BAB IV

PEMBAHASAN

A. Gambaran Umum Tentang *Spamming* di Indonesia

1. Tindak Pidana *Spamming*

Spamming adalah suatu jenis tindakan yang dapat dikatakan sebagai salah satu dari kejahatan dalam dunia maya, walaupun banyak yang menganggap bahwa tindakan *spamming* tersebut tidak merugikan tetapi dalam kenyataannya tidak sedikit yang merasa di rugikan oleh tindakan *spamming* ini, walaupun di dalam prakteknya jarang sekali orang yang melaporkan tindakan *spamming* apabila telah menjadi korban tindakan *spamming*.

Sebelum membahas mengenai *spamming*, terlebih dahulu membahas mengenai sistem keamanan dari dunia maya terlebih dahulu. Dunia maya merupakan suatu dimensi yang sangat luas dan tidak terbatas dimana semua orang dapat melakukan interaksi secara bebas, hal ini disebabkan oleh sifat dari dunia maya itu sediri yaitu anonimitas (*anonymity*) sehingga setiap orang dapat saling berinteraksi di dalam dunia maya tanpa harus mengetahui usia, jenis kelamin, agama dan sebagainya. Interaksi tersebut tidak hanya dalam ruang ligkup percakapan antar orang perorangan tetapi juga terdapat aktivitas yang lain misalnya jual beli, berbagi informasi, dan sebagainya. Sehingga dengan sifatnya yang anonim maka tidak menutup kemungkinan atau beresiko dapat terjadi penyalahgunaan terhadap aktifitas-aktifitas lain dalam

dunia maya misalnya jual beli maupun berbagi informasi. Khususnya dalam hal berbagi informasi, kegiatan ini menjadi salah satu kegiatan yang paling utama dalam berinteraksi di dunia maya, mulai dari penyebaran berita, tempat bersosialisasi maupun yang paling sering adalah di gunakan untuk menawarkan barang-barang tertentu.

Banyak cara yang dapat di gunakan untuk menawarkan barang-barang di dalam dunia maya dari menawarkan secara langsung dari situs-situs internet maupun blok-blok tersendiri sampai menawarkan barang dengan cara menyebarkan email secara meluas dan bertubi-tubi, *spamming* sendiri memiliki arti sebagai penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi para pengguna web yang biasanya datang secara bertubi-tubi dan sering tidak dikehendaki oleh penerimanya, sehingga dapat dikatakan bahwa *spamming* termasuk dalam kegiatan penyalahgunaan dari aktifitas dunia maya tersebut, *spam* dalam Wikipedia di bedakan menjadi beberapa bentuk *spam* yang biasanya banyak terjadi, yaitu:

1) Surat Elektronik

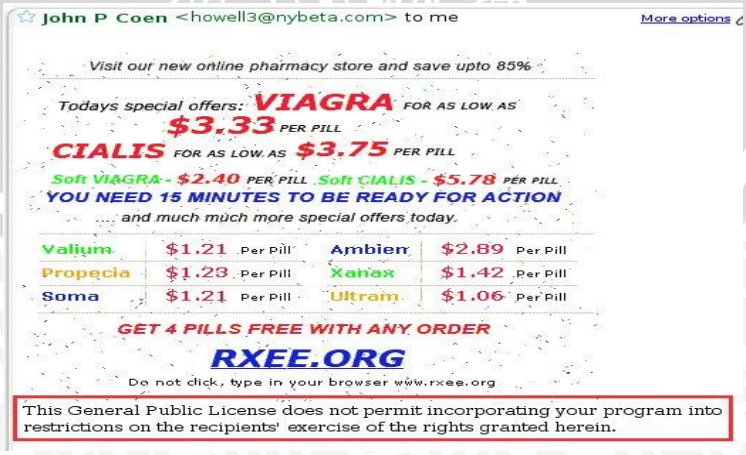
Spam surat elektronik, yang dikenal sebagai surat elektronik massal yang tidak diminta (*unsocialicited bulk email* atau UBE), junk mail, atau surat elektronik komersial yang tidak diminta (*unsocialited commercial email* atau UCE), adalah praktik pengiriman pesan dalam surat elektronik yang tidak diinginkan, sering bersifat komersial, dan masuk dalam jumlah besar kepada siapa pun. *Spam* di surat elektronik mulai menjadi masalah

ketika internet dibuka untuk umum pada pertengahan 1990-an. Pertumbuhan yang pesat dari tahun ke tahun hingga saat ini telah menghasilkan *spam* 80% – 85% dari seluruh surat elektronik di dunia. Tekanan untuk membuat *spam* surat elektronik telah berhasil di beberapa negara hukum. *Spammer*s mengambil keuntungan dari fakta ini dengan sering mengirimkan *spam* ke negara lain sehingga tidak akan membuat mereka bermasalah secara hukum.

