

# **TUGAS KEBIJAKAN, ETIKA DAN HUKUM TI**

## **KONSTRUKSI DASAR HUKUM CYBER**

**Pandangan dan Kebijakan Hukum Terhadap Pelanggaran Privasi dan  
Keamanan di Internet (Privacy and Security on the internet)**



**NAMA : FATHIR MA'RUF**

**NIM :13917213**

**Angkatan IX**

**Program Pascasarjana Teknik Informatika**

**Fakultas Teknik Industri**

**Universitas Islam Indonesia**

**2014**

## KATA PENGANTAR

**Ass... Wr... Wb..**

Puji syukur kehadirat tuhan yang maha kuasa, yang telah memberikan rahmad dan hidayahnya sehingga penulis dapat menyelesaikan makalah yang berjudul **“Pandangan dan Kebijakan Hukum Terhadap Pelanggaran Privasi dan Keamanan di Internet (Privacy and Security on the internet)”** tepat pada waktunya.

Penulis menyadari bahwa daalam pembuatan dan penulisan makalah ini sangat jauh dari kesempurnaan dan begitu banyak bentuk kekurangan, oleh karena itu penulis akan menerima kritik dan saran yang bersifat membangun dari berbagai pihak untuk kebaikan dan kesempurnaan makalah/laporan ini.

Besar harapan penulis semoga tulisan ini dapat memberikan manfaat kepada semua pihak yang berkepentingan dalam pengembangan ilmu pengetahuan, khususnya mahasiswa Fakultas Teknik Industri, jurusan Teknik Informatika Universitas Islam Indonesia.

Demikian yang dapat penulis sampaikan, mohon maaf atas beberapa kesalahan yang dilakukan dalam upaya penulisan makalah ini,

Terimakasih.

**Yogyakarta, 27 Mei 2014**

**Penulis**

## DAFTAR ISI

Halaman sampul	1
Kata Pengantar	2
Daftar Isi	3

### BAB I PENDAHULUAN

1.1. Latar Belakang	4
1.2. Rumusan Masalah	6
1.3. Tujuan	6
1.4. Metode Kajian	6

### BAB II TINJAUAN PUSTAKA

2.1. Definisi <i>CyberLaw</i>	7
2.2. Pengertian <i>Cybercrime</i>	9
2.3. Pengertian <i>Privasi</i> menurut para tokoh	9
2.4. Pengertian secara umum	10
2.5. Jenis <i>Cybercrime</i> yang dianggap sebagai pelanggaran privasi	11
2.6. UU yang berkaitan dan membahas tentang <i>CyberLaw</i>	12
2.7. Implementasi <i>Cyberlaw</i> di Indonesia	13
2.8. Aspek penting dalam UU ITE	13

### BAB III PEMBAHASAN

3.1. Contoh kasus dan jenis kejahatan yang dianggap sebagai bentuk pelanggaran privasi dan keamanan di internet ( <i>privacy and security on the internet</i> )	14
3.2. Pandangan dan kebijakan hukum terhadap pelanggaran privasi dan keamanan di internet ( <i>privacy and security on the internet</i> )	19

### BAB IV PENUTUP

4.1. Kesimpulan	27
4.2. Saran	27

### DAFTAR PUSTAKA

# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

Perkembangan teknologi informasi khususnya internet semakin pesat, hal ini tentu akan berpengaruh terhadap segala aspek kehidupan baik pengaruh positif maupun negatif. Berbagai kemudahan yang ditawarkan internet merupakan salah satu pengaruh positif dalam perkembangan internet masa kini, namun hal itu tidak bisa dipisahkan dengan keinginan pihak-pihak lain yang memiliki kepentingan sendiri dengan tujuan merugikan pengguna internet lain, Sebagian kegiatan tersebut ada yang bersifat pidana atau biasa kita kenal dengan kejahatan online, Hal inilah yang melatarbelakangi penulis untuk mengangkat pembahasan ini.

Dengan adanya kejahatan-kejahatan dan kendala-kendala hukum di bidang teknologi informasi, saat ini telah lahir suatu rezim hukum baru yang dikenal dengan hukum cyber, istilah hukum cyber diartikan sebagai padanan kata *Cyber Law*, yang saat ini secara internasional digunakan untuk istilah hukum yang terkait dengan pemanfaatan teknologi informasi.

Istilah lain yang juga digunakan adalah hukum teknologi informasi (*law of information technology*) hukum dunia maya (*virtual world law*) dan hukum mayantara, istilah-istilah tersebut lahir mengingat kegiatan internet dan pemanfaatan teknologi informasi berbasis virtual, dan berikut ini akan dijelaskan tentang beberapa **aspek hukum Cyberlaw yaitu:** (Bambang sutiyoso, SH, M.Hum: 2014).

