapatkan hukuman masa percobaan.

Kemudian pada perkembangan selanjutnya muncul kelompok lain yang menyebut-nyebut diri sebagai peretas, padahal bukan. Mereka ini (terutama para pria dewasa) yang mendapat kepuasan lewat membobol komputer dan mengakali telepon (*phreaking*). Peretas sejati menyebut orang-orang ini *cracker* dan tidak suka bergaul dengan mereka.

Peretas sejati memandang *cracker* sebagai orang malas, tidak bertanggung jawab, dan tidak terlalu cerdas. Peretas sejati tidak setuju jika dikatakan bahwa dengan menerobos keamanan seseorang telah menjadi peretas.

Para peretas mengadakan pertemuan tahunan, yaitu setiap pertengahan bulan Juli di Las Vegas. Ajang pertemuan peretas terbesar di dunia tersebut dinamakan *Def Con*. Acara Def Con tersebut lebih kepada ajang pertukaran informasi dan teknologi yang berkaitan dengan aktivitas peretasan. *Peretas miliki kesan yang negative di dalam* masyarakat karena perbedaan istilah tentang *hacker* dan *cracker*.

Banyak orang memahami bahwa peretaslah yang mengakibatkan kerugian pihak tertentu seperti

mengubah tampilan suatu situs web (*defacing*), menyisipkan kode-kode virus, dan lain-lain, padahal mereka adalah *cracker*. *Cracker*-lah menggunakan celah-celah keamanan yang belum diperbaiki oleh pembuat perangkat lunak (bug) untuk menyusup dan merusak suatu sistem. Atas alasan ini biasanya para *peretas* dipahami dibagi menjadi dua golongan: *White Hat Hackers*, yakni hacker yang sebenarnya dan *cracker* yang sering disebut dengan istilah *Black Hat Hackers*.

Peretas menurut Eric Raymond didefinisikan sebagai programmer yang pandai. Sebuah *hack* yang baik adalah solusi yang cantik untuk masalah pemrograman dan *hacking* adalah proses pembuatannya. Menurut Raymond ada lima (5) karakteristik yang menandakan seorang adalah hacker, yaitu:

1. Seseorang yang suka belajar detail dari bahasa pemrograman atau sistem.
2. Seseorang yang melakukan pemrograman, tidak cuma teori saja.
3. Seseorang yang bisa menghargai, menikmati hasil *hacking* orang lain.
4. Seseorang yang dapat secara cepat belajar pemrograman.
5. Seseorang yang ahli dalam bahasa pemrograman tertentu atau sistem tertentu, seperti *UNIX hacker*.

Pada hari Sabtu, 17 April 2004, Dani Firmansyah (25 th), konsultan Teknologi Informasi (TI) PT Danareksa di Jakarta berhasil membobol situs milik Komisi Pemilihan Umum (KPU) di http://tnp.kpu.go.id dan mengubah nama-nama partai di dalamnya menjadi nama-nama unik seperti Partai Kolor Ijo, Partai Mbah Jambon, Partai Jambu, dan lain sebagainya. Dani menggunakan teknik SQL Injection (pada dasarnya teknik tersebut adalah dengan cara mengetikkan string atau perintah tertentu di address bar browser) untuk menjebol situs KPU. Kemudian Dani tertangkap pada hari Kamis, 22 April 2004

Beberapa alasan mengenai pentingnya etika dalam dunia maya adalah sebagai berikut:

1. Bahwa pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adat istiadat yang berbeda-beda.
2. Pengguna internet merupakan orang-orang yang hidup dalam dunia anonymouse, yang tidak mengharuskan pernyataan identitas asli dalam berinteraksi.
3. Berbagai macam fasilitas yang diberikan dalam internet memungkinkan seseorang untuk bertindak etis seperti misalnya ada juga penghuni yang suka iseng dengan melakukan hal-hal yang tidak seharusnya dilakukan.
4. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat dan memungkinkan masuknya “penghuni” baru diduniamaya tersebut.