Dalam perkembangannya, *spam* surat elektronik saat ini dikirim melalui "jaringan zombie", jaringan virus yang terinfeksi di komputer pribadi baik rumah atau di kantor di seluruh dunia. Hal ini mempersulit upaya untuk mengontrol penyebaran *spam*, seperti banyak kasus di mana *spam* tidak berasal dari *spammer*s. Munculnya banyak *spam* yang bukan dari *spammer*s dikarenakan pembuat perangkat perusak, *spammer*s, dan penipu keuangan belajar satu sama lain sehingga memungkinkan mereka membentuk berbagai jenis kerja sama.

Gambar 4.1

Contoh iklan promosi *spamming*



Sumber: Data Sekunder diolah, 2012

2) Telepon genggam

Handphone atau telepon genggam adalah sebuah teknologi yang semakin lama semakin berkembang pesat, dalam periode ini telepon genggam berubah menjadi teknologi yang paling banyak digunakan oleh masyarakat sebagai kebutuhan primer dari masyarakat bawah, menengah sampai atas. Dengan menaiknya tingkat penggunaan telepon genggam ini maka otomatis nomor-nomor selular yang digunakan akan semakin tinggi. Para kriminal tidak membiarkan saja peluang di buang percuma, mereka mencari celah untuk melakukan tindakan kriminal, melalui metode *spamming* dengan menggunakan telepon genggam ini pelaku akan mengirimkan suatu informasi kepada calon korbannya.

Spam telepon genggam diarahkan pada layanan pesan teks di ponsel. *Spam* ini bisa sangat mengganggu pelanggan karena bukan hanya masalah ketidaknyamanan, tetapi juga karena biaya yang mungkin dikenakan dari setiap pesan teks yang diterima. Contoh dari model *spam* ini misalnya :

a) Pesan yang bertujuan untuk menyebarkan iklan

Pesan model ini dikirim secara massal hanya untuk unsur promosi saja, misalnya :

"Pameran Online 2012 Disc 50%, Dapatkan produk Dari Blackberry, Nokia, Samsung dll U/INFO HUB:0853-1091-8111. Klik www.planet-ponsel.yolasite.com."

b) Pesan yang bertujuan untuk penipuan belaka

Pesan model ini dikirim secara massal biasanya untuk menipu korban dengan dalih sebagai kenalan maupun keluarga, misalnya :

"Ini mama, tolong beliin pulsa 10 ribu aja soalnya penting, nanti kalau sudah masuk hubungi di nomor 0856xxxxxx."

c) Pesan yang bertujuan untuk penipuan dengan unsur ancaman

Pesan model ini dikirim secara massal dengan tujuan untuk memeras korban, misalnya :

"Aku tahu apa yang anda perbuat, anda telah melanggar hukum, kalau tidak mau terbongkar perbuatan anda, kirimkan uang sejumlah 3 juta ke nomer rekening ini xxxxxxxxxx."

2. *Spam* di Indonesia

Apabila berbicara mengenai seluk beluk *spam*, maka pertama kali perlu diketahui dari manakah datangnya *spam* tersebut. Pada tahun 2010 tepatnya per Oktober-Desember 2010, firma keamanan dan kendali IT, Sophos memberikan hasil persentase 12 negara sebagai pengirim *spam* terbanyak, negara-negara tersebut adalah :

Tabel 4.1

NO.	NEGARA	PERSENTASE
1.	Amerika Serikat	18,83 %
2.	India	6,88 %
3.	Brasil	5,04 %
4.	Rusia	4,64 %
5.	Inggris	4,54 %
6.	Prancis	3,45 %
7.	Italia	3,17 %
8.	Korea Selatan	3,01 %
9.	Jerman	2,99 %
10.	Vietnam	2,79 %
11.	Rumania	2,25 %
12.	Spanyol	2,24 %
13.	Lainnya	40,17 %

