

TUGAS MAKALAH
ETIKA PROFESI TEKNOLOGI INFORMASI & KOMUNIKASI
CYBERCRIME DAN CYBERLAW



Dosen Pengajar : Rini Nuraini

Disusun Oleh :

- | | |
|-----------------------------|----------|
| 1. Hasan Nuripno | 13121592 |
| 2. Ahmad Irsan | 13111323 |
| 3. Singgih Gustiyono Junier | 13120889 |
| 4. Rio Putra Yani | 13121500 |
| 5. Zaenal Arifin Efendi | 13121171 |

Jurusan Teknik Komputer
Akademi Manajemen Informatika dan Komputer
Bina Sarana Informatika
Keramat 18
2013

KATA PENGANTAR

Puji dan Syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya kepada kita semua. Shalawat serta salam semoga tetap tercurah kepada Nabi besar Muhammad SAW.

Etika Profesi Teknologi Informasi & Komunikasi adalah salah satu mata kuliah kami pada semester III Jurusan Teknik Komputer Akademi Manajemen Informatika dan Komputer Bina Sarana Informatika. Mata kuliah ini begitu penting bagi kami terutama dalam hal pengenalan etika dan estetika dalam berinteraksi dengan segala hal yang berkaitan dengan teknologi informasi dan komunikasi.

Makalah Cyber Crime dan Cyber Law ini merupakan salah satu tugas atau syarat dalam memenuhi nilai UAS pada mata kuliah Etika Profesi Teknologi Informasi & Komunikasi. Dengan terselesaiannya makalah ini kami mengucapkan terimakasih kepada segala pihak yang telah memberikan bantuan dan dukungan, terutama sekali kepada :

1. Orang tua kami tercinta yang telah mendukung langkah gerak kami menjalani kuliah.
2. Ibu Rini Nuraini selaku Dosen pengajar Mata Kuliah Etika Profesi Teknologi Informasi & Komunikasi yang telah memberikan dukungan semangat kepada kami dalam hal penyusunan makalah ini.
3. Rekan-rekan seperjuangan kelas 13.3F.07 Jurusan Teknik Komputer di Bina Sarana Informatika yang selama ini telah bahu membahu saling menolong dan saling memberi dorongan semangat dalam berbagai hal.

Akhirnya, penyusun berharap semoga makalah ini dapat memberikan manfaat bagi siapa saja yang membacanya, menambah wawasan dan pengetahuan terutama dalam hal cybercrime dan cyberlaw.

Jakarta, Oktober 2013

Penyusun

DAFTAR ISI

**HALAMAN JUDUL
KATA PENGANTAR
DAFTAR ISI**

BAB I

PENDAHULUAN

- A. Latar Belakang
- B. Metode Penulisan

BAB II

PEMBAHASAN

CYBEER CRIME

- A. Definisi Cyber Crime
- B. Karakteristik Cyber Crime
- C. Bentuk-bentuk Cyber Crime
- D. Motif Cyber Crime
- E. Faktor Penyebab Cyber Crime
- F. Jenis – Jenis Cyber Crime
- G. Cyber Crime Di Indonesia
- H. Penanganan Cybeer Crime
- I. Perangkat Anti Cyber Crime
- J. Contoh Kasus Cyber Crime

BAB III CYBER LAW

- A. Definisi Cyber Law
- B. Jenis – Jenis Kejahatan Cyber Law
- C. Aspek Hukum Terhadap Kejahatan Cyber Law
- D. Cyber Law Di Indonesia
- E. Contoh Kasus Cyber Law

BAB IV PENUTUP

- A. Kesimpulan
- B. Saran

LAMPIRAN

DAFTAR PUSTAKA

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Pemanfaatan Teknologi Informasi, media, dan komunikasi telah mengubah baik perilaku masyarakat maupun peradaban manusia secara global. Perkembangan teknologi informasi dan komunikasi telah pula menyebabkan hubungan dunia menjadi tanpa batas (borderless) dan menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan berlangsung demikian cepat. Teknologi Informasi saat ini menjadi pedang bermata dua karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif perbuatan melawan hukum.

B. METODE PENULISAN

www.bsimedia5.blogspot.com adalah salah satu blog dari tugas Mata Kuliah Etika Profesi Teknologi Informasi & Komunikasi. Penyusunan Blog ini (khususnya artikel yang berkaitan dengan cybercrime dan cyberlaw) adalah hasil dari apa yang telah kami pelajari dari kampus ataupun dari bantuan media internet maupun buku-buku yang telah kami pelajari sebelumnya. Kami berharap semoga dengan adanya blog ini dapat memberikan pengetahuan yang bermanfaat khususnya berkaitan dengan cybercrime dan cyberlaw.

