**MAKALAH *INFORMATION SYSTEM SECURITY***

***CYBERLAW* DI INDONESIA**

**TUGAS**

****

**Oleh:**

**NAMA : Rut Ramayanti**

**NIM : 170030892**

**JENJANG STUDI : STRATA SATU (S1)**

**PROGRAM STUDI : SISTEM INFORMASI**

**INSTITUT TEKNOLOGI DAN BISNIS**

**ITB STIKOM BALI**

**2020**

# BAB I PENDAHULUAN

## Latar Belakang

Perkembangan Teknologi Informasi dan Komunikasi (TIK) telah mengubah perilaku masyarakat secara global. Dalam pemanfaatannya, perkembangan TIK telah memudahkan manusia untuk memperoleh informasi, dan komunikasi yang dilakukan menjadi tanpa batas (*borderless*), baik antar sesama manusia maupun antar negara di dunia. Perkembangan tersebut juga menyebabkan perubahan sosial, ekonomi, dan budaya secara signifikan dengan cepat.

Internet merupakan salah satu sarana yang dihasilkan oleh perkembangan teknologi informasi dan komunikasi. Hingga muncul berbagai *network* dan *information company* yang akan memperjualbelikan berbagai fasilitas, bermacam jaringan, dan berbagai basis data informasi tentang berbagai hal yang dapat diakses oleh pengguna internet.

TIK saat ini menjadi pedang bermata dua, khususnya internet, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan, dan peradaban manusia, sekaligus menjadi sarana efektif yang dapat mengakibatkan perbuatan untuk melanggar hukum. Mereka sengaja masuk ke dalam web suatu instansi/lembaga tertentu kemudian melakukan kejahatan didalamnya, baik itu mencuri data ataupun mengacaukan data, bahkan tidak sedikit mencuri uang melalui internet seperti

1

pembobolan nomor pin ATM. Kejahatan-kejahatan seperti inilah yang disebut sebagai *Cybercrime*. Banyak jenis dan ragam *cybercrime* namun semuanya pada dasarnya sama yakni melakukan tindakan kejahatan di dunia maya atau internet.

Istilah (*cybercrime*) saat ini merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya dan tindakan kejahatan yang menggunakan komputer. Ada ahli yang menyamakan antara tindak kejahatan (*cybercrime*) dengan tindak kejahatan komputer, dan ada ahli yang membedakan di antara keduannya. Meskipun belum ada kesepahaman mengenai definisi kejahatan teknologi informasi, namun ada kesamaan pengertian universal mengenai kejahatan komputer. Bila seseorang menggunakan komputer atau bagian dari jaringan komputer tanpa seizin yang berhak, tindakan tersebut sudah tergolong pada kejahatan komputer. Keragaman aktivitas kejahatan yang berkaitan dengan komputer atau jaringan komputer sangat besar dan telah menimbulkan perbendaharaan bahasa baru, misalnya *hacking*, *cracking*, *virus*, *time bomb*, *worm*, *troyan horse*, *logical bomb*, *spamming*, *hoax*, dan lain-lain sebagainya. Masing-masing memiliki karakter dan dampak berbeda.

## Rumusan Masalah

Melihat latar belakang yang telah dikemukakan, maka beberapa masalah yang dapat penyusun rumuskan dan akan dibahas dalam makalah ini adalah :

1. Pengertian *cybercrime* dan *cyberlaw*;
2. Ciri-ciri dan jenis *cybercrime*;
3. Faktor pendorong peningkatan *cybercrime*;
4. Dampak dan penanggulangan *cybercrime;*
5. Kelebihan dan kekurangan UU ITE di Indonesia;
6. Contoh kasus *cybercrime*.