Sumber: Data Sekunder diolah, 2012

Sophos mengklaim email *spam* yang marak saat ini makin berbahaya. Meski kebanyakan *spam* berisi iklan-iklan farmasi, kini *spam* berisi malware yang berpotensi phishing terhadap data-data pribadi user juga mulai bermunculan. Berkaitan dengan hal tersebut konsultan teknologi Sophos Graham Cluley mengatakan bahwa "Spam belum menghilang dalam waktu dekat. Namun motivasi dan metode yang digunakan mengirim spam terus

berubah,"[62] Pada tahun 2011, berdasarkan *Report Spam Evolution 2011* yang dilakukan oleh Kapersky salah satu pembuat anti virus terbesar di dunia, penelitian dari Kaspersky tersebut menyebutkan bahwa India merupakan negara pengirim e-mail *spam* terbanyak. Selama kuartal ketiga tahun 2011, dari keseluruhan lalu lintas e-mail global, sebanyak 79,8 persen merupakan *spam*. Dari jumlah itu, 14,8 persen berasal dari India, dan 10,6 persen dari Indonesia, serta 9,7 persen dari Brasil.

Berdasarkan hasil Kaspersky tersebut diketahui bahwa Indonesia sendiri menjadi negara produsen *spam* kedua terbesar di dunia dengan persentase 10,6 %, hasil ini jauh meningkat dari tahun-tahun yang lalu dimana Amerika Serikat pada urutan pertama sebagai negara penghasil *spam* terbesar sedangkan Indonesia pada tahun 2010 menduduki peringkat 16 kemudian naik drastis menjadi 3 (tiga) negara teratas sebagai produsen *spam*.[63]

Darya Gudkova, seorang analis *spam* di Kaspersky mengatakan, statistik itu mencerminkan tren yang berkembang untuk *spam*. *Spam* banyak dikirim dari komputer di Asia dan negara-negara Amerika Latin karena kurangnya kesadaran tentang keamanan internet. Hukum untuk ranah e-mail *spam* ini pun masih lemah. Hal ini memudahkan penjahat *cyber* membangun botnet (jaringan yang terinfeksi). Wijay Mukhi, spesialis kemananan internet di Mumbai, ibukota India, mengatakan *spammer* terpaksa mencari basis baru setelah negara-negara lain menindak keras praktek *spam*. India saat ini

[62] Sumber Billy A Banggawan, *Siapa Pengirim Spam Terbanyak?*, http://nasional.inilah.com /read /detail/1136012/URLTEENAGE, di akses pada tanggal 28 Mei 2012.
[63] Sumber Ibnu Azis, *Indonesia Peringkat Ketiga Negara Produsen Spam*, http://sidomi.com/ 74533/indonesia-peringkat-ketiga-negara-produsen-*spam*/, di akses pada tanggal 28 Mei 2012

memiliki 112 juta pengguna internet, ketiga terbesar di dunia setelah Cina dan Amerika Serikat, menurut *The Internet and Mobile Association of India* (IMAI).[64] Kemudian sampai pada tahun 2012 terjadi penurunan pada negara Indonesia, dimana pada tahun 2011 menduduki peringkat 3 turun ke peringkat 4 bersaing dengan Rusia yang jumlah persentasenya adalah sama yaitu 5,0 %. Hasil persentase dari Sophos adalah sebagai berikut :[65]

Tabel 4.2

NO.	NEGARA	PERSENTASE
1.	India	9,3 %
2.	Amerika Serikat	8,3 %
3.	Korea Selatan	5,7 %
4.	Indonesia dan Rusia	5,0 %
5.	Italy	4,9 %
6.	Brazil	4,3 %
7.	Polandia	3,9 %
8.	Pakistan	3,3 %
9.	Vietnam	3,2 %
10.	Taiwan	2,9 %
11.	Peru	2,5 %
12.	Lainnya	41,7 %

Sumber: Data Sekunder diolah, 2012

[64] Sumber12. Kompas, *Indonesia jadi Penyumbang Spam Nomor 2 Terbesar di Dunia,* http://samuelbimo.blogspot.com/2012/01/indonesia-jadi-penyumbang-*spam*-nomor-2.html di akses pada tanggal 28 Mei 2012

[65] Sumber Gesit Prayogi, *Indonesia Posisi 4 Pengirim Spam Terbanyak di Dunia,* http://autos.okezone.com/read/2012/04/25/55/618378/indonesia-posisi-4-pengirim-*spam*-terbanyak-di-dunia, di akses pada tanggal 28 Mei 2012.