1. *E-Commerce*
2. *Trademark/Domain*
3. Privasi dan keamanan di internet (Privacy and Security on the internet)
4. Hak Cipta (Copyright)
5. Pencemaran nama baik (Defamation)
6. Pengaturan isi (Content Regulation)
7. Penyelesaian Perselisihan (Dispute Settlement)

Selain beberapa aspek hukum, *cyberlaw* juga memiliki beberapa Pro Kontra dalam Penerapan CyberLaw yaitu sebagai berikut:

- Munculnya kejahatan di internet pada awalnya terjadi pro kontra terhadap penerapan hukum yang harus dilakukan.
- Hal ini dikarenakan saat itu sangat sulit untuk menjerat secara hukum kepada para pelakunya karena alasan yang menjadi kendala seperti berikut ini :
  1. Sifat kejahatannya bersifat maya
  2. Lintas Negara
  3. Dan sulitnya menemukan pembuktian
- Munculnya pro kontra terhadap pertanyaan bisa atau tidaknya system hukum tradisional mengatur aktivitas-aktivitas di internet, yang memiliki karakteristik tersebut :
  1. Karakteristik aktivitas di internet yang bersifat lintas batas, sehingga tidak lagi tunduk pada batasan teritorial
  2. System hukum traditional (*the existing law*) yang justru bertumpu pada batasan-batasan teritorial dianggap tidak cukup memadai untuk menjawab persoalan-persoalan hukum yang muncul akibat aktivitas di internet.

Berikut ini terdapat beberapa kelompok pendapat terkait dengan penerapan *CyberLaw*:

1. Secara total menolak setiap usaha untuk membuat aturan hukum bagi aktivitas-aktivitas di internet yang didasarkan atas system hukum yang konvensional
2. Penerapan system hukum konvensional untuk mengatur aktivitas-aktivitas di internet sangat mendesak untuk dilakukan.
3. Sintesis dari kedua kelompok diatas, yaitu bahwa aturan hukum yang akan mengatur mengenai aktivitas di internet harus dibentuk secara evolutif dengan cara menerapkan prinsip-prinsip *common law* secara hati hati dengan menitik beratkan kepada aspek tertentu dalam aktivitas *cyberspace* yang menyebabkan ke khasan dalam transaksi di internet

#### **Pendekatan alternative UU *Cybercrime***

- Pendapat kedua kelompok di atas mendorong diajukanya tiga alternative pendekatan dalam penyediaan perundang-undangan yang mengatur masalah kriminalitas teknologi informasi yaitu:

1. Dibuat suatu undang-undang khusus yang mengatur masalah tindak pidana di bidang teknologi informasi
  2. Memasukan materi kejahatan teknologi informasi kedalam amandemen KUHP yang saat ini sedang di godok oleh tim department kehakiman dan HAM
  3. Melakukan amandemen terhadap semua undang-undang yang diperkirakan akan berhubungan dengan pemanfaatan teknologi informasi.
- Alternative yang digunakan dalam pembaharuan hukum pada bidang TIK di Indonesia adalah dengan ditertibkannya UU No. 11 tahun 2008 tentang informasi dan transaksi elektronik
  - Adanya UU, diharapkan dapat memberikan kepastian hukum dalam bidang TIK, terutama terkait dengan aspek pidana dan keperdataanya.

## **1.2. Rumusan Masalah**

Dari uraian latar belakang di atas maka perumusan masalah dalam penulisan ini adalah sebagai berikut:

1. Bagaimanakah contoh kasus dan jenis kejahatan yang dianggap sebagai bentuk pelanggaran privasi dan keamanan di internet.
2. Bagaimana pandangan dan kebijakan hukum terhadap pelanggaran privasi dan keamanan di internet (*privacy and security on the internet*).

## **1.3. Tujuan**

Adapun yang menjadi tujuan dalam penulisan makalah ini adalah sebagai berikut:

1. Untuk menjelaskan Bagaimanakah contoh kasus dan jenis kejahatan yang dianggap sebagai bentuk pelanggaran privasi dan keamanan di internet.
2. Untuk menjelaskan Bagaimana pandangan dan proses kebijakan penegakan hukum terhadap pelaku tindak pidana pelanggaran privasi dan keamanan di internet.

## **1.4. Metode Kajian**

Metode kajian yang digunakan penulis dengan library research, yaitu dengan mencari data-data via internet dan buku-buku terkait dengan masalah *cybercrime*, dan beberapa masalah yang terkait dengan hukum di Indonesia.

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **2.1. Definisi *Cyber Law***

*Cyber Law* adalah aspek hukum yang ruang lingkungannya 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, *Cyber Law* sendiri merupakan istilah yang berasal dari *Cyberspace Law*.