Dalam penyusunan makalah ini, kami menggunakan beberapa tahap. Pada tahap awal yaitu pengumpulan data dan fakta kami lakukan dengan cara paralel, kemudian seluruh data dan fakta yang kami dapat dihimpun untuk kemudian diseleksi, mana yang akan dibahas lebih lanjut dalam makalah kami. Kemudian, segala data dan fakta yang telah lolos seleksi kami kelompokkan dan kami urutkan berdasarkan tema pembahasan, kemudian penulisan makalah dilakukan dengan memperhatikan data dan fakta yang kami peroleh sebagai bahan referensi penulisan.

BAB II

CYBERCRIME

A. DEFINISI CYBERCRIME

Cybercrime adalah tindakan pidana kriminal yang dilakukan pada teknologi internet (cyberspace), baik yang menyerang fasilitas umum di dalam cyberspace ataupun kepemilikan pribadi. Secara teknik tindak pidana tersebut dapat dibedakan menjadi off-line crime, semi online crime, dan cybercrime. Masing-masing memiliki karakteristik tersendiri, namun perbedaan utama antara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

Cybercrime dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. The Prevention of Crime and The Treatment of Offenderes di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal:

1. **Cybercrime dalam arti sempit** disebut computer crime, yaitu prilaku ilegal/ melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses oleh komputer.
2. **Cybercrime dalam arti luas** disebut computer related crime, yaitu prilaku ilegal/ melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pengertian di atas, cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

B. KARAKTERISTIK CYBER CRIME

Karakteristik cybercrime yaitu :

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 melintas batas Negara.

C. Bentuk-Bentuk Cybercrime

Klasifikasi Kejahatan komputer :

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

Adapun pengelompokan bentuk kejahatan yang berhubungan dengan penggunaan TI, yaitu :

1. Unauthorized acces to computer system and service

Kejahatan yang dilakukan dengan memasuki / menyusup kedalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan yang di masuki.

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 penting yang tersimpan sebagai scriptless document 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 penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. Offense Against Intellectual Property

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

7. Infrengments of Piracy

Kejahatan ini ditujukan terhadap informasi seseorang yang merupakan hal sangat pribadi dan rahasia.

D. MOTIF CYBERCRIME

Motif pelaku kejahatan di dunia maya (cybercrime) pada umumnya dapat dikelompokkan menjadi dua kategori, yaitu :

1. **Motif intelektual**, yaitu kejahatan yang dilakukan hanya untuk kepuasan pribadi dan menunjukkan bahwa dirinya telah mampu untuk merekaya dan mengimplementasikan bidang teknologi informasi. Kejahatan dengan motif ini pada umumnya dilakukan oleh seseorang secara individual.
2. **Motif ekonomi, politik, dan kriminal**, yaitu kejahatan yang dilakukan untuk keuntungan pribadi atau golongan tertentu yang berdampak pada kerugian secara ekonomi dan politik pada pihak lain. Karena memiliki tujuan yang dapat berdampak besar, kejahatan dengan motif ini pada umumnya dilakukan oleh sebuah korporasi.

E. FAKTOR PENYEBAB MUNCULNYA CYBERCRIME

Jika dipandang dari sudut pandang yang lebih luas, latar belakang terjadinya kejahatan di dunia maya ini terbagi menjadi dua faktor penting, yaitu :

1. Faktor Teknis

Dengan adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan pihak yang satu lebih kuat daripada yang lain.

2. Faktor Sosial ekonomi

Cybercrime dapat dipandang sebagai produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan. Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Melihat kenyataan seperti itu, Cybercrime berada dalam skenario besar dari kegiatan ekonomi dunia.

F. JENIS-JENIS CYBERCRIME

Pengelompokan jenis-jenis cybercrime dapat dikelompokkan dalam banyak kategori. Bernstein, Bainbridge, Philip Renata, As'ad Yusuf, sampai dengan seorang Roy Suryo pun telah membuat pengelompokan masing-masing terkait dengan cybercrime ini. Salah satu pemisahan jenis cybercrime yang umum dikenal adalah kategori berdasarkan motif pelakunya :

1. Sebagai tindak kejahatan Murni

Kejahatan terjadi secara sengaja dan terencana untuk melakukan perusakan, pencurian, tindakan anarkis terhadap sistem informasi atau sistem komputer. (tindak kriminal dan memiliki motif kriminalitas) dan biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh Kasus: Carding, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet, Pengirim e-mail anonim yang berisi promosi (spamming).