Untuk zona wilayah dapat dibagi sebagai berikut :

Tabel 4.3

NO.	WILAYAH	PERSENTASE
1.	Asia	46,7 %
2.	Eropa	26,9 %
3.	Amerika Selatan	11,9 %
4.	Amerika Utara	10,9 %
5.	Afrika	3,0 %
6.	Lainnya	0,6 %

Sumber: Data Sekunder diolah, 2012

Senior Technology Consultant dari Sophos, Graham Cluley mengatakan, "Statistik terbaru menunjukkan bahwa pengguna internet di negara berkembang tidak mengambil langkah-langkah untuk memblokir infeksi *malware* yang kemudian dapat mengaktifkan PC mereka menjadi *spam-spewing* zombie." Sedangkan perngertian dari zombie sendiri adalah komputer yang terinfeksi dan membentuk jaringan botnet. Botnet digunakan oleh penjahat *cyber* untuk mengirim *spam*, mencuri informasi dan DDoS melakukan penyerangan *distributed denial of service* (DDoS).[66]

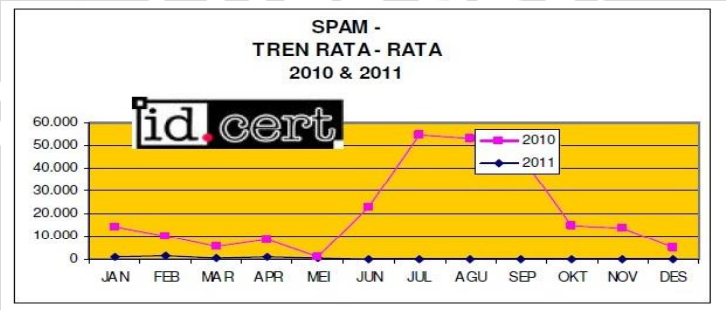
Menurut laporan tahunan Statistik Internet Abuse Indonesia Tahun 2011 yang di susun oleh Ahamd Khalil Alakazimy, ST mengenai *spam* bahwa dari

[66] *Ibid*

total laporan yang masuk, *spam* menduduki peringkat kedua dari total laporan yang diterima. Sedangkan bila dibandingkan dengan bulan yang sama tahun 2010 juga menurun. Dan dari sisi volume laporan, tahun ini jauh lebih rendah dibandingkan pada periode yang sama tahun 2010.

Gambar 4.2

GRAFIK I: *SPAM RATA-RATA*

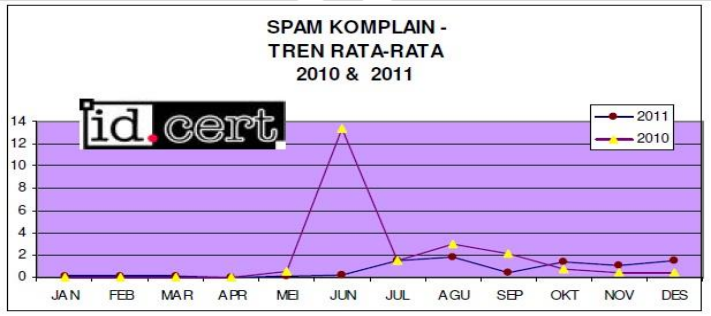


Sumber: Data Sekunder diolah, 2012

Sedangkan mengenai laporan mengenai *spam* menempati peringkat ke tujuh dimana yang masuk pada kategori ini adalah laporan korban *spam* dari network di Indonesia maupun luar negeri.

Gambar 4.3

GRAFIK II: *SPAM* KOMPLAIN



Sumber Data Sekunder, 2012

Sama halnya dengan laporan yang diterima, jumlah komplain *spam* juga menempati peringkat ke tujuh yang juga berasal dari network di Indonesia maupun luar negeri.

3. Karakteristik *Spamming*

Spamming memiliki pengertian sebagai penyalahgunaan sistem pesan elektronik (termasuk media penyiaran dan sistem pengiriman digital) untuk mengirim berita iklan dan keperluan lainnya secar massal, bertubi-tubi tanpa diminta dan sering kali tidak di kehendaki oleh penerimanya.

Sedangkan *spamming* sendiri memiliki karakteristik ataupun ciri-ciri yang dapat membedakan dari bentuk kejahatan siber (*cyber crime*) yang lain, karakteristik ini dapat dibedakan menjadi beberapa karakteristik, yaitu :

a) Tindakan yang dilakukan dengan sengaja dan biasanya tidak memiliki hak untuk mengirim *spam*.
b) Perbuatannya adalah menyebarkan secara luas atau global tanpa tujuan tertenu, karena hal tersebut para korban memiliki ruang lingkup yang luas dan biasanya tidak menyadari bahwa telah menjadi korban tindakan *spamming*.
c) Objek dari perbuatan ini biasanya digunakan untuk menyebarkan suatu iklan-iklan dari suatu produk tertentu, sebagian juga berbentuk sebagai berita atau informasi yang dapat berujung penipuan.
d) Kerugian atau akibat yang dapat dirasakan oleh korban tindakan *spamming* adalah :

1) Immateriil

Sebagian besar korban dari tindakan *spamming* memiliki kerugian immateriil misalnya

- memakan waktu dan tenaga dari si penerima email untuk membaca, menghapus dan menolak di kemudian hari.
- *Spam* dapat memenuhi mailbox yang dapat mengakibatkan mailserver sibuk sehingga memperlambat layanan yang lain.
- Menghabiskan resource jaringan internet
- Menyulitkan seseorang untuk menggunakan internet secara normal, misalnya banyaknya *Advertising* atau iklan yang memenuhi halaman web ataupun blog-blog yang ingin di cari.

