

## **PENGARUH PERKEMBANGAN TEKNOLOGI TERHADAP TERJADINYA KEJAHATAN MAYANTARA (CYBERCRIME)**

**Raodia**

Universitas Sawerigading Makassar

Email : *hj\_raodia@yahoo.co.id*

### **Abstract**

*simply influence of perkembangan of technology to the happening of badness of mayantara of cybercrime that is new badness appearance which exploit growth of technology. Badness also more and more to expand and vary. But morely special causing growth of wrong technology use to [do/conduct] badness that is 1. Accessing internet which is not limited 2. small risk, 3. weak Security network system. As for way of prevention and penanggulangan of badness of or mayantara of cybercrime that is 1. Make-Up of the quality of human resource in police institution and of aparatur enforcer of law 2. Making special [code/law] or regulation for the badness of or mayantara of cybercrime.*

**Key Words:** *Technology, badness of mayantara*

### **Abstrak**

Secara sederhana pengaruh perkembangan teknologi terhadap terjadinya kejahatan mayantara atau *cybercrime* yaitu munculnya kejahatan baru yang memanfaatkan perkembangan teknologi tersebut. Kejahatan juga makin berkembang dan bervariasi. Namun, secara lebih khusus yang menyebabkan perkembangan teknologi disalah gunakan untuk melakukan kejahatan yaitu: 1. Akses internet yang tidak terbatas, 2. Resiko yang kecil, 3. Sistem keamanan jaringan yang lemah. Adapun cara pencegahan dan penanggulangan kejahatan mayantara atau *cybercrime* yaitu : 1. Peningkatan kualitas sumber daya manusia dalam institusi kepolisian dan aparatur penegak hukum. 2. Membuat peraturan atau undang-undang khusus untuk kejahatan mayantara atau *cybercrime*.

**Kata Kunci:** *Teknologi, Kejahatan Mayantara*

## **PENDAHULUAN**

Dalam kehidupan ini terdapat berbagai macam hal, baik itu benda padat, air, udara, angin, api dan lain sebagainya. Selain itu ada pula yang bernama makhluk hidup yang berupa mikroba, makhluk hidup ber-sel satu, hewan, tumbuhan manusia dan makhluk hidup lainnya. Manusia merupakan makhluk hidup yang paling sempurna dan diberi kelebihan oleh Sang Pencipta yaitu berupa akal pikiran dan juga perasaan (hati). Sedangkan makhluk hidup lain mempunyai akal pikiran dan juga hati terbatas pada tingkatan-tingkatan tertentu. Manusia bisa mengembangkan kesemuanya itu dan terus berevolusi menjadi “makhluk yang paling sempurna”. Dengan akal pikiran itu manusia bisa berpikir dan mengembangkan segala sesuatunya demi kepentingan dirinya dan orang lain.

Dari akal pikiran tersebut manusia mengembangkan sesuatu yang disebut dengan IPTEK (Ilmu Pengetahuan dan Teknologi), yang dari masa ke masa semakin maju dan berkembang. Saat ini ilmu pengetahuan dan teknologi berkembang amat cepat terutama di bidang komputer, yang sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Dari itulah timbul apa yang disebut dengan bidang informasi, yang merupakan titik sentral dalam banyak kehidupan manusia tidak terkecuali bidang hukum.

Saat ini kebutuhan manusia akan teknologi informasi tersedia dengan bebas dan tanpa batas. Namun dari keadaan tersebut disamping banyak manfaat yang diberikan kepada pemenuhan kebutuhan manusia akan informasi dalam melakukan aktivitas hidupnya juga memberikan pengaruh yang tidak baik.

Teknologi yang sebenarnya merupakan alat bantu/ekstensi kemampuan diri manusia, dewasa ini telah menjadi sebuah kekuatan otonom yang justru membelenggu perilaku dan gaya hidup kita sendiri. Dengan daya pengaruhnya yang sangat besar, karena ditopang pula oleh sistem-sistem sosial yang kuat, dan dalam kecepatan yang makin tinggi, teknologi telah menjadi pengarah hidup manusia. Masyarakat yang rendah kemampuan teknologinya cenderung tergantung dan hanya mampu bereaksi terhadap dampak yang ditimbulkan oleh kecanggihan teknologi.