2. Sebagai tindak kejahatan Abu-abu (tidak jelas)

Kejahatan terjadi terhadap sistem komputer tetapi tidak melakukan perusakan, pencurian, tindakan anarkis terhadap sistem informasi atau sistem komputer. Contoh Kasus: Probing atau Portscanning; yaitu semacam tindakan pengintaian terhadap sistem milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

Convention on Cybercrime yang diadakan oleh Council of Europe dan terbuka untuk ditandatangani mulai tanggal 23 November 2001 di Budapest menguraikan jenis-jenis kejahatan yang harus diatur dalam hukum pidana substantif oleh negara-negara pesertanya, terdiri dari :

- Tindak pidana yang berkaitan dengan kerahasiaan, integritas dan keberadaan data dan sistem komputer: Illegal access (melakukan akses tidak sah), Illegal interception (intersepsi secara tidak sah), Data interference (mengganggu data), System interference (mengganggu pada sistem), Misuse of devices (menyalahgunakan alat).
- Tindak pidana yang berkaitan dengan komputer: Computer-related forgery (pemalsuan melalui komputer), Computer-related fraud (penipuan melalui komputer).
- Tindak pidana yang berhubungan dengan isi atau muatan data atau sistem komputer: Offences related to child pornography (Tindak pidana yang berkaitan dengan pornografi anak).
- Tindak pidana yang berkaitan dengan pelanggaran hak cipta dan hak-hak terkait.

G. CYBERCRIME DI INDONESIA

Ada beberapa fakta kasus cybercrime yang sering terjadi di Indonesia, diantaranya adalah :

1. Pencurian Account User Internet

Merupakan salah satu dari kategori Identity Theft and fraud (pencurian identitas dan penipuan), hal ini dapat terjadi karena pemilik user kurang aware terhadap keamanan di dunia maya, dengan membuat user dan password yang identik atau gampang ditebak memudahkan para pelaku kejahatan dunia maya ini melakukan aksinya.

2. Deface (Membajak situs web)

Metode kejahatan deface adalah mengubah tampilan website menjadi sesuai keinginan pelaku kejahatan. Bisa menampilkan tulisan-tulisan provokative atau gambar-gambar lucu. Merupakan salah satu jenis kejahatan dunia maya yang paling favorit karena hasil kejahatan dapat dilihat secara langsung oleh masyarakat.

3. Probing dan Port Scanning

Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan “port scanning” atau “probing” untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan firewall atau tidak) dan seterusnya.

4. Virus dan Trojan

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Trojan adalah sebuah bentuk perangkat lunak yang mencurigakan (malicious software) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

5. Denial of Service (DoS) attack

Denial of Service (DoS) attack adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

H. PENANGANAN CYBERCRIME

Cybercrime adalah masalah dalam dunia internet yang harus ditangani secara serius. Sebagai kejahatan, penanganan terhadap cybercrime dapat dianalogikan sama dengan dunia nyata, harus dengan hukum legal yang mengatur. Berikut ini ada beberapa Cara Penanganan Cybercrime :

1. Dengan Upaya non Hukum

Adalah segala upaya yang lebih bersifat preventif dan persuasif terhadap para pelaku, korban dan semua pihak yang berpotensi terkait dengan kejahatan dunia maya.

2. Dengan Upaya Hukum (Cyberlaw)

Adalah segala upaya yang bersifat mengikat, lebih banyak memberikan informasi mengenai hukuman dan jenis pelanggaran/ kejahatan dunia maya secara spesifik.

Beberapa contoh yang dapat dilakukan terkait dengan cara pencegahan cyber crime adalah sebagai berikut:

1. Untuk menanggulangi masalah Denial of Services (DoS), pada sistem dapat dilakukan dengan memasang firewall dengan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) pada Router.
2. Untuk menanggulangi masalah virus pada sistem dapat dilakukan dengan memasang anti virus dan anti spy ware dengan upgrading dan updating secara periodik.
3. Untuk menanggulangi pencurian password dilakukan proteksi security system terhadap password dan/ atau perubahan password secara berkala.

Pemanfaatan Teknologi Informasi dalam kehidupan sehari-hari kita saat ini. Contoh: penggunaan mesin ATM untuk mengambil uang; handphone untuk berkomunikasi dan bertransaksi (mobile banking); Internet untuk melakukan transaksi (Internet banking, membeli barang), beririm e-mail atau untuk sekedar menjelajah Internet; perusahaan melakukan transaksi melalui Internet (e-procurement). Namun demikian segala aktivitas tersebut memiliki celah yang dapat dimanfaatkan oleh orang yang tidak bertanggung jawab untuk melakukan kejadian dunia maya (cybercrime), misalnya: Penyadapan email, PIN (untuk Internet Banking), Pelanggaran terhadap hak-hak privacy, dll. Maka dari itu diperlukan sebuah perangkat hukum yang secara legal melawan cybercrime. Dalam hal ini cyberlaw tercipta.