2) Materiil

- Banyak uang terkuras setiap hari karena bandwidth yang diperlukan untuk mengirimkan jutaan email *spam*, padahal akhirnya akan di *bounce* atau langsung di hapus.
- *Spam* juga sebagai media penyebaran virus, dan apabila komputer telah terjangkit virus maka dapat menyebabkan kerusakan pada sistem komputer tersebut. Sehingga dapat dikatakan hal ini termesuk dalam kerugian materiil.
- Kerugian yang berikutnya adalah dapat berujung pada penipuan yang dapat merugikan korban dari segi materiil, hal ini dapat juga disebut sebagai akibat tidak langsung korban tindakan *spamming*.

4. Motif melakukan *Spamming*

Pelaku tindakan *spamming (spammer)* melakukan tindakan tersebut biasanya dilakukan berdasarkan latar belakang atau motif tertentu, misalnya :

a) Sebagai Media Promosi

Spammer melakukan tindakan ini dikarenakan nantinya promosi terhadap barang yang akan dijual akan menghemat biaya promosi, efektif dikarenakan disebarkan secara massal dan memiliki jangkauan yang sangat luas dan dapat menembus berbagai negara dalam waktu singkat.

b) Sebagai media untuk meningkatkan popularitas

Hal ini dilakukan oleh para *spammer* dengan cara *spam*dexing yang dapat menguasai suatu mesin pencari (search engine) untuk mencari popularitas bagi URL tertentu.

c) Sebagai media penipuan

Biasanya para pelaku *spamming* ini menyebarkan berbagai informasi yang dapat berupa iklan maupun berita belaka dengan adanya maksud tertentu, salah satunya adalah sebagai cara untuk melakukan kejahatan penipuan. Misalnya *spam* yang berupa iklan kemudian sangkorban tertarik untuk membeli barang tersebut tetapi setelah uang terkirim pada nomor rekening tertentu ternyata barang tersebut tidak dikirim, palsu maupun mengandung cacat pada barang tersebut atau dapat dikatakan barang tersebut tidak seperti yang di janjikan oleh penjual.

d) Sebagai alat untuk menyebarkan virus maupun Malware

Salah satu alasan yang paling mengganggu maupun merugikan yaitu sebagai alat atau media untuk menyebarkan virus maupun malware. Misalnya salah satu *spammer* terbesar di dunia yaitu Rustock botnet.

Botnet yang mulai beroperasi tahun 2006 ini dapat mengirimkan hingga 25 ribu *spam* per jam dengan file malware tertanam di dalamnya. Setiap komputer yang berhasil terinfeksi dengan malware ini akan dapat dikontrol secara *remote* oleh para hacker. Tetapi pada Maret 2011, Rustock botnet berhasil dihentikan oleh pihak Microsoft. Sejak saat itu, jumlah *spam* yang beredar di dunia maya berkurang hingga 15%.[67]

e) Sebagai "Bom Email"

Hal ini sengaja dilakukan oleh *spammer* apabila memiliki musuh di internet maupun berupa saingan perusahaan yang lain, para *spammer* nantinya akan mengirimkan *spam* dalam jumlah yang sangat besar dan secara terus-menerus sehingga korban yang menerima email *spam* tersebut akan kerepotan dengan jumlah email *spam* yang tidak diperlukan, apalagi apabila di antara email yang tercampur di dalam email *spam* tersebut adalah email penting yang menyangkut mengenai data-data penting perusahaan misalnya data keuangan, perjanjian ataupun pertemuan penting.

[67] Sumber Ernest Dimitria, *Astrindo Starvision Paparkan Data Evolusi Ancaman TI dari Kaspersky Lab*, http://www.jagatreview.com/2011/06/astrindo-starvision-paparkan-data-evolusi-ancaman-ti-dari-kaspersky-lab/, di akses pada tanggal 28 Mei 2012.