## Maksud dan Tujuan

Setelah mempelajari makalah ini, diharapkan agar para pembaca dan kami selaku penyusun mampu memahami tentang pengertian, jenis, ciri-ciri, faktor kejahatan dibidang TIK atau yang lebih dikenal dengan istilah *cybercrime*, dan mempelajari tentang undang-undang yang berlaku di Indonesia tentang *cybercrime*. Penulisan makalah ini juga dimaksudkan untuk mengenalkan *blog* yang penyusun buat, [http://frame2cyber.blogspot.co.id/,](http://frame2cyber.blogspot.co.id/) yang juga merupakan rangkaian tugas dari

matakuliah Etika Profesi Teknologi Informasi dan Komunikasi. *Blog* tersebut adalah hasil dari apa yang telah kami pelajari di kampus, media internet, dan buku-buku yang berkaitan dengan *cybercrime* dan *cyberlaw*.

Sedangkan tujuan penulisan tugas ini adalah sebagai syarat kelulusan pada matakuliah Etika Profesi Teknologi Informasi dan Komunikasi pada Jurusan Manajemen Informatika di Akademi Manajemen Informatika dan Komputer Bina Sarana Informatika (AMIK BSI).

# BAB II PEMBAHASAN

* 1. ***Cybercrime* dan *Cyberlaw***

*Cybercrime* merupakan salah satu tindak kriminal atau tindak kejahatan melalui dukungan perkembangan TIK berupa internet, karena aktivitas *cybercrime* biasanya merugikan pihak korban. Kerugian yang biasa dialami adalah perusakan atau pencurian data-data dalam sistem yang tak ternilai harganya.

*Cyberlaw* adalah kumpulan peraturan perundang-undangan yang mengatur tentang berbagai aktivitas manusia di *cyberspace* (dengan memanfaatkan teknologi informasi). *Cyberlaw* sendiri merupakan istilah yang berasal dari *Cyberspace*. *Cyberspace* berakar dari kata latin *Kubernan* yang artinya menguasai atau menjangkau. Karena *cyberspace* yang akan menjadi objek dari *cyberlaw*.

Sistem hukum Indonesia secara sah mengakui adanya peristiwa hukum yang terjadi di dunia maya (*cyber*). Hal tersebut merupakan suatu yang positif dalam rangka menuju perdagangan bebas dan globalisasi perdagangan lintas wilayah maupun lintas negara, tanpa perlu sesi tatap muka atau rumitnya birokrasi perdagangan yang ada.

*Cyberlaw* secara international digunakan untuk istilah hukum yang terkait dengan pemanfaatan TIK. Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*), hukum dunia maya (*virtual world law*),

4

dan hukum mayantara. Pada ranah penerapan hukumnya, ternyata banyak menimbulkan reaksi pro dan kontra pada praktiknya. Hal tersebut muncul seiring dengan bermunculan korban yang dijerat dengan UU ITE.

* 1. **Ciri-Ciri dan Jenis *Cybercrime***
     1. **Ciri-ciri *cybercrime***

Tindak pidana *cybercrime* dalam memiliki beberapa ciri khusus, antara lain sebagai berikut.

1. *Non-Violence* (tanpa kekerasan);
2. Sedikit melibatkan kontak fisik (*minimize of physical contact*);
3. Menggunakan peralatan (*equipment*) dan teknologi;
4. Memanfaatkan jaringan telematika global (telekomunikasi, media, dan informatika).

Ciri *cybercrime* ke-3 dan ke-4 yang menggunakan peralatan dan teknologi, serta memanfaatkan jaringan, jelas bahwa *cybercrime* dapat dilakukan di mana saja, kapan saja, dan kepada siapa saja tanpa batas. Keadaan ini mengakibatkan pelaku, korban, tempat kejadian, dan akibat yang ditimbulkan bisa terjadi di beberapa negara sekaligus.

* + 1. **Jenis *cybercrime***

1. *Cybercrime* berdasarkan karakteristik
   1. *Cyberpiracy* adalah penggunaan teknologi komputer untuk mencetak ulang *software* atau informasi dan mendistribusikannya melalui jaringan komputer.
   2. *Cybertrespass* adalah penggunaan teknologi komputer untuk meningkatkan akses pada sistem komputer sebuah organisasi atau individu, dan *website* yang dilindungi dengan *password*.
   3. *Cybervandalism* adalah penggunaan teknologi komputer untuk membuat program yang mengganggu proses transmisi informasi elektronik dan menghancurkan data di komputer.
2. Jenis *cybercrime* berdasarkan aktivitasnya
   1. *Ilegal Contents* (Konten Tidak Sah)

Merupakan 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.