Perkembangan *Cyber Law* di Indonesia sendiri belum bisa dikatakan maju, Hal ini diakibatkan oleh belum meratanya pengguna, internet di seluruh Indonesia Berbeda dengan Amerika Serikat yang menggunakan telah internet untuk memfasilitasi seluruh aspek kehidupan mereka, Oleh karena itu, perkembangan hukum dunia maya di Amerika Serikat pun sudah sangat maju. Landasan fundamental di dalam aspek yuridis yang mengatur lalu lintas internet sebagai hukum khusus, di mana terdapat komponen utama yang meng-cover persoalan yang ada di dalam dunai maya tersebut, yaitu:

- Yurisdiksi hukum dan aspek-aspek terkait. Komponen ini menganalisa dan menentukan keberlakuan hukum yang berlaku dan diterapkan di dalam dunia maya itu.
- Landasan penggunaan internet sebagai sarana untuk melakukan kebebasan berpendapat yang berhubungan dengan tanggung jawab pihak yang menyampaikan, aspek accountability, tanggung jawab dalam memberikan jasa online dan penyedia jasa internet (internet provider), serta tanggung jawab hukum bagi penyedia jasa pendidikan melalui jaringan internet.
- Aspek hak milik intelektual di mana ada aspek tentang patent, merek dagang rahasia yang diterapkan, serta berlaku di dalam dunia cyber.
- Aspek kerahasiaan yang dijamin oleh ketentuan hukum yang berlaku di masing-masing yurisdiksi negara asal dari pihak yang mempergunakan atau

memanfaatkan dunia maya sebagai bagian dari sistem atau mekanisme jasa yang mereka lakukan.

- Aspek hukum yang menjamin keamanan dari setiap pengguna dari internet.
- Ketentuan hukum yang memformulasikan aspek kepemilikan didalam internet sebagai bagian dari pada nilai investasi yang dapat dihitung sesuai dengan prinsip-prinsip keuangan atau akuntansi.
- Aspek hukum yang memberikan legalisasi atas internet sebagai bagian dari perdagangan atau bisnis usaha.

Berdasarkan faktor-faktor di atas, maka kita akan dapat melakukan penilaian untuk menjustifikasi sejauh mana perkembangan dari hukum yang mengatur sistem dan mekanisme internet di Indonesia. Walaupun belum dapat dikatakan merata, namun perkembangan internet di Indonesia mengalami percepatan yang sangat tinggi serta memiliki jumlah pelanggan atau pihak yang mempergunakan jaringan internet terus meningkat sejak paruh tahun 90-an. Salah satu indikator untuk melihat bagaimana aplikasi hukum tentang internet diperlukan di Indonesia adalah dengan banyak perusahaan yang menjadi provider untuk pengguna jasa internet di Indonesia. Perusahaan-perusahaan yang memberikan jasa provider di Indonesia sadar atau tidak merupakan pihak yang berperan sangat penting dalam memajukan perkembangan *Cyber Law* di Indonesia dimana fungsi-fungsi yang mereka lakukan seperti:

- Perjanjian aplikasi rekening pelanggan internet;
  - Perjanjian pembuatan desain home page komersial;
  - Perjanjian reseller penempatan data-data di internet server;
  - Penawaran-penawaran penjualan produk-produk komersial melalui internet;
  - Pemberian informasi yang di-update setiap hari oleh home page komersial;
  - Pemberian pendapat atau polling online melalui internet.
- Fungsi-fungsi di atas merupakan faktor dan tindakan yang dapat digolongkan sebagai tindakan yang berhubungan dengan aplikasi hukum tentang cyber di Indonesia. Oleh sebab itu ada baiknya di dalam perkembangan selanjutnya, setiap pemberi jasa atau pengguna internet dapat terjamin. Maka hukum tentang internet perlu dikembangkan serta



dikaji sebagai sebuah hukum yang memiliki disiplin tersendiri di Indonesia.

*\*dikutip dari <http://abangs03.wordpress.com/2011/10/22/hello-world/>*

## **2.2. Pengertian Cybercrime**

Cybercrime = computer crime DAN Computer crime:

- “any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution”
- “any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of data”
- “Kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara illegal”.

*Cybercrime* dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi.

## **2.3. Pengertian Privasi Menurut Para Tokoh**

Privasi merupakan suatu hal yang sangat penting baik bagi individu maupun lembaga atau instansi untuk berhadapan dan berinteraksi dengan individu lain atau lembaga lain. Salah dalam menyampaikan informasi yang memiliki kemungkinan bernilai confidential, classified dan rahasia tidak dapat dipungkiri akan menyebabkan kerugian baik material maupun non material. Apalagi jika sifat informasi tersebut merupakan rahasia berisi peta kekuatan dan strategi yang akan dirancang menghadapi persaingan dengan produk kompetitor, terlebih lagi jika rahasia tersebut berkaitan dengan organisasi. Kalau berkaitan dengan informasi pribadi yang tidak ingin dibagi dan diketahui oleh umum, namun sudah terlanjur tersebar dan diketahui oleh khalayak luas, kejadian ini akan menjadi sangat krusial dan mungkin dapat membahayakan posisi dan kredibilitas yang bersangkutan.