Pada versi FAU beberpa etika yang dikemukakan adalah sebagai berikut :

1. Internet tidak digunakan sebagai sarana kesaksian palsu
2. Internet tidak digunakan untuk mengcopy software tanpa adanya ijin dan pembayaran
3. Internet tidak digunakan sebagai sarana menyerobot atau mencuri file orang lain
4. Internet tidak digunakan untuk mencuri, contoh pengacakan kartu kredit dan pembobolan kartu kredit.
5. Internet tidak digunakan untuk mengcopy software tanpa adanya ijin dan pembayaran
6. Internet tidak digunakan sebagai sarana mengambil sumber – sumber penting tanpa adanya ijin atau mengikuti aturan yang berlaku.
7. Internet tidak digunakan untuk mengakui hak intelektual orang lain
8. Internet tidak digunakan sebagai sarana kejahatan bagi orang lain, artinya pemanfaatan internet semestinya tidak untuk merugikan orang lain baik secara materiil maupun moril.
9. Internet tidak digunakan sebagai sarana mengganggu kinerja orang lain yang bekerja menggunakan komputer. Contoh riil adalah penyebaran virus melalui internet
10. Bertanggung jawab terhadap isis pesan yang disampaikan.

Pentingnya Etika Dalam menggunakan Internet adalah sebagai berikut:

1. Harus diperhatikan bahwa pengguna internet akan selalu bertambah setiap saat dan memungkinkan masuknya penghuni baru didunia maya tersebut.
2. Berbagai macam fasilitas yang diberikan dalam internet memungkinkan seseorang untuk bertindak etis seperti misalnya ada juga penghuni yang suka iseng dengan melakukan hal-hal yang tidak seharusnya dilakukan.
3. Pengguna internet merupakan orang-orang yang hidup dalam dunia anonymouse, yang tidak mengharuskan pernyataan identitas asli dalam berinteraksi.

4. Bahwa pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adat istiadat yang berbeda-beda dan jangan terlibat dalam aktivitas pencurian/penyebaran data dan informasi yang memiliki hak cipta.Jika mengutip suatu tulisan, gambar, atau apapun yang bisa/diijinkan untuk dipublikasikan ulang, selalu tuliskan sumber aslinya. Jangan pernah memberikan nomor telepon, alamat email, atau informasi yang bersifat pribadi lainnya milik teman kepada pihak lain tanpa persetujuan teman itu sendri.Jangan menyindir, menghina, melecehkan, atau menyerang pribadi seseorang/pihak lain. Jangan sombong, angkuh, sok tahu, sok hebat, merasa paling benar, egois, berkata kasar, kotor, dan hal-hal buruk lainnya yang tidak bisa diterima orang.

Seperti halnya juga teknologi kumputer, orang yang sudah memiliki keahlian dibidang computer biasa membuat teknologi yang bermanfaat tetapi tidak jarang yang melakukan kejahatan. Aspek Hukum untuk mengatur aktifitas di internet terutama yang berhubungan dengan kejahatan maya antara lain masih menjadi perdebatan. Ada dua pandangan mengenai hal tersebut antara lain: a) Karakteristik aktifitas di internet yang bersifat lintas batas sehingga tidak lagi tunduk pada batasan-batasan territorial b) Sistem hukum tradisiomal (The Existing Law) yang justru bertumpu pada batasan-batasan teritorial dianggap tidak cukup memadai untuk menjawab persoalan-persoalan hukum yang muncul akibat aktifitas internet. Dilema yang dihadapi oleh hukum tradisional dalam menghadapi fenomena-fenomena cyberspace ini merupakan alasan utama perlunya membentuk satu regulasi yang cukup akomodatif terhadap fenomena-fenomena baru yang muncul akibat pemanfaatan internet. Aturan hukum yang akan dibentuk itu harus diarahkan untuk memenuhi kebutuhan hukum (the legal needs) para pihak yang terlibat di dalam transaksi-transaksi lewat internet. Hukum harus diakui bahwa yang ada di Indonesia sering kali belum dapat menjangkau penyelesaian kasus kejahatan computer. Untuk itu diperlukan jaksa yang memiliki wawasan dan cara pandang yang luas mengenai cakupan teknologi yang melatar belakangi kasus tersebut. Sementara hukum di Indonesia itu masih memiliki kemampuan yang terbatas didalam penguasaan terhadap teknologi informasi. 3. Aspek Pendidikan Dalam kode etik hacker ada kepercayaan bahwa berbagi informasi adalah hal yang sangat baik dan berguna, dan sudah merupakan kewajiban (kode etik) bagi seorang hacker untuk membagi hasil penelitiannya dengan cara menulis kode yang open source dan memberikan fasilitas untuk mengakses informasi tersebut dan menggunakn peralatan pendukung apabila memungkinkan. Disini kita bisa melihat adanya proses pembelajaran. Yang menarik dalam dunia hacker yaitu terjadi strata-strata atau tingkatan yang diberikan oleh komunitas hacker kepada seseorang karena kepiawaiannya bukan karena umur atau senioritasnya. Untuk memperoleh pengakuan atau derajat seorang hacker mampu membuat program untuk ekploit kelemahan system menulis tutorial/ artikel aktif diskusi di mailing list atau membuat situs web, dsb.