* 1. *Data Forgery* (Pemalsuan Data)

Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai *scriptless document* melalui internet. Contoh kejahatan ini pada dokumen-dokumen *e-commerce* dengan membuat seolah- olah terjadi salah ketik yang pada akhirnya akan menguntungkan pelaku.

* 1. *Cyber Spionase* (Mata-Mata)

Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan memata-matai pihak lain, dengan memasuki sistem jaringan komputer (*computer network system*) sasaran.

* 1. *Data Theft* (Mencuri Data)

Kegiatan memperoleh data komputer secara tidak sah, baik untuk digunakan sendiri ataupun untuk diberikan kepada orang lain.

* 1. *Misuse of Devices* (Menyalahgunakan Peralatan Komputer)

Dengan sengaja dan tanpa hak, memproduksi, menjual, berusaha memperoleh untuk digunakan, diimpor, diedarkan atau cara lain, sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan melawan hukum lainnya.

* 1. *Hacking* dan *Cracker*

Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs *web*, menyebarkan virus, hingga pelumpuhan target sasaran.

* 1. DoS (*Denial of Services*)

*Dos attack* merupakan serangan yang bertujuan melumpuhkan target (*hang*,

*crash*) sehingga tidak dapat memberikan layanan.

* 1. *Cybersquatting* dan *Typosquatting*

*Cybersquatting* merupakan sebuah kejahatan yang dilakukan dengan cara mendaftarkan *domain* nama perusahaan orang lain, dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun *typosquatting* adalah kejahatan dengan membuat *domain* plesetan yaitu *domain* yang mirip dengan nama *domain* orang lain.

* 1. *Hijacking*

*Hijacking* merupakan salah satu bentuk kejahatan yang melakukan pembajakan hasil karya orang lain.

* 1. *Cyber Terorism*

*Cyber terorism* adalah tindakan mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer.

* 1. *Unauthorized Access to Computer System and Service*

Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin. Biasanya pelaku kejahatan (*hacker*) melakukannya dengan maksud sabotase ataupun pencurian informasi penting.

* 1. *Ilegal Access* (Akses Tanpa Ijin ke Sistem Komputer)

Tanpa hak dan dengan sengaja mengakses secara tidak sah terhadap seluruh atau sebagian sistem komputer, dengan maksud untuk mendapatkan data komputer atau maksud-maksud tidak baik lainnya, atau berkaitan dengan sistem komputer yang dihubungkan dengan sistem komputer lain.

* 1. **Faktor Pendorong Peningkatan *Cybercrime***

Banyak hal yang mampu menjadi faktor pendorong peningkatan *cybercrime*, antara lain :

1. Kesadaran hukum masyarakat

Kesadaran hukum masyarakat Indonesia dalam merespon aktivitas *cybercrime*

masih sangat kurang. Hal ini disebabkan oleh kurangnya pemahaman dan

pengetahuan (*lack of information*) masyarakat terhadap jenis kejahatan

*cybercrime*.

1. Faktor keamanan

Rasa aman tentunya akan dirasakan oleh pelaku kejahatan (*cybercrime*) pada saat sedang menjalankan aksinya. Hal ini dikarenakan internet lazim digunakan di tempat-tempat yang relatif tertutup, seperti di rumah, kamar, warung internet (warnet), tempat kerja, perpustakaan, dll. Aktivitas di tempat-tempat tersebut sulit untuk diketahui oleh pihak luar dan mengakibatkan saat pelaku melakukan aksinya para pihak luar jarang mengetahuinya.

1. Faktor penegak hukum

Faktor penegak hukum sering kali mejadi penyebab maraknya kejahatan *cybercrime*. Hal ini dilatarbelakangi masih sedikitnya aparat penegak hukun yang memahami seluk beluk teknologi informasi (internet), sehingga pada saat pelaku tindak pidana ditangkap, aparat penegak hukum mengalami kesulitan untuk menemukan alat bukti yang dapat dipakai menjerat pelaku, apalagi jika kejahatan yang dilakukan memiliki sistem pengoperasian yang sangat rumit.