1. Craig Van Slyke dan France Belanger: Kemampuan seseorang untuk mengatur informasi mengenai dirinya sendiri.
2. Alan Westin: Hak dari masing-masing individu untuk menentukan sendiri kapan, bagaimana, dan untuk apa penggunaan informasi mengenai mereka dalam hal berhubungan dengan individu lain.

## 2.4. Pengertian Secara Umum

Kerahasiaan pribadi (Bahasa Inggris: *privacy*) adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka. Privasi kadang dihubungkan dengan anonimitas walaupun anonimitas terutama lebih dihargai oleh orang yang dikenal publik. Privasi dapat dianggap sebagai suatu aspek dari keamanan.

Hak pelanggaran privasi oleh pemerintah, perusahaan, atau individual menjadi bagian di dalam hukum di banyak negara, dan kadang, konstitusi atau hukum privasi. Hampir semua negara memiliki hukum yang, dengan berbagai cara, membatasi privasi, sebagai contoh, aturan pajak umumnya mengharuskan pemberian informasi mengenai pendapatan. Pada beberapa negara, privasi individu dapat bertentangan dengan aturan kebebasan berbicara, dan beberapa aturan hukum mengharuskan pemaparan informasi publik yang dapat dianggap pribadi di negara atau budaya lain.

Privasi dapat secara sukarela dikorbankan, umumnya demi keuntungan tertentu, dengan risiko hanya menghasilkan sedikit keuntungan dan dapat disertai bahaya tertentu atau bahkan kerugian. Contohnya adalah pengorbanan privasi untuk mengikut suatu undian atau kompetisi; seseorang memberikan detail personalnya (sering untuk kepentingan periklanan) untuk mendapatkan kesempatan memenangkan suatu hadiah. Contoh lainnya adalah jika informasi yang secara sukarela diberikan tersebut dicuri atau disalahgunakan seperti pada pencurian identitas.

Privasi sebagai terminologi tidaklah berasal dari akar budaya masyarakat Indonesia. Samuel D Warren dan Louis D Brandeis menulis artikel berjudul "Right to Privacy" di Harvard Law Review tahun 1890. Mereka seperti halnya Thomas Cooley di tahun 1888 menggambarkan "Right to Privacy" sebagai "Right to be Let Alone" atau secara sederhana dapat diterjemahkan sebagai hak untuk tidak di usik dalam kehidupan pribadinya. Hak atas Privasi dapat diterjemahkan sebagai hak dari setiap orang untuk melindungi aspek-aspek pribadi kehidupannya untuk dimasuki dan dipergunakan oleh orang lain (Donald M Gillmor, 1990 : 281). Setiap orang yang merasa privasinya dilanggar memiliki hak untuk mengajukan gugatan yang dikenal dengan istilah Privacy Tort. Sebagai

acuan guna mengetahui bentuk-bentuk pelanggaran Privasi dapat digunakan catatan dari William Prosser yang pada tahun 1960 memaparkan hasil penelitiannya terhadap 300 an gugatan privasi yang terjadi. Pembagian yang dilakukan Proses atas bentuk umum peristiwa yang sering dijadikan dasar gugatan Privasi yaitu dapat kita jadikan petunjuk untuk memahami Privasi terkait dengan media.

## **2.5. Jenis *Cybercrime* yang di anggap sebagai pelanggaran privasi**

Berdasarkan jenis aktivitas yang dilakukannya, *cybercrime* dapat digolongkan menjadi beberapa jenis sebagai berikut:

### **1. Illegal Contents**

kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh realnya adalah pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya, seperti penyebaran pornografi.

### **2. Data Forgery**

Kejahatan yang dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini bisaanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database. Kejahatan ini bisaanya ditujukan pada dokumen-dokumen e-commerce dengan membuat seolah-olah terjadi "salah ketik" yang pada akhirnya akan menguntungkan pelaku karena korban akan memasukkan data pribadi dan nomor kartu kredit yang dapat saja disalah gunakan.

### **3. Cyber Espionage, Sabotage, and Extortion**

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

#### 4. Cyberstalking

Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer.

#### 5. Hacking and Cracker

Istilah hacker bisaanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya, Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut cracker, Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif.

#### 6. Hijacking

Merupakan kejahatan melakukan pembajakan hasil karya orang lain.