1. Menurut Mandell dalam Suhariyanto (2012,10) disebutkan ada dua kegiatan Computer Crime: penggunaan komputer untuk melaksanakan perbuatan,penipuan,pencurian,atau,penyembunyian yang dimaksud untuk memperoleh keuntungan keuangan, keuntungan bisnis, kekayaan atau pelayanan.
2. Ancaman terhadap komputer itu sendiri, seperti pencurian perangkat keras atau lunak, sabotase,dan,pemerasan.

   Pada dasarnya cybercrime meliputi tindak pidana yang berkenaan dengan sistem informasi baik sistem informasi itu sendiri juga sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

kararistik cyber crime :

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etis tersebut dilakukan dalam ruang/wilayah cyber sehingga tidak dapat dipastikan yuridiksi negara mana yang berlaku.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan tersebut mengakibatkan kerugian material maupun immaterial yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya.
5. Perbuatan tersebut sering dilakukan lintas batas negara.

Bentuk-bentuk Cybercrime

Klasifikasi kejahatan komputer:

1. Kejahatan yang menyangkut data atau informasi computer

2. Kejahatan yang menyangkut program atau software kompter
3. Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan yang tidak sesuai dengan tujuan pengolahan atau operasinya
4. Tindakan yang mengganggu operasi computer
5. Tindakan merusak peralatan komputer atau yang berhubungan dengan komputer atau sarana penunjangnya

Pengelompokan bentuk kejahatan yang berhubungan dengan penggunaan TI :

1. Unauthorized acces to computer system and service
2. Illegal Content
3. Data Forgery
4. Cyber Espionage
5. Cyber sabotage and extortion
6. Offense Against Intellectual Property
7. Infrengments of Privacy

1. Unauthorized acces to computer system and service

Kejahatan yang dilakukan dengan memasuki / menyusup kedalam suatu sistem jaringan komputer secara tidak dah, tanpa izin, atau tanpa sepengetahuan dari pemilik system jaringan yang dimasuki

2. Illegal Content

Kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum

Cth, Pornografi, penyebaran berita yang tidak benar

3. Data Forgery

Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptelss documen melalui internet

4. Cyber Espionage

Kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan memata-matai terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasaran

5. Cyber Sabotage and Extortion

Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau gangguan terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet

6. Offense Against Intellectual Property

Kejahatan ini ditunjukkan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet

7. Infrengments of Privacy

Kejahatan ini ditunjukkan terhadap informasi seseorang yang merupakan hal sangat priabdi dan rahasia

Hacker dan Cracker

Menurut Mansfield, hacker didefinisikan sebagai seseorang yang memiliki keinginan untuk melakukan eksplorasi dan penetrasi terhadap sebuah sistem operasi dan kode komputer pengamanan lainnya, tetapi tidak melakukan tindakan pengrusakan apapun, tidak mencuri uang atau informasi, sedangkan cracker adalah sisi gelap dari hacker dan memiliki ketertarikan untuk mencuri informasi, melakukan berbagai macam kerusakan dan sesekali waktu juga melumpuhkan keseluruhan sistem komputer.