I. PERANGKAT ANTI CYBERCRIME

Beberapa Hal yang perlu dilakukan dalam menangani Cybercrime adalah memperkuat aspek hukum dan aspek non hukum, sehingga meskipun tidak dapat direduksi sampai titik nol paling tidak terjadinya cybercrime dapat ditekan lebih rendah.

1. **Modernisasi Hukum Pidana Nasional.** Sejalan dengan perkembangan teknologi, cybercrime juga mengalami perubahan yang significant. Contoh: saat ini kita mengenal ratusan jenis virus dengan dampak tingkat kerusakan yang semakin rumit.
2. **Meningkatkan Sistem Pengamanan Jaringan Komputer.** Jaringan komputer merupakan gerbang penghubung antara satu sistem komputer ke sistem yang lain. Gerbang ini sangat rentan terhadap serangan, baik berupa denial of service attack atau virus.
3. **Meningkatkan pemahaman & keahlian Aparatur Penegak Hukum.** Aparatur penegak hukum adalah sisi brainware yang memegang peran penting dalam penegakan cyberlaw. dengan kualitas tingkat pemahaman aparat yang baik terhadap cybercrime, diharapkan kejadian dapat ditekan.
4. **Meningkatkan kesadaran warga mengenai masalah cybercrime.** Warga negara merupakan konsumen terbesar dalam dunia maya. Warga negara memiliki potensi yang sama besar untuk menjadi pelaku cybercrime atau corban cybercrime. Maka dari itu, kesadaran dari warga negara sangat penting.

5. **Meningkatkan kerjasama antar negara dalam upaya penanganan cybercrime.** Berbagai pertemuan atau konvensi antar beberapa negara yang membahas tentang cybercrime akan lebih mengenalkan kepada dunia tentang fenomena cybercrime terutama beberapa jenis baru.

J. CONTOH KASUS CYBER CRIME

Adapun contoh kasus Cyber Crime yang terjadi di Indonesia adalah sebagai berikut;

1. Kasus Pencucian Uang yang Dilakukan Foshan Zebro, LTD

Terbongkar kejadian dunia maya (**Cybercrime**) berskala internasional bernilai Rp2,2 miliar.

Direktorat Tindak Pidana Ekonomi Khusus Bareskrim Polri dan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) mengungkap kasus tindak pidana pencucian uang (TPPU) berskala internasional. Kejadian dunia maya (cyber crime) yang melibatkan tiga negara yakni Indonesia, Senegal, dan China itu merugikan korban senilai Rp2,2 miliar.

Kasubdit TPPU Bareskrim Polri Kombes Pol Agung Setya mengatakan kasus ini berasal dari jual beli bawang putih secara legal antara dua perusahaan yakni Tall Fall dari Senegal dengan Jinxiang Country Huaguang Food Import-Export Co LTD dari China.

"Transaksinya benar namun uangnya hilang, tidak terbayar," kata Agung di Bareskrim Polri, Jakarta, Jumat (30/8).

Agung menjelaskan, Tall Fall selaku perusahaan importir bawang putih melakukan komunikasi dengan pihak Jinxiang melalui surat elektronik (email).

Adapun email Tall Fall elmorfall@yahoo.fr dan Jinxiang County, danica@garlic.com. Namun dalam proses pembayarannya, ada penyusup melalui email yang meminta pembayaran dilakukan melalui rekening BTN cabang ITC Mangga Dua, Jakarta, atas nama Foshan Zebro, LTD.

"Pelaku yang teridentifikasi bernama Foshan Zebro LTD ternyata memiliki email yang mirip dengan email Jinxiang County yakni danica.garliccn@yahoo.cn. Pelaku menggunakan email tersebut untuk berkomunikasi dengan pihak Tall Fall," ungkap Agung.

Pada Februari 2013, perusahaan Tall Fall membayar uang sebesar USD 45,759,50 dan USD 99,946,00 atau setara dengan Rp2,2 miliar kepada Jinxiang sebagai pelunasan pembelian bawang putih.

Namun, lanjut Agung, uang itu justru masuk ke rekening Foshan. Sempat ada upaya pengambilan uang oleh dua orang dari pihak Foshan. Namun, pihak Bank curiga lantaran keduanya tidak bisa menunjukkan identitas diri.

"Pihak Bank BTN Cabang Mangga Dua akhirnya melapor ke PPATK dan kami telusuri kasus tersebut. Pelaku hingga kini belum ditemukan," imbuhnya.

PPATK pun akhirnya meminta pihak BTN untuk membekukan rekening senilai Rp2,2 miliar itu. Sementara itu, Polisi belum dapat menangkap Foshan lantaran identitas fiktif. Diketahui, identitas KTP atas nama Foshan Zebro, LTD tidak terdata dalam data base kantor Kelurahan Pademangan Timur, Jakarta Utara. Hingga saat ini, belum diketahui keberadaan pelaku.