#### 2.6. UU yang berkaitan dan membahas tentang *CyberLaw*

- UU No. 8 tahun 1997 Tentang *Dokumen perusahaan*
- UU No. 30 Tahun 200 Tentang Rahasia Dagang
- UU No. 31 Tahun 2000 Tentang Design industry
- UU No. 14 Tahun 2001 Tentang Paten
- UU No. 15 Tahun 2001 Tentang Merek
- UU No. 19 Tahun 2002 Tentang Hak cipta
- UU No. 32 Tahun 2002 Tentang Penyiaran
- UU No. 11 Tahun 2008 Tentang *Informasi dan transaksi elektronik, dll*

#### 2.7. Implementasi *CyberLaw* di Indonesia

*CyberLaw* dibuat dengan tujuan untuk mendukung ketertiban pemanfaatan teknologi informasi yang di gunakan oleh orang berkewarganegaraan Indonesia, dan atau badan hukum yang berkependudukan di Indonesia, orang asing, atau badan hukum asing yang melakukan kegiatan atau transaksi dengan orang, atau badan hukum yang lahir dan berkependudukan di Indonesia dan hak asasi manusia (HAM)

##### Tentang UU No. 11 Tahun 2008

- Setelah melalui perjalanan panjang sejak tahun 1999, RUU ITE disetujui dalam rapat paripurna DPR menjadi UU ITE pada tanggal 25 Maret 2008, dan disahkan oleh presiden serta mulai berlaku tanggal 21 April 2008
- UU ITE terdiri dari 13 BAB dan 54 Pasal yang merupakan rezim hukum baru untuk mengatur aktifitas cyberspace di Indonesia.

## **2.8. Aspek penting dalam UU ITE**

- Aspek Yuridiksi
- Aspek Pembuktian Elektronik
- Aspek Informasi dan perlindungan konsumen
- Aspek tanda tangan elektronik dan pengamanannya
- Aspek penyelenggaraan Sertifikasi elektronik
- Aspek Transaksi Elektronik
- Aspek nama domain
- Aspek Perlindungan Privacy
- Aspek peran pemerintah dan masyarakat
- Aspek Perlindungan kepentingan umum
- Aspek Perbuatan yang dilarang

## BAB III PEMBAHASAN

### 2.1. Contoh kasus dan jenis kejahatan yang dianggap sebagai bentuk pelanggaran privasi dan keamanan di internet (*privacy and security on the internet*)

#### A. Pelanggaran Privasi

Salah satu dampak negatif dari era informasi adalah pelanggaran privasi, Pelanggaran privasi dapat diartikan sebagai pembeberan informasi tanpa memperhatikan kode etik yang semestinya, Salah satu contoh kasusnya adalah mempublikasikan dokumen elektronik seperti gambar, video, tulisan, dll tanpa menggunakan aturan dan sopan santun yang layak. **Berikut ini adalah beberapa hal yang berkaitan dengan contoh kasus terhadap pelanggaran privasi antara lain:**

1. Mengirim dan mendistribusikan dokumen yang bersifat pornografi, menghina, mencemarkan nama baik, dll. Contohnya pernah terjadi pada Prita Mulyasari yang menurut pihak tertentu telah mencemarkan nama baik karena surat elektronik yang dibuat olehnya.
2. Melakukan penyadapan informasi. Seperti halnya menyadap transmisi data orang lain.
3. Melakukan pengadaan tanpa ijin pihak yang berwenang. Bisa juga disebut dengan hijacking. Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Contoh yang sering terjadi yaitu pembajakan perangkat lunak (Software Piracy).
4. Melakukan pembobolan secara sengaja ke dalam sistem komputer. Hal ini juga dikenal dengan istilah *Unauthorized Access*. Atau bisa juga diartikan sebagai kejahatan yang terjadi ketika seseorang memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan pemilik sistem jaringan komputer yang dimasukinya. Jelas itu sangat melanggar privasi pihak yang berkepentingan (pemilik sistem jaringan komputer). Contoh kejahatan ini adalah *probing* dan *port*.
5. Memanipulasi, mengubah atau menghilangkan informasi yang sebenarnya. Misalnya data *forgery* atau kejahatan yang 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 berbasis web database. Contoh lainnya adalah *Cyber Espionage*, *Sabotage*, dan *Extortion*. *Cyber Espionage* merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain dengan memasuki system jaringan Komputernya. *Sabotage* dan *Extortion* merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

Pelanggaran privasi di era informasi seperti hal-hal di atas tentu dapat merugikan orang/pihak terkait, Belum ada aturan yang baku untuk menangani masalah tersebut. Walau ada juga kasus-kasus berkaitan dengan itu yang telah dibawa ke meja hukum, Kode etik dan etika profesi sangat diperlukan agar pelanggaran privasi tidak lagi terjadi, Kesadaran individu tentang kode etiklah yang paling diharapkan agar pihak-pihak terkait tak dirugikan.

## **B. Contoh Pelanggaran Privasi .**

**berikut ini adalah contoh pelanggaran privasi di internet :**

- Menerima email penawaran dari orang yang tidak dikenal sebelumnya.
- Menerima surat fisik mengenai penawaran berbagai hal atau terkadang undian.
- Data transaksi pembelian barang digunakan oleh orang lain untuk menawarkan barang tertentu
- Menerima telepon dari orang yang tidak dikenal sebelumnya mengenai penawaran suatu barang.
- Pesan berantai dari seseorang yang tidak dikenal .