Penggolongan Hacker dan Cracker

Recreational Hacker, kejahatan yang dilakukan oleh netter tingkat pemula untuk sekedar mencoba kekurangan handalan sistem sekuritas suatu perusahaan.

Crackers/Criminal Minded hackers, pelaku memiliki motivasi untuk mendapat keuntungan finansial, sabotase dan pengrusakan data. Tipe kejahatan ini dapat dilakukan dengan bantuan orang dalam.

Political Hackers, aktifis politis (*hactivist*) melakukan pengrusakan terhadapa ratusan situs web untuk mengkapanyekan programnya, bahkan tidak jarang dipergunakan untuk menempelkan pesan untuk mendiskreditkan lawanya.

Denial Of Service Attack

Didalam keamanan komputer, Denial Of Service Acttack (DoS Attack) adalah suatu usaha untuk membuat sumber daya komputer yang ada tidak bisa digunakan oleh para pemakai.

Secara khas target adalah high-profile web server, serangan ini mengarahkan menjadikan host halaman web tidak ada di Internet. Hal ini merupakan suatu kejahatan komputer yang melanggar kebijakan penggunaan internet yang diindikasi oleh Internet Arsitecture Broad (IAB).

Denial Of Service Attack mempunyai dua format umum:

1. Memaksa komputer-komputer korban untuk me*reset* atau korban tidak bisa lagi menggunakan perangkat komputernya seperti yang diharapkannya.
2. Menghalangi media komunikasi antara para pemakai dan korban sehingga mereka tidak bisa lagi berkomunikasi.

Denial Of Service Attack ditandai oleh suatu usaha eksplisit dengan penyerang untuk mencengah para pemakai memberi bantuan dari penggunaan jasa tersebut.

Contoh meliputi

1. Mencoba untuk "membanjiri" suatu jaringan, dengan demikian mencegah lalu lintas jaringan yang ada.
2. Berusaha untuk menggangu konkesi antara dua mesin, dengan demikian mencegah akses kepada suatu service.
3. Berusaha untuk mencegah individu tertentu dari mengakses suatu service.
4. Berusaha untuk menggangu service kepada suatu orang atau sistem spesifik

Pelanggaran *Privacy*

Privacy adalah kemampuan dari suatu individu atau kelompok untuk memelihara urusan pribadi dan hidup mereka ke luar dari pandangan publik, atau untuk mengedalikan alir informasi tentang diri mereka.

Pembajakan software aplikasi dan lagu dalam bentuk digital (MP3, MP4, MVA dll) merupakan trend dewasa ini, software dan lagu dapat dibajak melalui download dari internet dan copy ke dalam CD room ysng selanjutnya diperbanyak secara ilegal dan diperjual belikan secara ilegal.

Fraud

Merupakan kejahatan manipulasi informasi dengan tujuan mengeruk keuntungan yang sebersar-besarnya. Biasanya kejahatan yang dilakukan adalah memanipulasi informasi keuangan. Sebagai contoh adanya situs lelang fiktif. Melibatkan berbagai macam aktifitas yang berkaitan dengan kartu kredit. *Carding* muncul ketika seseorang yang bukan pemilik kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

Data Forgery

Kejahatan ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasi web database. Dokumen tersebut disimpan sebagai scriptless document dengan menggunakan media internet.

Istilah-istilah dalam Cyber Crime

Probing, aktivitas yang dilakukan untuk melihat servis-servis apa saja yang tersedia di server target.

Phising, e-mail penipuan yang seakan-akan berasal dari sebuah toko, bank atau perusahaan kartu kredit. Email ini mengajak anda untuk melkukan berbagai hal, misalnya memverifikasi informasi kartu kredit, meng-*update* password dan lainnya.

Cyber Espionage, kejahatan yang memanfaatkan internet untuk melakukan mata-mata terhadap pihak lain dengan memasuki sistem jaringan komputer pihak sasaran.

Offence Againts Intelectual Property, kejahatan yang ditunjukkan terhadap HAKI yang dimiliki pihak lain di internet

Kebijakan Hukum Cybercrime

I. Cyberlaw

Hukum pada prinsipnya merupakan pengaturan terhadap sikap tindakan (perilaku) seseorang dan masyarakat dimana akan ada sangsi bagi yang melanggar.