Tujuan utama perkembangan IPTEK adalah perubahan kehidupan masa depan manusia yang lebih baik, mudah, murah, cepat dan aman. Perkembangan IPTEK, terutama teknologi informasi (*information technology*) seperti internet sangat menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat, baik legal maupun illegal dengan menghalalkan segala cara karena ingin memperoleh keuntungan secara “potong kompas”. Dampak buruk dari

perkembangan teknologi ini tidak dapat dihindarkan dalam kehidupan masyarakat moderen saat ini.

Pada satu sisi, perkembangan dunia IPTEK yang demikian mengagumkan itu memang telah membawa manfaat yang luar biasa bagi kemajuan peradaban umat manusia. Jenis-jenis pekerjaan yang sebelumnya menuntut kemampuan fisik yang cukup besar, kini relatif sudah bisa digantikan oleh perangkat mesin-mesin otomatis. Demikian juga ditemukannya formulasi-formulasi baru kapasitas komputer, seolah sudah mampu menggeser posisi kemampuan otak manusia dalam berbagai bidang ilmu dan aktifitas manusia. Kemajuan teknologi informasi yang serba digital membawa orang ke dunia bisnis yang revolusioner (digital revolution era) karena dirasakan lebih mudah, murah, praktis dan dinamis berkomunikasi dan memperoleh informasi.

Di sisi lain, berkembangnya teknologi informasi menimbulkan pula sisi rawan yang gelap sampai tahap mencemaskan dengan kekhawatiran pada perkembangan tindak pidana di bidang teknologi informasi yang berhubungan dengan kejahatan mayaantara atau “*cybercrime*”. Masalah kejahatan mayaantara dewasa ini sepatutnya mendapat perhatian semua pihak secara seksama pada perkembangan teknologi informasi masa depan, karena kejahatan ini termasuk salah satu *extra ordinary crime* (kejahatan luar biasa) bahkan dirasakan pula sebagai *serious crime* (kejahatan serius) dan *transnational crime* (kejahatan antar negara) yang selalu mengancam kehidupan warga masyarakat, bangsa dan negara.

Tindak pidana atau kejahatan ini adalah sisi paling buruk di dalam kehidupan moderen dari masyarakat informasi akibat kemajuan pesat teknologi dengan meningkatnya peristiwa kejahatan komputer, pornografi, terorisme digital, “perang” informasi sampah, bias informasi, hacker, cracker, dan sebagainya. Oleh karena itu tidaklah salah apabila perkembangan teknologi informasi harus diperhatikan dan diawasi dengan sebaik-baiknya, untuk mencegah timbulnya berbagai macam kejahatan yang memanfaatkan dan yang diakibatkan oleh perkembangan teknologi.

## **PEMBAHASAN**

### **A. Sejarah Perkembangan Teknologi Dan Cybercrime**

#### **1. Sejarah perkembangan teknologi**

Sejarah perkembangan teknologi informasi tidak bisa dilepaskan dari Perang dingin antara Uni Soviet dan Amerika Serikat. Uni Soviet memulai perang dingin dalam bidang teknologi dengan meluncurkan *Sputnik*. Sebagai respon yang diberikan oleh Uni Soviet, Amerika Serikat membentuk *Advanced Research Project Agency* (ARPA) pada tahun 1958. Dengan dibentuknya *Advanced*

*Research Project Agency* (ARPA) menjadikan *Departement of Devense* (DoD) Amerika Serikat memimpin dalam pemanfaatan ilmu pengetahuan dan teknologi yang diterapkan untuk kepentingan militer.

Usaha itu dilakukan Amerika didasarkan pada kekhawatiran terhadap ancaman perang nuklir yang bisa saja terjadi. Untuk itu, Amerika mengambillangkah dengan mengamankan atau melindungi data-data dan sistem komunikasi yang telah dibangun agar tidak dapat dihancurkan. Kekhawatiran tersebut mengakibatkan munculnya keinginan dikalangan militer Amerika Serikat (dibantu oleh akademisi dari berbagai universitas) untuk membuat suatu jaringan komunikasi yang dapat menghindari kehancuran data dan arsip rahasia lainnya.