## **CONTOH KASUS TERHADAP PELANGGARAN PRIVASI SEBAGAI BERIKUT :**

- **Contoh kasus 1 :** Google telah didenda 22.5 juta dolar Amerika karena melanggar privacy jutaan orang yang menggunakan web browser milik Apple, Safari. Denda atas Google kecil saja dibandingkan dengan pendapatannya di kuartal kedua. (Credit: Reuters) Denda itu, yang diumumkan oleh Komisi Perdagangan Federal Amerika Serikat (FTC), adalah yang terbesar yang pernah dikenakan atas sebuah perusahaan yang melanggar persetujuan sebelumnya dengan komisi tersebut. Oktober lalu Google menandatangani sebuah persetujuan yang mencakup janji untuk tidak menyesatkan konsumen tentang praktik-praktik privacy. Tapi Google dituduh menggunakan cookies untuk secara rahasia melacak kebiasaan dari jutaan orang yang menggunakan Safari internet browser milik Apple di iPhone dan iPads. Google mengatakan, pelacakan itu tidak disengaja dan Google tidak mengambil informasi pribadi seperti nama, alamat atau data kartu kredit. Google sudah setuju untuk membayar denda tadi, yang merupakan penalti terbesar yang pernah dijatuhkan atas sebuah perusahaan yang melanggar instruksi FTC.
- **Contoh kasus 2 :** Contoh kasus diatas sangat mungkin untuk terjadi pula di pertelevisian Indonesia. Momentum pelanggaran Privasi dapat berlangsung pada proses peliputan berita dan dapat pula terjadi pada penyebarluasan (broadcasting) nya. Dalam proses peliputan, seorang objek berita dapat saja merasakan derita akibat tindakan reporter yang secara berlebihan mengganggu wilayah pribadi nya. Kegigihan seorang reporter mengejar berita bisa mengakibatkan terlewatnya batas-batas kebebasan gerak dan kenyamanan pribadi yang sepatutnya tidak di usik. Hak atas kebebasan bergerak dan melindungi kehidupan pribadi sebenarnya telah disadari oleh banyak selebritis Indonesia. Beberapa cuplikan infotainment menggambarkan pernyataan-pernyataan cerdas dari beberapa selebriti kita tentang haknya untuk melindungi kehidupan pribadinya. Dalam menentukan batas-batas Privasi dimaksud memang tidak terdapat garis hukum yang tegas sehingga masih bergantung pada subjektifitas pihak-pihak yang terlibat. Dalam proses penyebarluasan



(penyiaran), pelanggaran Privasi dalam bentuk fakta memalukan (embarrassing fact) anggapan keliru (false light) lebih besar kemungkinannya untuk terjadi. Terlanggar atau tidaknya Privasi tentunya bergantung pada perasaan subjektif si objek berita. Subjektifitas inilah mungkin yang mendasari terjadinya perbedaan sikap antara PARFI dan PARSI yang diungkap diatas dimana disatu pihak merasa prihatin dan dipihak lain merasa berterimakasih atas pemberitaan-pemberitaan infotainment.

sebagai contoh :

1. Pelanggaran terhadap privasi Tora sudiro, hal ini terjadi Karena wartawan mendatangi rumahnya tanpa izin dari Tora.
  2. Pelanggaran terhadap privasi Aburizal bakrie, hal ini terjadi karena publikasi yang mengelirukan pandangan orang banyak terhadap dirinya.
  3. Pelanggaran terhadap privasi Andy Soraya dan bunga citra lestari, hal ini terjadi karena penyebaran foto mereka dalam tampilan vulgar kepada publik
- **Contoh kasus 3** : Apple iPhone berada di tengah kontroversi yang cukup besar awal tahun ini, di mana ketika para peneliti mengungkapkan adanya bug di sistem operasi perangkat iOS yang menyimpan data lokasi GPS dalam folder yang terlindungi. Informasi tersebut memungkinkan aparat penegak hukum, detektif swasta dan pihak lainnya menggunakan iPhone untuk melacak pengguna perangkat di setiap tempat di mana mereka berada, karena setiap saat iPhone melakukan ping ke sebuah menara seluler untuk GPS koordinat lalu disimpan pada perangkatnya. Ketika berita ini keluar, banyak protes yang mencuat dari kalangan pemilik smartphone tersebut. Meskipun pada saat itu banyak pengguna yang protes, sebuah survei baru dari Adaptive Mobile menemukan bahwa 65 persen dari pemilik iPhone sebetulnya tidak menyadari fakta bahwa aplikasi yang mereka download ke perangkat mereka berpotensi melanggar privasi mereka. Sebagian pengguna lainnya sebenarnya telah tertangkap karena menggunakan aplikasi untuk mengumpulkan informasi mengenai kebiasaan pengguna dan mengirimkan mereka kembali ke pengembang

untuk tujuan pengiklanan. Survei Adaptive Mobile global ini dilakukan terhadap 1.024 pengguna iPhone.