Alasan Cyberlaw itu diperlukan menurut Sitompul (2012,39) sebagai berikut:

1. Masyarakat yang ada di dunia virtual ialah masyarakat yang barasal dari dunia nyata yang memilki nilai dan kepentingan.
2. Meskipun terjadi di dunia virtual, transaksi yang dilakukan oleh masyarakat memiliki pengaruh dalam dunia nyata

Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya) yang umumnya diasosiasikan dengan internet.

Cyberlaw merupakan aspek hukum yang ruang lingkupnya meliputi setiap 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.

II. Ruang Lingkup Cyber Law

Jonathan Rosenoer dalam Cyber law, the law of internet mengingatkan tentang ruang lingkup dari cyber law diantarnya:

1. Hak Cipta (*Copy Right*)
2. Hak Merk (*Trademark*)
3. Pencemaran nama baik (*Defamation*)
4. Fitnah, Penistaan, Penghianaan (*Hate Speech*)
5. Serangan terhadap fasilitas komputer (*Hacking, Viruses, Illegal Access*)
6. Pengaturan sumber daya internet seperti IP-Address, domain name
7. Kenyamanan Individu *(Privacy*)
8. Prinsip kehati-hatian (*Duty Care*)
9. Tindakan kriminal biasa yang menggunakan TI sebagai alat
10. Isu prosedural seperti yuridiksi, pembuktian, penyelidikan dll
11. Kontak / transaksi elektronik dan tanda tangan digital
12. Pornografi
13. Pencurian melalui internet
14. Perlindungan Konsumen
15. Pemanfaatan internet dalam aktivitas keseharian seperti ecommerce, e-government, e-education dll

III. Pengaturan Cybercrime dalam UU ITE

Latar Belakang UU ITE

Undang-undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik (UU ITE) adalah undang-undang pertama di Indonesia yang secara khusus mengatur tindak pidana cyber

Berdasarkan surat Presiden RI. No.R./70/Pres/9/2005 tanggal 5 September 2005, naskah UU ITE, secara resmi disampaikan kepada DPR RI. Pada tanggal 21 April 2008, Undang-undang ini disahkan.

Dua muatan besar yang diatur dalam UU ITE, adalah:

1. Pengaturan transaksi elektronik
2. Tindak pidana cyber

Pengaturan Tindak Pidana TI dan Transaksi Elektronik

Tindak pidana yang diatur dalam UU ITE diatur dalam Bab IV tentang perbuatan yang dilarang, perbuatan tersebut dikategorikan menjadi kelompok sebagai berikut :

Tindak pidana yang berhubungan dengan aktifitas illegal, yaitu :

a. Distribusi atau penyebaran, transmisi, dapat diaksesnya konten illegal (kesusilaan, perjudian, berita bohong dll)
b. Dengan cara apapun melakukan akses illegal
c. Interpensi illegal terhadap informasi atau dokumen elektronik dan sistem elektronik.

Tindak Pidana yang berhubungan dengan gangguan (interfensi), yaitu:

a. Gangguan terhadap informasi atau dokumen elektronik
b. Gangguan terhadap sistem elektronik
c. Tindak Pidana memfasilitasi perbuatan yang dilarang
d. Tindak Pidana pemalsuan informasi atau dokumen elektronik
e. Tindak pidana tmabahan dan perbuata-perbuaan terhadap ancaman pidana

Pengertian Etika

Menurut kamus besar Bahasa Indonesia terbitan Departemen Pendidikan dan Kebudayaan (1988).

1. Ilmu tentang apa yang baik dan yang buruk, tentang hak dan kewajiban moral.
2. Kumpulan asas atau nilai yang berkenaan dengan akhlak.
3. Nilai mengenai benar atau salah yang dianut di masyarakat.

Etika berasal dari bahasa yunani “ethos” yang berarti adat istiadat atau kebiasaan yang baik.