Pelaku akan disangkakan dengan pasal 4 UU No 15/2002 tentang TPPU yang telah diubah dengan UU No 25/2003 tentang TPPU dengan tindak pidana pokok pemalsuan Pasal 263 ayat (1) dan (2) KUHP.

2. Kasus Pembobolan Kartu Kredit di Bodyshop

Jakarta - Kepolisian mengindikasikan adanya keterlibatan jaringan internasional pada para tersangka pembobol data kartu kredit di Bodyshop, Jakarta. Hal ini mengingat alamat internet protokol (IP address) pembobol berada di luar negeri.

"Disamping gunakan program khusus, mereka ini diduga sindikat internasional. Karena setelah dilacak IP addressnya ternyata ada di Jerman, Prancis, Cina, dan Amerika," kata Kasubdit Sumdaling Ditreskimsus Polda Metro Jaya AKBP Nazli Harahap kepada wartawan di Mapolda Metro Jaya, Jakarta, Kamis (30/5/2013).

Lanjut Nazli, para pembobol data kartu kredit dan debit ini sudah beroperasi sejak tahun 2009. Mereka satu sindikat dengan pelaku pembobol kartu kredit modus offline yang pernah diungkap oleh jajaran Subdit Resmob Polda Metro Jaya, tahun lalu.

"Salah satu tersangka Andi Rubianto dia sudah divonis, lalu keluar dan melakukan aksinya lagi. Sekarang dia ditahan di Polres Pangkal Pinang untuk kasus yang sama," kata Nazli.

Subdit Sumdaling Ditreskimsus Polda Metro Jaya menangkap empat tersangka terkait pembobolan kartu kredit di Bodyshop ini. Keempat tersangka yang ditangkap yakni seorang perempuan SA alias A (36) ditangkap di Medan bersama suaminya TK alias Acuan (37), seorang lelaki berinisial KN (28) ditangkap di Sidoarjo, Jawa Tengah dan seorang laki-laki berinisial FA (36) di Sidoarjo, Jawa Tengah.

"FA merupakan residivis kasus yang sama yang pernah ditangani Resmob Polda Metro Jaya," kata Nazli lagi.

Dalam praktiknya, mereka membeli data yang sudah diretas oleh pelaku internasional melalui toko-toko yang menggunakan mesin EDC (electronic data capture). Data-data tersebut kemudian dijual di situs-situs seperti www.topdumpspro.com, www.icq.com dan www.dumps777.com.

Data yang diperoleh dari situs-situs tersebut kemudian dikloning dengan menggunakan encoder dan kartu magnetik. Tersangka lalu melapisi kartu magnetik yang sudah diisi data tersebut kemudian dibuat mirip seperti kartu aslinya.

Dalam kasus tersebut, polisi masih memburu 2 DPO yakni AC, seorang perempuan berusia 39 tahun. Ia berperan membantu SA untuk berbelanja dengan menggunakan kartu kredit yang telah dipalsukan dengan kartu kredit atau kartu debit curian.

Selain itu, polisi juga masih memburu MD, laki-laki berusia 30 tahun. Ia turut membantu FA untuk berbelanja dengan menggunakan kartu kredit yang telah dipalsukan.

Beberapa tersangka lain yang sudah diamankan oleh Polda Metro Jaya terkait kelompok ini antara lain AW, laki-laki berusia 40 tahun. Dia ditangkap pada Februari 2013 dan diproses atas keterlibatan penggunaan kartu kredit yang telah dipalsukan dengan data kartu kredit curian.

Kemudian, tersangka ER alias AS (45), telah ditangkap pada April 2013 dan diproses atas keterlibatan penggunaan kartu kredit yang telah dipalsukan dengan data kartu kredit curian di Carrefour, Bintaro.

"Saat ditangkap, 2 orang DPO berhasil melarikan diri yakni AY dan HK, dimana HK berperan memberikan mesin EDC kepada tersangka SA, yang saat ini sudah disita," tukasnya.

Sementara itu, Kepala Bidang Humas Polda Metro Jaya mengimbau kepada pengguna kartu kredit dan debit agar lebih waspada pada saat melakukan transaksi pembelian barang.

"Usahakan hindari penggesekkan kartu lebih dari satu kali atau selain dari digesek di mesin EDC milik bank yang resmi," kata dia.

Ia juga mengimbau nasabah untuk memusnahkan kartu debit atau kredit yang habis masa berlakunya dengan cara dipotong.