* 1. **Dampak dan Penanggulangan *Cybercrime***

Kejahatan di dunia maya sudah pasti memiliki kerugian-kerugian yang dirasakan oleh korbannya. Kerugian-kerugian yang ditimbulkan *cybercrime* diantaranya sebagai berikut :

1. Pencemaran nama baik.
2. Kehilangan sejumlah data sehingga menyebabkan kerugian yang tak ternilai

harganya terutama data yang bersifat sangat rahasia dan penting.

1. Kerusakan data akibat ulah *cracker* yang merusak suatu sistem komputer, sehingga kinerja suatu lembaga yang bersangkutan menjadi kacau.
2. Kehilangan materi yang cukup besar akibat ulah *carder* yang berbelanja dengan kartu kredit atas identitas milik korban.
3. Rusaknya *software* dan program komputer akibat ulah seseorang dengan menggunakan virus komputer.

*Cybercrime* merupakan sebuah fenomena kejahatan yang sangat merugikan sehingga pelaku kejahatannya harus dihukum sesuai kadar kejahatannya. Indonesia adalah salah satu negara yang membuat Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) untuk para pelaku *cybercrime*. Penerapan UU ITE diharapkan dapat menghilangkan atau paling tidak meminimalkan kasus-kasus *cybercrime* di Indonesia. Diharapkan pula agar undang-undang ini secara maksimal mampu memberikan efek jera kepada para pelaku *cybercrime*, sehingga para pelaku akan berpikir dua kali untuk melakukan kejahatannya mengingat sanksi yang diberikan tidak bisa dianggap ringan.

Berikut beberapa contoh yang dapat dilakukan terkait dengan upaya pencegahan terhadap *cybercrime*.

1. Untuk menanggulangi masalah *Denial of Services* (DoS), pada sistem dapat dilakukan dengan memasang *firewall* dengan *Instrusion Detection System* (IDS) dan *Instrussion Prevention System* (IPS) pada *router*.
2. Untuk menanggulangi masalah virus pada sistem dapat dilakukan dengan

memasang anti virus dan anti *spyware* dengan *upgrading* dan *updating* secara periodik.

1. Untuk menanggulangi pencurian *password* dilakukan proteksi *security system*

terhadap *password* atau perubahan *password* secara berkala.

## Kelebihan dan Kekurangan UU ITE di Indonesia

1. Kekurangan UU ITE
   1. UU ITE sangat membatasi hak kebebasan berekspresi, mengeluarkan pendapat dan dapat menghambat kreativitas masyarakat dalam bermain internet, terutama pada pasal 27 ayat (1), Pasal 27 ayat (3), Pasal 28 ayat (2), dan Pasal 31 ayat (3) ini sangat bertentangan pada UUD 1945 pasal 28 tentang kebebasan berpendapat. Pada pasal 16 disebutkan penyelenggara sistem elektronik wajib memenuhi persyaratan dalam mengopersikan sistem elektronik, persyaratan yang dikemukakan masih kurang jelas. Pada pasal 27 tentang perbuatan yang dilarang yaitu pada pasal 1 dan 2 muatan yang melanggar kesusilaan dan muatan perjudian tidak dijelaskan bagaimana standar kesusilaan dan definisi suatu perjudian.
   2. Beberapa yang masih terlewat, kurang lugas dan perlu didetailkan dengan peraturan dalam tingkat lebih rendah dari UU ITE adalah :
      1. *Spamming*, baik untuk email spamming maupun masalah penjualan data pribadi oleh perbankan, asuransi, dsb.
      2. *Virus* dan *worm* komputer (masih implisit di Pasal 33), terutama untuk pengembangan dan penyebarannya.
      3. Kemudian juga tentang kesiapan aparat dalam implementasi UU ITE.
   3. UU ITE masih rentan terhadap pasal karet, atau pasal-pasal yang intepretasinya bersifat subjektif/individual.
2. Kelebihan UU ITE
   1. UU ITE dapat mengantisipasi kemungkinan penyalahgunaan internet yang merugikan. Contohnya pembobolan situs-situs tertentu milik pemerintah dan transaksi elektronik, seperti bisnis lewat internet dan dapat meminimalisir adanya penipuan. Pada pasal 2, UU ITE berlaku terhadap orang-orang yang tinggal di Indonesia maupun di luar Indonesia ini dapat menghakimi dan menjerat orang-orang yang melanggar hukum di luar Indonesia.
   2. UU ITE tidak hanya membahas situs porno atau masalah asusila. Total ada 13 Bab dan 54 Pasal yang mengupas bagaimana aturan hidup di dunia maya dan transaksi yang terjadi didalamnya.
   3. **Contoh Kasus *Cybercrime***