B. Urgensi Krimininalisasi mengenai tindakan "*spamming*" dalam hukum pidana di Indonesia

Apabila berbicara mengenai urgensi kriminalisasi maka dihadapkan dengan sepenting atau seurgensi apa sehingga dibutuhkannya kriminalisasi terhadap tindakan *spamming* tersebut, maka perlu sekali untuk dikaji lebih lanjut mengenai hal tersebut.

Pertama mengenai kebijakan kriminalisasi memiliki pengertian sebagai suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana), tindakan *spamming* sendiri didalam sistem perundang-undangan dapat dikatakan belum diatur, apabila dilihat di dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik mengenai perbuatan yang dilarang dapat dirangkum sebagai berikut:

1. Pasal 27
    a. Ayat 1 mengenai tindakan yang melanggar kesusilaan.
    b. Ayat 2 mengenai tindakan yang bermuatan perjudian.
    c. Ayat 3 mengenai tindakan penghinaan dan/atau pencemaran nama baik.
    d. Ayat 4 mengenai tindakan pemerasan dan/atau pengancaman.
2. Pasal 28
    a. Ayat 1 mengenai tindakan menyebarkan berita bohong dan menyesatkan.

b. Ayat 2 mengenai tindakan yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan.

3. Pasal 29 mengenai tindakan yang bertujuan untuk memberikan ancaman kekerasan atau menakut-nakuti.
4. Pasal 30 mengenai tindakan yang bertujuan untuk mengakses komputer dan/atau sistem elektonik milik orang lain dengan cara apapun atau biasa disebut dengan cracking.
5. Pasal 31 mengenai tindakan penyadapan, perubahan dan penghilangan informasi dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.
6. Pasal 32
   a. Ayat 1 mengenai tindakan mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan dan menyembunyikan.
   b. Ayat 3 mengenai tindakan membuka rahasia.
7. Pasal 33 mengenai tindakan yang berakibat terganggunya sistem elektronik sehingga menjadi tidak bekerja sebagaimana mestinya.
8. Pasal 34 mengenai tindakan memproduksi, menjual, mengandakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau lunak dan sandi lewat komputer maupun kode akses untuk memfalitasi perbuatan dalam pasal 27 sampai dengan pasal 33.

9. Pasal 35 mengenai tindakan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan yang bertujuan agar informasi dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik.

Berdasarkan penjelasan mengenai perbuatan yang dilarang di dalam peraturan perundang-undangan nomor 11 tahun 2008 tentang informasi dan transaksi elektronik diatas, maka dapat dikatakan bahwa masih belum tercantum peraturan yang menyangkut mengenai tindakan *spamming* karena itu perlu adanya kajian lebih lanjut mengenai kriminalisasi tindakan *spamming*.

Apabila dibandingkan dengan pasal 28 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik yang berbunyi "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

Dari pasal tersebut Drs. Adami Chazawi, S.H. dalam bukunya menyebutkan bahwa dalam ayat (1) terdiri dari unsur-unsur sebagai berikut :[68]

1. Kesalahan : *dengan sengaja;*
2. Melawan hukum : *tanpa hak;*
3. Perbuatan : *menyebarkan;*
4. Objek : *berita bohong dan menyesatkan;*
5. Akibat konstitutif : *mengakibatkan kerugian konsumen dalam transaksi elektronik.*

[68] Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, Bayumedia Publishing, Malang, 2011, hal.128.

Sedangkan ayat (2) terdiri dari unsur-unsur sebagai berikut :

1. Kesalahan : *dengan sengaja;*
2. Melawan hukum : *tanpa hak;*
3. Perbuatan : *menyebarkan;*
4. Objek : *informasi;*
5. Tujuan : *untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar golongan (SARA).*

Apabila dibandingkan dengan unsur-unsur tindakan *spamming* dapat di sebutkan unsur-unsurnya sebagai berikut:

1. Kesalahan : *dengan sengaja;*
2. Melawan hukum : *tanpa hak;*
3. Perbuatan : *menyebarkan secara massal;*
4. Objek : *informasi berupa promosi ataupun berita;*
5. Akibat : *dapat mengakibatkan kerugian konsumen dalam transaksi elektronik.*

Dalam perbandingan ini dapat dikatakan bahwa sangat kontradiktif dimana dalam ayat (1) memiliki objek berita bohong dan menyesatkan sedangkan ayat (2) objeknya adalah informasi, sehingga ayat (2) memiliki objek yang sama dengan tindakan *spamming* yaitu objeknya adalah informasi, tetapi apabila dilihat lebih lanjut ayat (1) menekankan bahwa akibat konstitutifnya adalah mengakibatkan

kerugian konsumen dalam transaksi elektronik sedangkan di dalam ayat (2) menekankan bahwa memiliki tujuan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar golongan (SARA).