Pemilik merchant yang menyediakan mesin EDC juga diimbau untuk memastikan masa berlaku dan keaslian kartu yang digunakan konsumen. Pastikan juga nomor kartu yang tertera pada sales draft sesuai dengan nomor kartu yang tertera pada fisik kartu.

"Hindari penggesekan kartu diluar pada mesin EDC milik bank yang telah diotorisasi," kata dia.

Kemudian, teliti tandatangan pemegang kartu di atas sales draft dengan yang tertera pada fisik kartu. Waspada terhadap konsumen yang mengeluarkan kartu dalam jumlah yang tidak wajar.

BAB III

CYBERCLAW

A. DEFINISI

Cyberlaw dapat didefinisikan sebagai seperangkat aturan hukum yang diberlakukan untuk menanggulangi perbuatan melawan hukum yang dilakukan dengan menggunakan teknologi internet (Cybercrime).

B. JENIS-JENIS KEJAHATAN CYBER

- **Joy Computing** Adalah pemakaian komputer orang lain tanpa izin . Hal ini termasuk pencurian waktu operasi komputer.
- Hacking Adalah mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal.
- **The Trojan Horse** Manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program , menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain.
- **Data Leakage** Adalah menyangkut bocornya data keluar terutama mengenai data yang harus dirahasiakan.
- **Data Didling** Yaitu suatu perbuatan mengubah data valid atau sah dengan cara tidak sah mengubah input atau output data.
- **To Frustate Data Communication ata Diddling** Yaitu penyanyiaan data computer
- **Software Privaci** Yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI

C. ASPEK HUKUM TERHADAP KEJAHATAN CYBER

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

1. **Azas Subjective Territoriality** Azas yang menekankan bahwa keberlakuan hukum ditentukan berdasarkan tempat perbuatan dilakukan dan penyelesaian tindak pidananya dilakukan dinegara lain

2. **Azas Objective Territoriality** Azas yang menyatakan bahwa hukum yang berlaku adalah hukum dimana akibat utama perbuatan itu terjadi dan memberikan dampak yang sangat merugikan bagi Negara yang bersangkutan
3. **Azas Nasionality** Azas yang menentukan bahwa Negara mempunyai jurisdiksi untuk menentukan hukum berdasarkan kewarganegaraan pelaku
4. **Azas Protective Principle** Azas yang menekankan jurisdiksi berdasarkan kewarganegaraan korban
5. **Azas Universality** Azas ini menentukan bahwa setiap Negara berhak untuk menangkap dan menghukum para pelaku pembajakan
6. **Azas Protective Principle** Azas yang menyatakan berlakunya hukum didasarkan atas keinginan Negara untuk melindungi kepentingan Negara dari kejahatan yang dilakukan diluar wilayahnya yang umumnya digunakan apabila korban adalah Negara atau pemerintah

C. CYBERLAW DI INDONESIA

Sejak satu dekade terakhir Indonesia cukup serius menangani berbagai kasus terkait Cybercrime. Menyusun berbagai rancangan peraturan dan perundang-undangan yang mengatur aktivitas user di dunia maya. Dengan peran aktif pemerintah seperti itu, dapat dikatakan Cyberlaw telah mulai diterapkan dengan baik di Indonesia.

Berikut ini adalah beberapa kategori kasus Cybercrime yang telah ditangani dalam UU Informasi dan Transaksi Elektronik (Pasal 27 sampai dengan Pasal 35) :

27. Illegal Contents

- muatan yang melanggar kesusilaan (Pornograph)
- muatan perjudian (Computer-related betting)
- muatan penghinaan dan pencemaran nama baik
- muatan pemerasan dan ancaman (Extortion and Threats)

28. Illegal Contents

- berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik. (Service Offered fraud)
- informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan (SARA).

29. Illegal Contents

- Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman
- kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

30. Illegal Access

- Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.

- Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
- Dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

31. Illegal Interception

- Intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
- Intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.

32. Data Leakage and Espionag

Mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

33. System Interferenc

Melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

34. Misuse Of Device

Memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi cybercrime, sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi cybercrime.

35. Data Interferenc

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

Berikut ini Table Pelanggaran Di Dunia Maya (Cybercrime) dan Hukuman yang diambil dari UU Informasi dan Transaksi Elektronik Indonesia :

Tabel di atas hanya menangkap pelanggaran sampai dengan pasal 35, sedangkan dua pasal berikutnya (36 dan 37) sengaja tidak ditampilkan karena merupakan pasal tersebut membahas tentang pelanggaran turunan dari pasal-pasal sebelumnya.

E. CONTOH KASUS CYBER LAW DI INDONESIA

1. Kasus Pencemaran nama baik yang dilakukan Olga Syahputra terhadap dokter Febby Karina

Komedian dan presenter Olga Syahputra telah resmi ditetapkan sebagai tersangka oleh Polda Metro Jaya atas kasus pencemaran nama baik yang dilakukannya pada seorang dokter kecantikan bernama Febby Karina.