Aplikasi berbahaya pada smartphone memang bukan kasus yang benar-benar baru. Pada sistem operasi Google Android pun pernah terdapat virus dan aplikasi yang mampu mencuri data. Untuk iPhone sendiri, Proses pemeriksaan perusahaan Apple cukup ketat sebelum aplikasi disetujui untuk dijual di App Store, namun salah satu ahli keamanan mencatat bahwa masih banyak kemungkinan pengeksploitasian lubang keamanan di iOS yang berpotensi adanya pembajakan iPhone. Sementara AdaptiveMobile menemukan bahwa sebagian besar pengguna iPhone tidak menyadari ancaman keamanan potensial pada perangkat mereka, ia juga menemukan bahwa 7 dari 10 pengguna cenderung menganggap pelanggaran privasi yang notabene merupakan sebuah kejahatan.

### **C. Dasar Gugatan Pelanggaran Privasi.**

#### **Adapun peristiwa-peristiwa itu yakni :**

##### **1. Intrusion,**

yaitu tindakan mendatangi atau mengintervensi wilayah personal seseorang tanpa diundang atau tanpa ijin yang bersangkutan. Tindakan mendatangi dimaksud dapat berlangsung baik di properti pribadi maupun diluarnya. Kasus terkait hal ini pernah diajukan oleh Michael Douglas dan istrinya Catherine Zeta Jones yang mempermasalahkan photo pesta perkawinan mereka yang diambil tanpa ijin oleh seorang Paparazi. Kegusaran Douglas timbul karena sebenarnya hak eksklusif pengambilan dan publikasi photo dimaksud telah diserahkan kepada sebuah majalah ternama.

##### **2. Public disclosure of embarrassing private facts ,**

yaitu penyebarluasan informasi atau fakta-fakta yang memalukan tentang diri seseorang. Penyebarluasan ini dapat dilakukan dengan tulisan atau narasi maupun dengan gambar. Contohnya, dalam kasus penyanyi terkenal Prince vs Out Magazine, Prince menggugat karena Out Magazine mempublikasi photo setengah telanjang Prince dalam sebuah pesta dansa. Out Magazine selamat dari gugatan ini karena pengadilan

berpendapat bahwa pesta itu sendiri dihadiri sekitar 1000 orang sehingga Prince dianggap cukup menyadari bahwa tingkah polahnya dalam pesta tersebut diketahui oleh banyak orang.

3. **Publicity which places some one false light in the public eye,**  
yaitu publikasi yang mengelirukan **pandangan** orang banyak terhadap seseorang. Clint Eastwood telah menggugat majalah The National Enquirer karena mempublikasi photo Eastwood bersama Tanya Tucker dilengkapi berita "Clint Eastwood in love triangle with Tanya Tucker". Eastwood beranggapan bahwa berita dan photo tersebut dapat menimbulkan pandangan keliru terhadap dirinya.
4. **Appropriation of name or likeness,**  
yaitu penyalahgunaan nama atau kemiripan seseorang untuk kepentingan tertentu. Peristiwa ini lebih terkait pada tindakan pengambilan keuntungan sepihak atas ketenaran seorang selebritis. Nama dan kemiripan si selebritis dipublikir tanpa ijin.

## **2.2. Pandangan dan kebijakan hukum terhadap pelanggaran privasi dan keamanan di internet (*privacy and security on the internet*)**

Acuan hukum di Negara Indonesia terkait dalam melindungi dan membahas tentang privasi yaitu bersumber pada Undang-Undang Teknologi Informasi ayat 19 yang menyatakan bahwa privasi adalah *hak individu untuk mengendalikan penggunaan informasi tentang identitas pribadi baik oleh dirinya sendiri atau oleh pihak lainnya*. Bahkan diatur pula sanksi bila terjadi pelanggaran terhadap privasi yaitu Hukuman dan Pidana tentang privasi pada Pasal 29: Pelanggaran Hak Privasi yang berbunyi;

***“Barang siapa dengan sengaja dan melawan hukum memanfaatkan Teknologi Informasi untuk mengganggu hak privasi individu dengan cara menyebarkan data pribadi tanpa seijin yang bersangkutan, dipidana penjara paling singkat 3 (tiga) tahun dan paling lama 7 (tujuh) tahun”.***

Berikut ini adalah ketentuan yang telah mengatur terkait dengan perbuatan yang melanggar hak dan privasi di internet yang telah di atur dalam UU ITE.

## **BAB VII UU ITE**

### **PERBUATAN YANG DILARANG**

#### **Pasal 27**

- (1) 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 yang melanggar kesusilaan.
- (2) 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 perjudian.
- (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.

#### **Pasal 28**

- (1) Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.
- (2) Setiap Orang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA).