Pada tahun 1965, *Anvanced Research Project Agency* (ARPA) mensponsori studi tentang *Cooperative Network or Time-Sharing Computer* untuk mengembangkan jaringan komputer. Untuk mewujudkan hal tersebut, Roberts bekerja sama dengan Thomas Merrill menghubungkan komputer TX-2 di Massachusetts (Lincoln Lab. *Massachusetts Institute of Technology* (MIT)) ke AN/FSQ-32 pada *System Development corporation* (Santa Monica, California) dengan *dial up* saluran telepon berkecepatan rendah. Inilah tonggak pertama dibangunnya *Wide-area network*.

Keberhasilan diciptakannya *Wide-area network*, maka berbagai pihak mulai berusaha mengembangkan teknologi tersebut. Sampai pada akhirnya perhatian terhadap teknologi informasi khususnya internet mulai berkembang dan menjadi semakin besar dari tahun ke tahun. Hal ini dibuktikan dengan banyaknya organisasi-organisasi baru yang didirikan dengan tujuan dengan mengembangkan teknologi tersebut.

Dari situlah awal mula berkembangnya teknologi informasi khususnya internet. Perkembangan itupun terus berkembang dari tahun ke tahun sampai sekarang, dan bahkan masih akan terus berkembang pada tahun tahun selanjutnya, baik software maupun hardwarenya.

## **2. Sejarah kejahatan mayantara atau *cybercrime***

Sejarah *cybercrime* tidaka dapat dilepas dari sejarah perkembangan teknologi. Awal mula dari munculnya kejahatan di dunia maya atau yang lebih dikenal dengan istilah "*Cybercrime*" ini dimulai pada tahun 1988. Pada tahun itu, seorang mahasiswa berhasil menciptakan sebuah *worm* atau virus yang menyerang program komputer dan mematikan sekitar 10% dari seluruh jumlah komputer di dunia yang terhubung ke internet.

Akan tetapi jauh sebelum itu sebenarnya benih-benih kejahatan di dunia maya telah ada. Dimulai pada tahun 1950-an, para mahasiswa di *Massachusetts*

*Institute of Technology* (MIT) yang memiliki rasa ingin tahu dan kepandaian untuk mengeksplorasi peralihan jaringan telepon (*the phone switching networks*) dan sistem control pada *Tech Model Railroad Club* dan menyusun komputer di *Massachusetts Institute of Technology Artificial Intelligence Laboratorium* (MIT AI Lab). Pada saat ini sebenarnya para mahasiswa dan ahli-ahli teknologi lainnya hanya bertujuan untuk mengembangkan teknologi informasi khususnya internet, dan belum ada niat untuk memanfaatkan teknologi ini untuk melakukan kejahatan. Seiring berjalannya waktu, perkembangan teknologi komputer dan teknologi informasi semakin maju dan berkembang ke seluruh negara-negara di dunia.

Pada tahun 1990 muncul sebuah gelombang baru yang lebih memanfaatkan perkembangan teknologi informasi ini untuk melakukan kejahatan. Mereka mulai menyerang situs-situs milik publik ataupun pribadi, demi mencari kesenangan atau keuntungan. Dari situlah lahir istilah *cybercrime* atau yang disebut juga sebagai kejahatan mayantara.

## **B. Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime)**

Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer, yang kemudian melahirkan piranti baru yang disebut internet. Kehadiran internet telah memunculkan paradigma baru dalam kehidupan manusia. Kehidupan berubah dari yang hanya bersifat nyata (*real*) ke realitas baru yang bersifat maya (*virtual*). Realitas yang kedua ini biasa dikaitkan dengan internet dan cyberspace.

Perkembangan Internet yang semakin hari semakin meningkat, baik perangkat maupun penggunaannya, membawa dampak positif atau pun negatif. Teknologi selain membawa keuntungan berupa semakin dipermudahnya hidup manusia, juga membawa kerugian-kerugian berupa semakin dipermudahnya penjahat untuk melakukan kejahatan. Teknologi juga memberikan pengaruh yang signifikan dalam pemahaman mengenai kejahatan terutama terhadap aliran-aliran dalam kriminologi yang menitik beratkan pada faktor manusia, baik secara lahir maupun psikologis.