Mengetahui penetapan tersangka, Febby menyambut baik dan mengapresiasi kinerja pihak kepolisian yang telah bersungguh-sungguh memperhatikan laporannya tersebut.

“Sebagai korban, Dokter Febby menyambut baik penetapan tersangka dari OS. Dia merasa ini adalah jalan terbaik untuk memberikan suatu pelajaran,” ujar Malik Bawazier selaku kuasa hukum Febby di Jakarta, Kamis (26/9).

Malik sendiri sudah menduga jika Olga Syahputra bakal menjadi tersangka karena terbukti melakukan tindak pidana terhadap kliennya tersebut.

“Secara hukum terlapor atau tersangka OS jelas nyata telah melakukan serangkaian dugaan tindak pidana sebagaimana dimaksud Pasal 27 UU ITE serta Pasal 310, 311, 335 KUHP,” terang Malik.

Olga dilaporkan oleh dokter bernama Febby Karina pada 19 Juni 2013 ke Polda Metro Jaya. Olga dianggap telah melecehkan Febby karena menuduh Febby merusak rumah tangga orang lain saat tampil di acara komedi yang disiarkan secara langsung.

2. Kasus Pencemaran Nama baik yang dilakukan Dosen UI

Jakarta - Dosen FISIP Universitas Indonesia, Ade Armando ditetapkan sebagai tersangka dalam kasus dugaan pencemaran nama baik terhadap mantan Direktur Kemahasiswaan UI, Kamarudin.

Kepala Bidang Humas Polda Metro Jaya Kombes Pol Rikwanto mengatakan, Ade seyogyanya menjalani pemeriksaan sebagai tersangka di Polda hari ini, Senin (17/6/2013).

"Yang bersangkutan semestinya menjalani pemeriksaan sebagai tersangka pada hari ini. Tapi berhalangan hadir, karena masih ada sejumlah urusan di KPK," ungkap Kabid Humas Polda Metro Jaya, Kombes Pol Rikwanto.

Penyidik, kata Rikwanto, telah meminta keterangan sejumlah saksi ahli seperti ahli IT, ahli bahasa dan ahli pidana terkait kasus yang membela Ade Armando tersebut.

Rikwanto mengatakan, pihaknya akan melayangkan panggilan kedua terhadap pengkritik korupsi itu.

Ade Armando menjadi tersangka pencemaran nama baik melalui dunia maya setelah memuat artikel yang diposting di blog pribadi Ade, <http://adearmando.wordpress.com>. Dua artikel itu berjudul "Bungkamnya BEM-BEM UI: Tak Peduli, Pengecut, atau Dikadali?" dan "BEM-BEM di UI SEGERA BERTINDAK; REKTOR DAN PARA KACUNGNYA GAGAL!".

Dua artikel tersebut dimuat Ade pada 29 Januari 2012 dan 4 Maret 2012. Pada kedua artikel itu, Ade menjelaskan, dirinya tidak pernah menulis secara definitif bahwa Kamarudin korupsi. Dia hanya memaparkan adanya berbagai bentuk dugaan korupsi di UI, termasuk di dalamnya penyulitan uang beasiswa.

3. Kasus Pelanggaran Hak Cipta

Kasus pembajakan karya cipta lagu 'Cari Jodoh' yang dipopulerkan Band Wali mulai disidangkan di Pengadilan Negeri (PN) Malang, Jawa Timur, Rabu (1/5/2013).

Di sidang pertama itu, bos PT Nagaswara, Rahayu Kertawiguna, dihadirkan. Rahayu adalah bos dari label yang selama ini mendistribusikan karya-karya Faang dan kawan-kawannya itu. Selain bos PT Nagaswara, Rahayu hadir di persidangan sebagai saksi atas dugaan pembajakan yang dilakukan Malikul Akbar Atjil.

Kala dihubungi lewat telepon, Kamis (2/5/2013), Rahayu mengatakan, perbuatan yang dilakukan Atjil dengan membajak karya orang lain itu jelas merugikan. "Akan lebih merugikan lagi apabila tindakan pembajakan itu dibiarkan," ujar Rahayu. Sebagai pemilik label yang mendistribusikan lagu-lagu musisi Indonesia, termasuk artis dan penyanyi Nagaswara, Rahayu mempunyai tugas dan kewajiban untuk ikut-serta menjaga karya para artisnya itu.

Kasus lagu 'Cari Jodoh' milik Band Wali, cerita Rahayu, pihaknya semula tidak tahu

perbuatan yang dilakukan Atjil. "Jangankan memberi tahu, minta ijin memakai lagu 'Cari Jodoh-nya' Wali saja tidak dilakukan Atjil," tutur Rahayu.