Menurut Profesor Salomon dalam Wahyono (2006:3) etika dikelompokkan dalam dua definisi, yaitu:

1. Etika merupakan karakter individu, disebut pemahaman manusia sebagai individu beretika.
2. Etika merupakan hukum sosial. Sebagai hukum yang mengatur, mengendalikan serta membatasi perilaku manusia.

Etika, Moral dan Norma Moral

Moral berasal dari bahasa Latin ***“Mos”*** yang berarti adat kebiasaan.

Secara etimologis, moral Sama dengan etika yaitu nilai dan moral yang menjadi pegangan seseorang.

Magnis Suseno (1975) mengemukakan hal yang menjadi dasar Norma moral untuk

mengakui perbuatan baik atau buruk yaitu kebiasaan**.**

Hobbes dan Rousseau seperti dikutip oleh Huijbers (199: 50) mengemukakakan kesepakatan masyarakat sebagai dasar pengakuan perbuatan.
Menurut Lowrence Konhberg dalam Wahyono (2006:6), enam tahap perkembangan moral yang terkait dengan etika:

1. Orientasi pada hukuman, ganjaran, kekuatan fisik dan material.
2. Orientasi hedonistis hubungan antar manusia.
3. Orientasi konformitas.
4. Orientasi pada otoritas.
5. Orientasi kontrak sosial.
6. Orientasi moralitas prinsip suara hati, individual, komprehensif dan universal.

Hubungan etika dengan moral:
Etika merupakan refleksi kritis dari nilai moral, sedangkan dalam kondisi berbeda ia bisa sama dengan moral, yaitu nila-nilai yang menjadi pegangan seseorang atau suatu kelompok dalam mengatur tingkah laku didalam komunitas kehidupannya.
Aliran yang digunakan untuk menyatakan perbuatan moral itu baik atau buruk :

1. Aliran ***Hedonise*** (Aristippus pendiri mazhab Cyrene 400 SM, Epicurus 34 1271 SM)
Perbuatan manusia dikatakan baik apabila menghasilkan kenikmatan atau kebahagian bagi dirinya sendiri atau orang lain (perbuatan itu bermanfaat bagi semua orang).

2. Aliran ***Utilisme*** (Jeremy Bentham 1742-1832, John Stuart Mill 1806-1873)
Perbuatan itu baik apabila bermanfaat bagi manusia, buruk apabila menimbulkan mudharat bagi manusia.

3. Aliran ***Naturalisme*** (J.J.Roussea)
Perbuatan manusia dikatakan baik apabila bersifat alami, tidak merusak alam.

4. Aliran ***Vitalisme*** (Albert Schweizer abad 20) Perbuatan baik adalah perbuatan yang menambah daya hidup, perbuatan buruk adalah perbuatan yang mengurangi bahkan merusak daya hidup.
Sumaryono (1995) mengklasifikasikan moralitas menjadi dua golongan:

1. Moralitas Objektif
Moralitas yang melihat perbuatan sebagaimana adanya, terlepas dari segala bentuk modifikasi kehendak bebas pelakunya.

2. Moralitas Subjektif
Moralitas yang melihat perbuatan sebagai dipengaruhi oleh pengetahuan dan perhatian pelakunya, latar belakang, stabilitas emosional dan perlakuan personal lainnya.

METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif. Suharsimi (2005: 234) menyatakan bahwa penelitian kualitatif merupakan penelitian yang dimaksudkan untuk mengumpulkan informasi mengenai status atau gejala yang ada, yaitu gejala menurut apa adanya pada saat penelitian dilakukan. Bogdan dan Taylor (1975) dalam Lexy J. Moleong (2005: 4) mendefinisikan metodologi kualitatif adalah prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang diamati. Pendekatan epistimologi kualitatif bertujuan untuk mendeskripsikan gejala-gejala ataupun menginterpretasikan fenomena yang terjadi di lapangan. Dapat disimpulkan bahwa penelitian ini berusaha untuk memdeskripsikan sebuah fenomena dimana peneliti melakukan penelitian. Sedangkan jenis penelitian ini adalah studi kasus. Menurut Creswell (2009) "*A case study is an exploration of a 'bounded system' or a case (or multiple cases) over time through detailed, in depth data collection involving multiple sources of information rich in context.*

Menurut Flick dalam (Gunawan, 2013: 81) "*specific relevance to the study of social relations, owing to the fact of the pluralization of life worlds.* Penelitian kualitatif menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati (Margono, 2003: 36). Menurut Denzin dan Lincoln (1998) *qualitative research aims to get a better understanding through first hand experience, truthful reporting, and quotations of actual conversation.*
Dalam penelitian ini peneliti mengkaji pengaruh negatif etika dan moralitas peretas atau hacker dalam upaya membangun sumberdaya manusia yang

berbasis science dan teknologi di exploid id hacker forum.