Kejahatan sebenarnya telah ada sejak awal zaman, hingga sekarang. Seiring dengan perkembangan zaman bentuk-bentuk kejahatanpun semakin bervariasi. Perkembangan teknologi merupakan salah satu faktor yang dapat menimbulkan kejahatan. Seiring dengan perkembangan teknologi, maka jenis-

jenis kejahatan semakin berkembang dan bervariasi. Banyak kejahatan-kejahatan baru yang bermunculan dengan semakin berkembangnya teknologi, khususnya teknologi internet.

Kejahatan mayaantara (*cybercrime*) adalah salah satu bentuk atau dimensi baru dari kejahatan masa kini yang diakibatkan oleh perkembangan teknologi yang sangat pesat. Kejahatan ini bahkan sudah menjadi perhatian dunia internasional. Kejahatan mayaantara atau *cybercrime* merupakan salah satu sisi gelap dari kemajuan teknologi yang mempunyai dampak negatif sangat luas bagi seluruh bidang kehidupan modern saat ini.

*Cybercrime* adalah perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. *Cybercrime* sebenarnya bukan hanya menggunakan kecanggihan teknologi komputer akan tetapi juga memanfaatkan teknologi informasi dalam pengoperasiannya.

### **C. Cara Pencegahan Dan Penanggulangan Kejahatan Mayaantara Atau *Cybercrime***

Pemanfaatan dan penggunaan teknologi secara meluas, pada satu sisi membawa perubahan paradigma pada bidang kehidupan yang positif, tetapi pada sisi lain juga menimbulkan perubahan paradigma dalam studi mengenai kejahatan. Kajian kriminologi yang ada saat ini merupakan kajian terhadap kajian yang terjadi di dunia nyata. Sedangkan penggunaan dan pemanfaatan teknologi internet menimbulkan dimensi baru kejahatan, yaitu kejahatan yang terjadi di dunia maya.

Kajian kriminologi terhadap kejahatan yang terjadi di dunia maya telah berkembang seiring dengan berkembang pula kejahatan yang terjadi di dunia maya. Dari kajian-kajian itu lahirlah berbagai macam cara pencegahan dan penanggulangan terhadap kejahatan mayaantara atau *cybercrime* ini. Akan tetapi hal ini belum dapat menanggulangi maraknya kejahatan mayaantara atau *cybercrime* yang terjadi.

Sebenarnya kejahatan mayaantara atau *cybercrime* bukannya tidak bisa dicegah atau ditanggulangi, tetapi keterbatasan yang dimiliki pihak polisi kita dalam mengungkap kejahatan mayaantara atau *cybercrime* ini, yang membuat kejahatan ini belum bisa dicegah dan ditanggulangi.

Pencegahan dan penanggulangan kejahatan mayaantara atau *cybercrime*. Mengacu pada teori pre-emptif, preventif, dan represif yang dikemukakan Prof.A.S.Alam, maka ada beberapa cara yang dapat dilakukan dalam pencegahan dan penanggulangan kejahatan ini yaitu:

## 1. Mengamankan sistem

Tujuan yang nyata dari sebuah sistem keamanan adalah mencegah adanya kerusakan bagian dalam sistem karena dimasuki oleh pemakai yang tidak diinginkan. Pengamanan sistem secara terintegrasi sangat diperlukan untuk meminimalisasikan kemungkinan kerusakan tersebut. Membangun sebuah keamanan sistem harus merupakan langkah-langkah yang terintegrasi pada keseluruhan subsistemnya, dengan tujuan dapat mempersempit atau bahkan menutup adanya celah-celah *unauthorized actions* yang merugikan. Hal ini tergantung dari pemilik komputer atau jaringan komputer tersebut.

