

Nama : Levina Gunawan

NIM : 201402052

Kelas : K01 A - TI

Tugas 3
Etika Profesi

1. Adakah hukum di Indonesia yang digunakan untuk mencegah atau menghukum tindakan cyberbullying, cyberstalking, dan pengungkapan materi yang tidak pantas? Apabila ada, tuliskan Undang-undang yang mengatur masalah ini! (pasalnya dan isinya)
2. Cyberbullying merupakan aksi mengintimidasi, mengancam, menyakiti, atau menghina orang lain melalui media internet terutama anak-anak dengan usia sekitar 15 tahun. Cyberstalking adalah aksi menyorot seseorang melalui sosial media yang berisi pesan mengancam dan menguntit bahkan serangan fisik yang dapat menyebabkan korban merasa takut dan menderita secara mental. Sedangkan, pengungkapan materi tidak pantas di sosial media dapat berupa artikel atau video pencabulan atau kekerasan ataupun pencemaran nama baik. Kejahatan-kejahatan tersebut dapat mengakibatkan korban mengalami gangguan psikologis bahkan hingga bunuh diri. Oleh karena itu, Cybercrime tentunya diatur dalam UU No 19 Tahun 2016 Pasal 27 Ayat 3 dan 4 yang berbunyi:

(3) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik.

(4) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman.

Sementara mengenai hukuman atas pelanggaran terhadap UU No 19 Tahun 2016 Pasal 27 ayat 3 dan 4 tertulis dalam UU No 19 Tahun 2016 Pasal 45 ayat 3 dan 4 yang berbunyi:

(3) Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan penghinaan dan/atau pencemaran nama baik sebagaimana dimaksud dalam Pasal 27 ayat (3) dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750.000.000,00 (tujuh ratus lima puluh juta rupiah).

(4) Setiap orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan pemerasan dan/atau pengancaman sebagaimana dimaksud dalam pasal 27 ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000.000,00 (satu miliar rupiah).

Selain itu, dalam UU No 19 Tahun 2016 Pasal 29 juga diatur hal serupa yang mawo berbunyi:
"Setiap orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi"

sementara hukuman atas pelanggaran UU No 19 tahun 2016 Pasal 29 diatur dalam UU No 19 tahun 2016 Pasal 45b yang berbunyi :

"Setiap orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakutkan yang ditujukan secara pribadi sebagai mana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp 750.000.000 (tujuh ratus lima puluh juta rupiah)"

2. Adakah masalah etika lainnya yang terjadi di Internet (jejaring media, website, grup percakapan, mailing list)? Jelaskan.

- a. Cyberterrorism adalah serangan berencana terhadap informasi, sistem komputer, dan data yang biasanya bersifat politik. Kejahatan ini dilakukan dengan tujuan untuk mengancam atau mengintimidasi hukum dan pemerintah. Salah satu contohnya, seperti kasus seorang cracker yang mengubah isi halaman web dengan propaganda Anti-American, Anti-Israel, Pro-Tan Loden selama kurang lebih lima tahun. Kasus lainnya seperti kasus perungkapan pelaku pembuat situs yang digunakan oleh kelompok jaringan teroris di Indonesia untuk melakukan propaganda terorisme melalui Internet pada tahun 2004 lalu.
- b. Denial of Service Attack adalah serangan yang dilakukan melalui sebuah komputer atau server di dalam jaringan sehingga membuat suatu website tidak dapat diakses oleh pengguna. Kejahatan ini dilakukan dengan cara membombardir lalu lintas jaringan dan menghabiskan bandwidth server sehingga layanan menjadi tidak tersedia bagi pengguna. Contoh kasusnya seperti serangan terhadap situs pemerintah <http://www.polri.go.id> yang mengakibatkan terhambatnya pelayanan publik karena situs down 10%.
- c. Piracy adalah aksi pembajakan software. Kejahatan tersebut dapat dilakukan dengan cara memasukkan software ilegal ke harddisk, pemakaian lisensi melebihi kapasitas, penjualan CDROM ilegal, download ilegal, penyewaan software ilegal. Terjadi pada tahun 2007, sekitar 84 software yang ada di Indonesia tercatat sebagai software bajakan yang menyebabkan kerugian sebesar US\$ 411 juta. Contoh kasusnya seperti kasus website file sharing terbesar, Megaupload, yang diduga melakukan pelanggaran piracy terbesar di dunia karena mendukung adanya situs yang memiliki berjuta-juta software ilegal.
- d. Fraud adalah aksi kejahatan yang dilakukan dengan tujuan untuk meraup keuntungan sebanyak-banyaknya. Fraud dapat dilakukan dengan memanipulasi informasi seperti pajak, kartu kredit, kartu telepon, dan lain-lain. Fraud juga dapat diartikan sebagai pelaporan keuangan palsu secara disengaja untuk mengkhianatkan sejumlah uang tertentu yang perlu dibayar. Contoh kasusnya adalah penipuan finansial yang dialami Facebook (kerugian US\$ 99 juta) dan Google (kerugian US\$ 23 juta) pada tahun 2013-2015 akibat tagihan palsu yang dikirim melalui email.