Berikut ini adalah beberapa contoh kasus yang berkaitan dengan UU ITE dan *cybercrime*, yang terjadi di Indonesia dalam beberapa tahun terakhir.

## Kasus 1 :

Dosen Universitas Indonesia (UI), Ade Armando, ditetapkan sebagai tersangka oleh Subdit *Cyber Crime* Ditreskrimsus Polda Metro Jaya karena postingannya di media sosial. Postingan tersebut ditulis Ade pada tahun 2015 lalu, namun baru pada tahun 2017 ia ditetapkan sebagai tersangka. Kasus ini

bermula dari laporan seorang warga bernama Johan Khan yang melaporkan Ade pada tahun 2016. Dalam laporan yang dilayangkan oleh Johan Khan, Ade dianggap telah menistakan agama berdasarkan Pasal 156A KUHP. Namun penyidik baru menemukan unsur pidana dalam perkara tersebut berdasarkan Pasal 28 ayat 2 UU Nomor 19 tahun 2016 dengan hukuman 5 tahun penjara. Ade disangkakan melakukan penghasutan berbau SARA melalui media sosial.

Namun pada Februari 2017, penyidik Subdit *Cyber Crime* Ditreskrimsus Polda Metro Jaya menerbitkan Surat Perintah Penghentian Penyelidikan (SP3) kasus dugaan penghasutan berbau SARA dengan tersangka Ade Armando. Ade menyambut gembira keputusan polisi menerbitkan SP3. Ade mengatakan, polisi tidak menemukan pelanggaran pidana dalam tulisan di akun jejaring sosial miliknya beberapa tahun lalu.

## Kasus 2 :

Perkataan penyanyi dangdut Inul Daratista di akun media sosialnya, terkait tuduhan terhadap ulama yang berperilaku 'merusak moral' berbuntut panjang. Inul dilaporkan oleh Advokat Peduli Ulama ke Polisi akibat tulisannya tersebut. Wakil Ketua Advokat Cinta Tanah Air (ACTA), Novel Bamukmin, menilai Inul pantas dijerat Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). "Inul pantas di jerat pasal 310-311 KUHP dan UU ITE pasal 28," ujarnya kepada *republika.co.id*, Selasa (28/3).

Sebelumnya tulisan Inul di akun instagramnya menyebut pihak-pihak yang bersurban bisa 'mojok' bersama wanita sambil main *sex skype*. Perkataan Inul tersebut kemudian berujung laporan ke polisi karena Inul dianggap melanggar

UU ITE oleh beberapa pihak.

## Kasus 3 :

Situs penjualan tiket *online*, *tiket.com* diretas oleh seorang remaja, SH alias Haikal (19) beserta MKU (19), AI (19), dan NTM (27) hingga menelan kerugian mencapai Rp 4 miliar. Setelah menangkap para tersangka, Mabes Polri terus melakukan pengembangan penyidikan. Rekan-rekan Haikal memberikan kesaksian bahwa ada 4.600 situs yang pernah dibuka Haikal. "Ini pemain baru. Tiga berdomisili di Balikpapan, Haikal di Pulau Jawa," kata Brigadir Jenderal Rikwanto, Kepala Biro Penerangan Masyarakat Polri, Rabu (5/4).