Pengamanan secara personal ini dapat dilakukan mulai dari tahap instalasi sistem sampai akhirnya menuju ke tahap pengamanan fisik dan pengamanan data. Pengamanan akan adanya penyerangan sistem melalui jaringan juga dapat dilakukan dengan melakukan pengamanan FTP, SMTP, Telnet dan pengamanan Web Server. Ada beberapa perangkat lunak yang dapat membantu memperkuat sistem keamanan, yaitu :

### *a. Internet Firewall*

Jaringan komputer yang terhubung ke Internet perlu dilengkapi dengan *internet Firewall*. *Internet Firewall* berfungsi untuk mencegah akses dari pihak luar ke sistem internal. Dengan demikian data-data yang berada dalam jaringan komputer tidak dapat diakses oleh pihak-pihak luar yang tidak bertanggung jawab. *Firewall* bekerja dengan 2 cara, yaitu :

#### (1) Menggunakan filter

*Firewall filter* menyaring komunikasi agar terjadi seperlunya saja, hanya aplikasi tertentu saja yang bias lewat dan hanya komputer dengan identitas tertentu saja yang bisa berhubungan.

#### (2) Menggunakan proxy

*Firewall proxy* berarti mengizinkan pemakai dari dalam untuk mengakses internet seluas-luasnya, namun dari luar hanya dapat mengakses satu komputer tertentu saja.

### *b. Kriptografi*

*Kriptografi* adalah seni menyandikan data. Data yang akan dikirim disandikan terlebih dahulu sebelum dikirim melalui internet. Di komputer tujuan, data tersebut dikembalikan ke bentuk aslinya sehingga dapat dibaca dan dimengerti oleh penerima. Data yang disandikan dimaksudkan agar apabila ada pihak-pihak yang

menyadap pengiriman data, pihak tersebut tidak dapat mengerti isi data yang dikirim karena masih berupa kata sandi. Dengan demikian keamanan data dapat dijaga. Ada dua proses yang terjadi dalam kriptografi, yaitu:

- 1) Proses enkripsi, proses enkripsi adalah proses mengubah data asli menjadi data sandi.
- 2) Proses dekripsi, proses dekripsi adalah proses mengembalikan data sandi menjadi data aslinya.

Data asli atau data yang akan disandikan disebut dengan plain text, sedangkan data hasil penyandian disebut cipher text. Proses enkripsi terjadi di komputer pengirim sebelum data tersebut dikirimkan, sedangkan proses dekripsi terjadi di komputer penerima sesaat setelah data diterima sehingga si penerima dapat mengerti data yang dikirim.

c. *Secure Socket Layer (SSL)*

Jalur pengiriman data melalui internet melalui banyak transisi dan dikuasai oleh banyak orang. Hal ini menyebabkan pengiriman data melalui Internet rawan oleh penyadapan. Maka dari itu, browser di lengkapi dengan *Secure Socket Layer* yang berfungsi untuk menyandikan data. Dengan cara ini, komputer-komputer yang berada di antara komputer pengirim dan penerima tidak dapat lagi membaca isi data.

2. Membuat undang-undang khusus untuk kejahatan mayantara atau *cybercrime*

Melakukan modernisasi dalam penegakan hukum merupakan hal penting, karena seiring dengan berjalannya waktu kejahatanpun terus berkembang. Walaupun sekarang sudah ada undang-undang ITE yang mengatur tentang kejahatan berteknologi, tetapi penting rasanya untuk membuat undang-undang tersendiri untuk *cybercrime*, karena tidak semua kejahatan berteknologi itu dapat dikatakan sebagai *cybercrime*. Dan yang paling penting tentunya penerapan undang-undang tersebut dengan sebaik mungkin.

3. Peningkatan sumber daya manusia

Hal ini dapat dilakukan dengan meningkatkan pemahaman serta keahlian aparaturnya penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan *cybercrime*. Hal ini akan sangat bermanfaat karena, dengan pemahamannya aparat penegak hukum tentang masalah *cybercrime* akan sangat membantu mereka dalam mengatasi dan

menanggulangnya.

4. Meningkatkan kerjasama antar negara

Kejahatan mayaantara atau *cybercrime* merupakan *transnational crime*. Bisa saja pelakunya berada di luar negeri, sedangkan kejahatannya terjadi di Indonesia. Maka kerjasama antar negara dalam upaya penanganan *cybercrime* ini perlu dilakukan.