- e. Gambling adalah aksi perjudian untuk meraup lebih banyak keuntungan dari yang diberikan sebagai bahan judian. Saat ini, gambling tidak hanya terjadi secara konvensional, tetapi juga melalui jaringan sosial, website, ataupun media internet lainnya. Jenis-jenis online gambling dapat berupa casino, poker, dll. Contoh kasus seperti ditangkapnya 7 orang pria yang diduga terlibat judi poker online pada tahun 2013 lalu.
- f. Sebenarnya masih banyak lagi masalah-masalah etika selain kelima poin yang dijelaskan di atas, seperti hacking, spoofing, spamming, dll. Semakin pesatnya perkembangan internet membuat kasus kejahatan cyber pun menjadi semakin marak terjadi.
3. Menurut Ando apakah solusi terbaik yang sesuai (dapat diterima masyarakat Indonesia) untuk mengatur semua tindakan tidak etis (masalah etika) yang terjadi di Internet?
- = Akibat perkembangan sistem informasi yang semakin pesat, kasus-kasus pelanggaran etika di Internet juga semakin marak terjadi. Kasus cybercrime bertambah pesat setiap tahunnya, bahkan bermunculan kasus-kasus baru yang belum ada sebelumnya. Hal ini membuat masyarakat merasa resah apalagi internet saat ini sudah menjadi kebutuhan sehari-hari setiap orang baik di bidang pendidikan, ekonomi, sosial, budaya, hukum, dan lain-lain. Kasus-kasus seperti Cyberbullying, Cyberstalking, Judi Online, Hacking, spoofing, DoS Attack, Fraud, dan Piracy mengganggu aktivitas sehari-hari masyarakat Indonesia, merugikan mereka, bahkan menyebabkan terjadinya gangguan fisik maupun mental hingga bunuh diri. Oleh karena itu, tentunya diperlukan solusi yang tepat dalam mengatur tindakan etis yang terjadi di Internet. Akan tetapi, tidak semua solusi dianggap cocok untuk menyelesaikan kasus tersebut.

Menurut saya, salah satu tindakan yang tepat untuk dilakukan, yakni dengan menetapkan UU yang mengatur pelanggaran dan hukuman terhadap Cyber Crime. Yang mau sebenarnya hal ini sudah dilakukan oleh pemerintah, seperti yang dapat kita lihat pada UU No 19 Tahun 2016 Pasal 27, 28, 29, 30, 33, 34, 35, 45 UU ITE yang meniadakan aksi yang termasuk pelanggaran Cyber Crime beserta sanksi yang akan dikenakan terhadap pelanggaran tersebut. Akan tetapi, kasus Cyber Crime di Indonesia masih marak terjadi sehingga diperlukan tindakan pemerintah untuk memperkuat hukum yang mengatur tentang pelanggaran tersebut sehingga dapat mengurangi kasus kejahatan Cyber Crime di Indonesia.

Solusi lain yang dapat dilakukan adalah dengan memasukkan pendidikan mengenai Cyber Crime ke dalam kurikulum sehingga masyarakat dapat diajarkan mengenai bahaya tindakan kejahatan di Internet. Solusi ini selain dapat mengajarkan masyarakat mengenai cara menghadapi kasus-kasus kejahatan tersebut, juga dapat

menghindarkan mereka dari tindakan kejahatan yang mungkin saja mereka lakukan tanpa mereka sadari.

Selain itu, upaya seperti pengadaan sosialisasi antisipasi kasus kejahatan Cyber Crime juga dapat dilakukan oleh pemerintah untuk memberi pemahaman bagi masyarakat tentang Cyber Crime dan cara mencegahnya. Sosialisasi juga dapat dilakukan melalui poster, ataupun iklan website, juga dapat melalui artikel-artikel yang diposting melalui media sosial.

Tindakan untuk menyaring artikel-artikel yang dimasukkan ke Internet juga bisa menjadi solusi tambahan dalam mencegah semakin meningkatnya kasus Cyber Crime di Indonesia.