### **Pasal 29**

Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.

### **Pasal 30**

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
- (2) Setiap Orang 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.
- (3) Setiap Orang 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.

### **Pasal 31**

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan 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.

- (3) Kecuali intersepsi sebagaimana dimaksud pada ayat (1) dan ayat (2), intersepsi yang dilakukan dalam rangka penegakan hukum atas permintaan kepolisian, kejaksaan, dan/atau institusi penegak hukum lainnya yang ditetapkan berdasarkan undang-undang.
- (4) Ketentuan lebih lanjut mengenai tata cara intersepsi sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Pemerintah.

### **Pasal 32**

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
- (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak.
- (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

### **Pasal 33**

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

### **Pasal 34**

- (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki:
  - a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33;

- b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.
- (2) Tindakan sebagaimana dimaksud pada ayat (1) bukan tindak pidana jika ditujukan untuk melakukan kegiatan penelitian, pengujian Sistem Elektronik, untuk perlindungan Sistem Elektronik itu sendiri secara sah dan tidak melawan hukum.

### **Pasal 35**

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.

### **Pasal 36**

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 34 yang mengakibatkan kerugian bagi Orang lain.

### **Pasal 37**

Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.

Sedangkan untuk ketentuan pidana terhadap pelanggaran dari beberapa pasal diatas telah diatur dalam Ketentuan pidana UU ITE seperti yang akan diapaparkan berikut ini:

## **BAB XI UU ITE**

### **KETENTUAN PIDANA**

#### **Pasal 45**

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 28 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

#### **Pasal 46**

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).



**Pasal 47**

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

**Pasal 48**

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah).
- (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).

**Pasal 49**

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

**Pasal 50**

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

**Pasal 51**

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

- (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

## **Pasal 52**

- (1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok.
- (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.
- (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.
- (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.

## **BAB IV**

### **PENUTUP**

#### **4.1. Kesimpulan**

Dari apa yang telah dibahas terkait pelanggaran hak dan privasi di internet yang telah di tentukan dalam UU ITE sesuai yang telah dijelaskan sebelumnya dianggap sebagai tindak kejahatan pidana pelanggaran hak dan privasi yang dilakukan dan memanfaatkan media internet dapat diproses secara hokum karena telah bahas dan ditentukan dalam pasal 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, terkait perbuatan yang dilarang dalam UU ITE, sedangkan pasal 45, 46, 47, 48, 49, 50, 51, 52 adalah pasal dalam UU ITE yang membahas terkait dengan tindak pidana yang telah dijelaskan dalam pasal sebelumnya.

#### **4.2. Saran**

- Aparat kepolisian secara terus menerus melakukan operasi dalam penegakan hokum untuk menindak lanjuti terkait tindak pidana pelanggaran privasi di internet dengan melibatkan beberapa pihak yaitu dengan melibatkan warnet dan tokoh masyarakat.
- Peningkatkan kemampuan aparat kepolisian dibidang teknologi informasi dalam pengungkapan tindak pidana pelanggaran privasi di internet.
- Pemanfaatan media masa untuk mengetahui dan mengungkap fenomena pelanggaran hak dan privasi yang menggunakan media internet.

## DAFTAR PUSTAKA

- Bambang sutyoso, SH, M.Hum, *Etika & hukum teknologi informasi*, 2014
- Helmy Prasetyo Yuwinanto, *Kebijakan Informasi Dan Privacy*, 2009
- Satjipto Rahardjo, Hukum Progresif: Hukum yang Membebaskan, Jurnal Hukum Progresif, Vol. 1, No. 1, April 2005
- SR. Sianturi, Asas-asas Hukum Pidana Di Indonesia dan Penerapannya, Alumni Ahaem-Petehaem, Jakarta, 1996
- Moeljanto, Kitab Undang-Undang Hukum Pidana, Bumi Aksara, Yogyakarta, 2006
- Muladi, Barda Nawawi Arief, Teori-Teori dan Kebijakan Pidana, Alumni, Bandung, 1992
- Muladi, Kapita Selekta Hukum Pidana, Badan Penerbit Universitas Diponegoro, Semarang, 1995
- <http://ihsanirawan001.blogspot.com/2013/10/contoh-study-kasus-cyber-crime-dan.html> (diakses pada: pukul 11.45 tanggal 05/27/2014).
- [http://etikaprofesikelompok5.blogspot.com/p/blog-page\\_4111.html](http://etikaprofesikelompok5.blogspot.com/p/blog-page_4111.html) (diakses pada: pukul 10.45 tanggal 05/29/2014).
- <http://dianaandisah.wordpress.com/contoh-kasus-penyalahgunaan-teknologi-informasi/> (diakses pada: pukul 15.45 tanggal 05/29/2014).
- <http://abanqs03.wordpress.com/2011/10/22/hello-world/> (diakses pada: pukul 13.45 tanggal 05/29/2014).