Apabila di bandingkan dengan tindakan *spamming* ayat (1) yang masih dapat memenuhi dari unsur-unsur tersebut,maka dapat dikatakan bahwa pasal 28 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik yang dapat mendekati unsur tindakan *spamming* masih belum dapat digunakan sebagai dasar pemidanaan tindakan *spamming* dikarenakan pasal ini dapat dikatakan masih belum jelas atau kabur.

1. Bentuk urgensi dari tindakan *spamming*

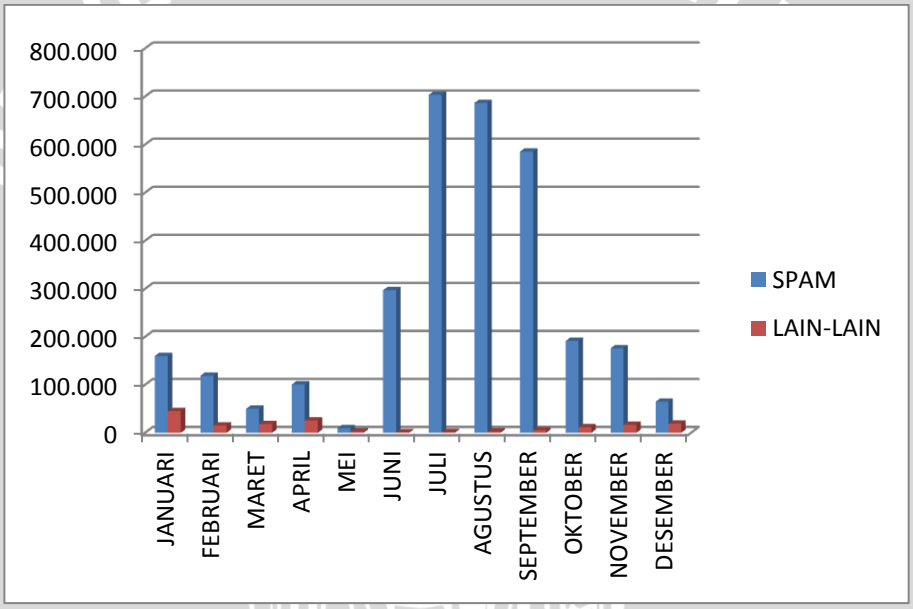
   Yang menarik dalam pembahasan mengenai tindakan *spamming* ini adalah dalam bagian dimanakah letak dari urgensi untuk bisa meng-kriminalisasikan tindakan *spamming* ini, sebagian telah di jelaskan pada bagian gambaran umum sehingga dalam hal ini lebih dijelaskan secara lebih rinci mengenai urgensi dari kriminalisasi tindakan *spamming* ini di dalam hukum pidana Indonesia.

   Apabila dilihat kebelakang tepatnya pada tahun 2010, tindakan *spamming* ini adalah salah satu dari kejahatan dunia maya yang paling banyak terjadi di Indonesia. Ahmat Khalil Alkazimy, ST dengan didukung oleh KEMKOMINFO (Kementerian Komunikasi dan Informasi), ID-CERT (*Indonesia Computer Emergency Response Team*) dan PANDI (Pengelola

Nama Domain Internet Indonesia) serta sejumlah responden telah menghasilkan suatu riset independen yang berjudul STATISTIK *ABUSE* INTERNET INDONESIA 2010 yang dilakukan secara berkala yaitu dengan 4 kwartal, selanjutnya akan dirangkum dan dijelaskan dengan rinci mengenai 4 kwartal tersebut.