Observasi ialah studi yang disengaja dan sistematis tentang fenomena sosial dan gejala-gejala psikis dengan jalan pengamatan dan pencatatan (Kartono, 1980: 142). Observasi selalu menjadi bagan dalam penelitian, dapat berlangsung dalam konteks experimental maupun dalam konteks ilmiah.

HASIL PENELITIAN DAN PEMBAHASAN

Sesuai dengan munculnya terminologi peretas pada awal tahun 1960 Para anggota organisasi mahasiswa Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT).Kelompok mahasiswa tersebut merupakan salah satu perintis perkembangan teknologi komputer dan mereka berkutat dengan sejumlah komputer *mainframe*. Kata bahasa Inggris "hacker" pertama kalinya muncul dengan arti positif untuk menyebut seorang anggota yang memiliki keahlian dalam bidang komputer dan mampu membuat program komputer yang lebih baik daripada yang telah dirancang bersama. Kemudian pada tahun 1983, istilah *hacker* mulai berkonotasi negatif. Pasalnya, pada tahun tersebut untuk pertama kalinya FBI menangkap kelompok kriminal komputer "The 414s" yang berbasis di Milwaukee, Amerika Serikat. 414 merupakan kode area lokal mereka. Dan untuk menghindari hal tersebut pihak akademisi untuk lebih baik dalam membangun kompetensi serta inovasi berbasis teknologi. Tentu, pelaksanaannya juga harus mengedepankan moral dan etika. Hal itu bertujuan agar semua dapat berjalan sesuai dengan norma yang telah tertanam pada masyarakat Indonesia. Seperti yang disampaikan oleh Direktorat Jendral Pembelajaran dan Kemahasiswaan pada Kementerian Riset Teknologi dan Pendidikan Tinggi (Kemenristekdikti), Syahril Caniago dalam seminar teknologi bertajuk 'Penerapan Teknologi Untuk Menyiapakan Generasi Muda Dalam Nasional' yang diselenggarakan pihak Badan Esekutif Mahasiswa (BEM) Fakultas Teknik Unversitas Muhamadiyah Tangerang (UMT), di Aula Pendopo Bupati Kabupaten Tangerang, Sabtu (7/1/17).

"Jadi kita mulai dari kampus, kami menyampaikan moral dan etika tujuannya itu. Menggunakan teknologi harus sesuai dengan fakta data, tidak bisa sembarangan mengupload informasi yang tidak bertanggungjawab. Kalau kita mau maju ya harus punya etika dan bertanggungjawab," tegas Syahril.

Untuk itu, seiring dengan perkembangan Informasi Teknologi (IT), kedepan pemerintah melalui Kemristekdikti sedianya telah melakukan upaya agar pengguna teknologi di jadikan ke hal yang positif, yakni dengan memberikan kuliah umum kepada mahasiswa diseluruh tanah air.

"Kedepan Kemendikti akan memberikan kuliah umum secara video konpren. Nanti kita akan fasilitasi itu.untuk mengambil contoh ke hal-hal yang lebih baik lagi," tandasnya.

Sementara, Ketua Panitia pelaksana Bem Fakultas Teknik UMT Trisana Anggoro mengatakan, ada sebayak 250 peserta dari berbagai universitas yang ada di Kota Tangerang, yang mengikuti seminar tersebut. Dimana, tujuannya adalah untuk membangun karakter mahasiswa dalam bidang teknologi.