5. Mempekerjakan para hacker

Para hacker adalah orang-orang cerdas yang memiliki keahlian khusus dalam bidang teknologi. Sebenarnya hal itu dapat dimanfaatkan oleh pemerintah atau aparat penegak hukum untuk mencegah atau mengurangi terjadinya kejahatan mayaantara atau *cybercrime* ini. Dengan mempekerjakan hacker, mereka dapat membantu memblokir situs-situs atau jaringan-jaringan dalam negeri yang ingin atau akan diserang oleh pihak lain yang tidak bertanggung jawab. Dengan kata lain, para hacker ini dipekerjakan untuk membantu mengetes dan memperkuat sistem keamanan jaringan yang ada. Sehingga tingkat keamanan terhadap jaringan internet yang ada di Indonesia bisa terus berkembang. Ini merupakan cara yang cukup berisiko untuk dilakukan oleh pemerintah atau aparat penegak hukum, karena apabila tidak dilakukan dengan baik, hal ini dapat menjadi boomerang untuk pemerintah atau aparat penegak hukum. Karena bisa saja para hacker tersebut malah mencuri atau merusak data-data dan jaringan yang ada. Oleh karena itu, maka cara yang satu ini perlu dilakukan dengan pengawasan yang baik.

## **PENUTUP**

Perkembangan teknologi informasi berada pada dua sisi yaitu sisi inovasi dan efektivitas dan sisi gelap seperti kejahatan mayaantara atau "*cybercrime*". Kemajuan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Banyak kejahatan-kejahatan baru yang bermunculan dengan semakin berkembangnya teknologi, khususnya teknologi internet. Pencegahan dan penanggulangan kejahatan mayaantara atau *cybercrime* dapat dilakukan secara pre-emptif, preventif, dan represif

## DAFTAR PUSTAKA

### Buku

- Abdul Wahid dan Mohammad Labib, 2005. *Kejahatan Mayantara (cybercrime)*. Refika Aditama. Bandung
- Agus Raharjo. 2002. *Cybercarime , Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Citra Aditya Bakti. Bandung
- Amiruddin dan Zainal Asikin. 2003. *Pengantar Metode Penelitian dan Penulisan Hukum*. P.T Raja Grafindo Persada. Jakarta
- Andi Hamzah. 1987. *Aspek-Aspek Pidana Di Bidang Komputer*. Sinar Grafika. Jakarta
- A.S. Alam, 2010. *Pengantar Kriminologi*. Pustaka Refleksi. Makassar
- Barda Nawawi, 2005. *Tindak Pidana Mayantara, Perkembangan Kajian Cybercrime di Indonesia*. P.T Raja Grafindo Persada. Jakarta
- B.Bosu. 2002. *Sendi-Sendi Kriminologi*. Usana Offset. Surabaya
- Departemen Pendidikan Nasional. 2002. *Kamus Besar Bahasa Indonesia Edisi Ketiga*. Balai Pustaka. Jakarta
- Edmon Makarim. 2003. *Kompilasi Hukum Telematika*. P.T Raja Garfindo Persada. Jakarta
- Gorys Keraf. 1970. *Komposisi, Sebuah Pengantar Kemahiran Berbahasa*. Nusa Indah. Jakarta
- Judhariksawan, 2005. *Pengantar Hukum Telekomunikasi*. P.T Raja Garfindo Persada. Jakarta
- Maskun. 2010. *Kejahatan Siber , Suatu Pengantar*.
- Soejono dan Abdurrahman. 1997. *Metode Penelitian Hukum*. P.T Rineka Cipta. Jakarta
- Zainal Abidin Farid. 2007. *Hukum Pidana I*. Sinar Grafika. Jakarta

### Laporan dan Tulisan Ilmiah

- Ahmad Mu'arif,dkk, 2009. *Cybercrime: Modus, Penyebab, dan Penanggulangannya, Makalah*. Sekolah Tinggi Manajemen Informatika dan Ilmu Komputer El Rahma. Yogyakarta
- Dewi Lestari. 2004. *Kejahatan Dan Komputer* . LKHT-UI, Jakarta