Menurut Rahayu, akibat aksi pembajakan lagu 'Cari Jodoh' itu, sebagai pemegang hak cipta karya tersebut, pihaknya dirugikan Atjil sebesar Rp 1 Milyar. Dalam laporannya yang dibuat tahun 2010, Rahayu menyertakan jumlah kerugian itu.

Selama Atjil belum diputus bersalah oleh majelis hakim PN Malang, jelas Rahayu, pihak distribusi Malaysia Incitech bisa terus menjual karya lagu 'Cari Jodoh-nya' Band Wali versi Atjil tanpa ada ijin yang jelas.

Perkara tersebut dimulai ketika lagu 'Cari Jodoh' karya cipta Band Wali dibajak di Malaysia tahun 2009. Setelah dilakukan penyidikan, Polda Jawa Timur menangkap Atjil di Surabaya pada awal tahun 2013. Atjil belakangan diketahui pernah menjadi aktivis Antipembajakan. Saat ditangkap, Atjil mengaku, Malaysia Incitech sudah membeli karya lagu 'Cari Jodoh' dari Wali Band. (kin)

BAB IV

PENUTUP

A. KESIMPULAN

Di dunia ini banyak hal yang memiliki dualisme yang kedua sisinya saling berlawanan. Seperti teknologi informasi dan komunikasi, hal ini diyakini sebagai hasil karya cipta peradaban manusia tertinggi pada zaman ini. Namun karena keberadaannya yang bagai memiliki dua mata pisau yang saling berlawanan, satu mata pisau dapat menjadi manfaat bagi banyak orang, sedangkan mata pisau lainnya dapat menjadi sumber kerugian bagi yang lain, banyak pihak yang memilih untuk tidak berinteraksi dengan teknologi informasi dan komunikasi. Sebagai manusia yang beradab, dalam menyikapi dan menggunakan teknologi ini, mestinya kita dapat memilih mana yang baik, benar dan bermanfaat bagi sesama, kemudian mengambilnya sebagai penyambung mata rantai kebaikan terhadap sesama, kita juga mesti pandai melihat mana yang buruk dan merugikan bagi orang lain untuk selanjutnya kita menghindari atau memberantasnya jika hal itu ada di hadapan kita.

B. SARAN

Cybercrime adalah bentuk kejahatan yang mestinya kita hindari atau kita berantas keberadaannya. Cyberlaw adalah salah satu perangkat yang dipakai oleh suatu negara untuk melawan dan mengendalikan kejahatan dunia maya (cybercrime) khususnya dalam hal kasus cybercrime yang sedang tumbuh di wilayah negara tersebut. Seperti layaknya pelanggar hukum dan penegak hukum.

Demikian makalah ini kami susun dengan usaha yang maksimal dari tim kami, kami mengharapkan yang terbaik bagi kami dalam penyusunan makalah ini maupun bagi para pembaca semoga dapat mengambil manfaat dengan bertambahnya wawasan dan pengetahuan baru setelah membaca tulisan yang ada pada makalah ini. Namun demikian, sebagai manusia biasa kami menyadari keterbatasan kami dalam segala hal termasuk dalam penyusunan makalah ini, maka dari itu kami mengharapkan kritik atau saran yang membangun demi terciptanya penyusunan makalah yang lebih sempurna di masa yang akan datang. Atas segala perhatiannya kami haturkan terimakasih.

LAMPIRAN

Daftar Nama Kelompok:

1. Nama : Hasan Nuripno
NIM : 13121592



2. Nama : Ahmad Irsan
NIM : 13111323



3. Nama : Singgih Gustiyono Junier
NIM : 13120889



4. Nama : Rio Putra Yani
NIM : 13121500



5. Nama : Zaenal Arifin Efendi

NIM : 13121171



DAFTAR PUSTAKA

- . *Etika Profesi Teknologi dan Komunikasi, Slide; BSI.*
- . Sitompul, Josua (2012). *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana: Tatanusa.*
- <http://www.lipi.go.id/intra/informasi/1250035982.pdf>
- <http://news.detik.com/read/2013/05/30/171210/2260727/10/3/pembobol-kartu-kredit-di-bodyshop-diduga-terkait-jaringan-internasional>
- <http://www.vivaindonesia.com/2013/09/olga-syahputra-resmi-jadi-tersangka-kasus-pencemaran-nama-baik.html>
- <http://news.detik.com/read/2013/06/17/234817/2276273/10/dosen-ui-jadi-tersangka-pencemaran-nama-baik>
- <http://mundir-asror.blogspot.com/2010/12/malaysia-mengklaim-reog-ponorogo-dan.html>