"Kalau kita lihat dari sisi persentasinya, teknologi dipakai untuk medsos sekitar 20 persen dan dipakai untuk pembelajaran buku hanya 20 persen. Sedangkan, sisanya itu di gunkan kearah kurang baik, kita berharap,dengan seminar ini," katanya.

Dia berharap kedepan instansi pendidikan ikut mendorongnya. Karena saat ini dia menilai seperti ada pembiaran. "Saya yakin anak muda sekarang ini sebenarnya memiliki gagasan dan ide-ide cemerlang bagi kemajuan bangsa ini," tandasnya.dikarenakan pengguna internet berasal dari berbagai negara yang mungkin memiliki budaya, bahasa dan adat istiadat yang berbeda-beda diaharapkan para pengguna teknologi tersebut jangan terlibat dalam aktivitas pencurian/penyebaran data dan informasi.. Jangan menyebarkan nomor telepon, alamat email, atau informasi yang bersifat pribadi lainnya milik teman kepada pihak lain tanpa persetujuan teman itu sendri.Jangan menyindir, menghina, melecehkan, atau menyerang pribadi seseorang/pihak lain. Jangan sombong, angkuh, sok tahu, sok hebat, merasa paling benar, egois, berkata kasar, kotor, dan hal-hal buruk lainnya yang tidak bisa diterima orang.

Seperti halnya juga teknologi kumputer, orang yang sudah memiliki keahlian dibidang computer biasa membuat teknologi yang bermanfaat tetapi tidak jarang yang melakukan kejahatan oleh karena itu seharusnya hal tersebut dapat dimanfaatkan sebaik-baiknya di arah yang sesuai dengan apa yang telah diterapkan oleh aturan- aturan yang telah buat oleh pemerintah sesuai dengan perkembangan Informasi Teknologi (IT), agar pengguna teknologi selalu menggunaka teknologi ke hal yang positif.

KESIMPULAN

Pihak akademisi dituntut untuk lebih baik dalam membangun kompetensi serta inovasi berbasis teknologi. Tentu, pelaksanaannya juga harus mengedepankan moral dan etika. Hal itu bertujuan

agar semua dapat berjalan sesuai dengan norma yang telah tertanam pada masyarakat Indonesia.dan para pengguna teknologi diharapkan untuk bijak dalam penggunaannya diakarenakan apabila salah dalam pengunaannya dan merugikan orang lain akan berdampak kepada diri sendiri karena telah uu yang mengantur keseimbangan hak- hak para pengguna lainnya dan dapat dipidanakan menurut uu yang berlaku di wilayah tersebut khususnya indonesia

DAFTAR PUSTAKA

1. Logik Bomb: Hacker's Encyclopedia (1997)
2. Hafner,Katie; Markoff,John (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster. ISBN 0-671-68322-5.
3. Sterling, Bruce (1992). *TheHacker Crackdown*. Bantam. ISBN 0-553-08058-X.
4. Slatalla, Michelle (1995). *Masters of Deception: The Gang That Ruled Cyberspace*. HarperCollins. ISBN 0-06-017030-1
5. Dreyfus, Suelette (1997). *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*. Mandarin. ISBN 1-86330-595-5.
6. Verton, Dan (2002). *The Hacker Diaries : Confessions of Teenage Hackers*. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.
7. Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. ISBN 0-8166-3345-2.
8. Taylor, Paul A. (1999). *Hackers: Crime in the Digital Sublime*. Routledge. ISBN 978-0-415-18072-6.
9. Levy, Steven (2002). *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. Penguin. ISBN 0-14-024432-8.
10. Ventre, Daniel (2009). *Information Warfare*. Wiley - ISTE. ISBN 978-1-84821-094-3.
11. http://wahyudifebriansyach.blogspot.com/2012/04/tugas-etika-profesionalisme.html
12. http://wartawarga.gunadarma.ac.id/2012/05/pelanggaran-kode-etik-terkait-penggunaan-hi-tech/
13. http://alandacreative.blogspot.com/2012/03/artikel-tentang-kejahatan-dan-praktek.html
14. http://reza-ajie.mhs.narotama.ac.id
15. http://slamet10018075.blogspot.co.id/2011/10/makalah-ethic-cyber-perkembangan.html