Direktur Tindak Pidana Siber Bareskrim Polri Brigjen Fadil Imran melalui keterangannya menyebut, cara pelaku membobol situs *tiket.com* yakni melakukan ilegal akses *server* Citilink dengan menggunakan *user name* dan *password* milik travel agen *tiket.com*. Pelaku mendapatkan kode *booking* tiket pesawat untuk memesan sejumlah tiket. Setelah mendapatkan kode *booking*, Haikal bersama tim menjual kembali tiket tersebut melalui *facebook*.

Para pelaku dijerat dengan Pasal 46 Ayat (1), (2), dan (3) juncto Pasal 30

ayat (1), (2), dan (3) dan/atau Pasal 51 Ayat (1) dan (2) junto Pasal 35 dan/atau Pasal 36 Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan/atau Pasal 363 KUHP dan/atau Pasal 3, Pasal 5, dan Pasal 10 Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang.

## Kasus 4 :

Ketua Umum Partai Persatuan Indonesia (Perindo), Hary Tanoesoedibjo, lewat kuasa hukumnya melaporkan media *online*, *tirto.id*, dengan tuduhan melakukan fitnah dan pencemaran nama baik ke Kepolisian Daerah Metro Jaya. Laporan tersebut diterima Polda Metro Jaya dengan kasus dugaan pencemaran nama baik melalui media elektronik, dan diancam dengan Pasal 310 KUHAP atau Pasal 311 KUHP dan atau Pasal 27 Ayat 3 Jo Pasal 45 A Ayat 2 UU RI Nomor 19 Tahun 2016 tentang ITE.

## Kasus 5 :

Serangan masif yang disebabkan oleh *ransomeware WannaCrypt* atau *WannaCry* diprediksi telah menginfeksi 100 ribu komputer di hampir 150 negara di dunia. Atas kejadian ini, Microsoft kabarnya turut meminta tanggung jawab pemerintah Amerika Serikat. *Ransomeware* dibuat berdasarkan alat atau tool ekspolitasi yang bernama "Eternal Blue" milik NSA yang pada akhirnya diretas hacker berkode *Shadow Brokers* dan kemudian disebarkan melalui *github*.

*Ransomeware WannaCry* memudahkan penggunanya untuk mengambil alih kendali atas perangkat Windows lawas yang sistemnya sudah tidak diperbarui. *Ransomeware WannaCry* juga telah memasuki Indonesia dan menyerang sistem pada Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais di Jakarta (13/5). Sistem tersebut terkena *malicious software* yang polanya adalah mengunci komputer dan mengenkripsi semua data, sehingga komputer tidak dapat dibuka kecuali pengguna komputer tadi mengirimkan ‘tebusan’ senilai USD 300 dengan mata uang Bitcoin atau setara dengan Rp. 6,9 milyar kepada pemilik virus.

# BAB III PENUTUP

## Kesimpulan

Berdasarkan pembahasan pada bab-bab sebelumnya, maka penyusun menarik kesimpulan tentang kenakalan remaja, yaitu sebagai berikut.

1. *Cybercrime* adalah segala bentuk kejahatan di dalam dunia maya atau di internet.
2. *Cybercrime* sangat merugikan pihak korban, karena data-data yang penting dan rahasia dapat diambil.
3. Kejahatan *cybercrime* dapat dilakukan oleh siapa saja dan dibutuhkan pembuktian yang cukup kuat untuk menangkap para pelakunya.
4. Berbagai upaya telah dilakukan pemerintah dalam menanggulangi *cybercrime*, dengan membuat undang-undang tentang tindak pidana *cybercrime*.

## Saran

Saran yang mungkin dapat penyusun sampaikan untuk beberapa pihak yang terkait masalah *cybercrime*, yaitu:

1. Kepada pemerintah agar lebih tegas dan membuat undang-undang yang lebih terperinci untuk menangani berbagai kasus *cybercrime*.
2. Kepada para pakar IT, agar mampu membuat program pengamanan data lebih optimal, sehingga kasus-kasus kejahatan dunia maya dapat diminimalkan.

16

17

1. Kepada teman-teman mahasiswa supaya janganlah menggunakan ilmu yang kita miliki untuk melakukan kejahatan di internet.