Gambar 4.4

Data grafik laporan *spamming* pada tahun 2010



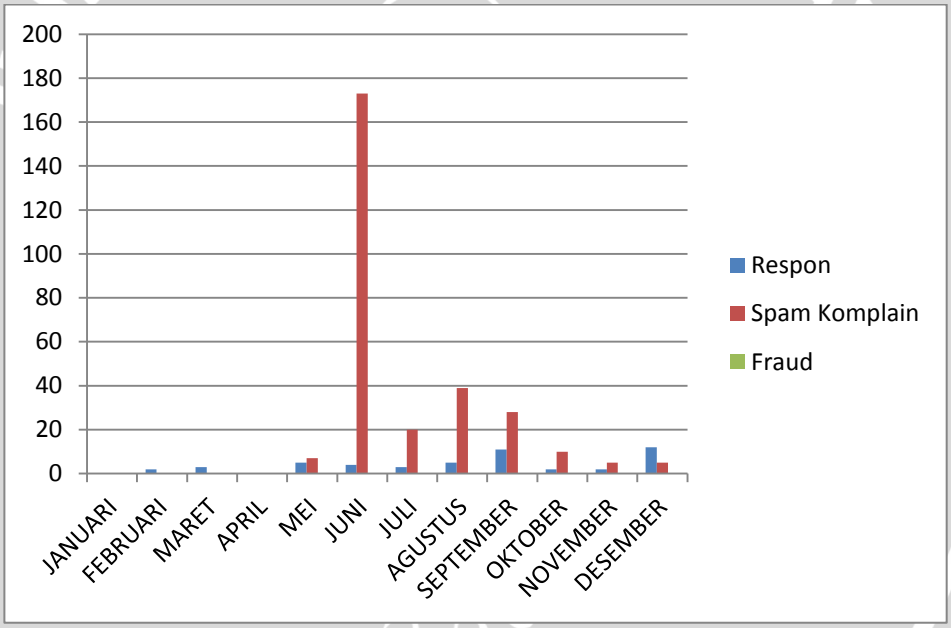
Sumber: Data Sekunder diolah, 2012

Pada gambar tersebut grafik berwarna biru menunjukkan bahwa tindakan *spamming* masih dalam urutan pertama dalam kejahatan dunia maya walaupun dalam bulan mei terjadi penurunan, kemudian pada bulan berikutnya terjadi kenaikan jumlah *spamming* yang signifikan walaupun pada bulan-bulan berikutnya terjadi penurunan berkala, sedangkan grafik warna merah ditempati oleh kejahatan yang lain misalnya terbesar kedua adalah kejahatan mengenai Intellectual Property (HaKI), kemudian urutan ketiga

adalah penyebaran Malware, posisi keempat yaitu semacam insiden jaringan (Network Incident) yang mencakup: DoS Attack, Open Relay, Open Proxy, Hacking, Port Scanning, Port Probe (HTTP/HTTPS, FTP, TELNET, TCP, SSH Brute, CGI, RPC, Netbios, VNC Portscan), TCP Sweep dan SQL Injection, kemudian yang terakhir adalah Spoofing/ Phishing yang mencakup pula IP Spoofed, Web Spoofed dan Scam.

Gambar 4.5

Data grafik perbandingan antara respon, fraud dan *spam* pada 2010



Sumber: Data Sekunder diolah, 2012

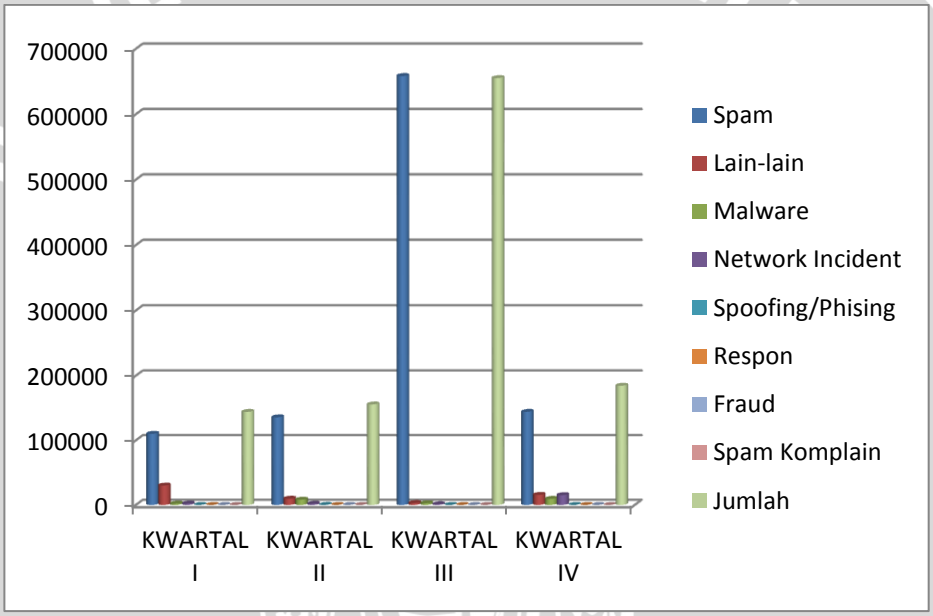
Kemudian mengenai bentuk respon atau pengaduan mengenai kejahatan siber (*Cyber crime*) pada 4 bulan pertama tingkat respon maupun *spam* komplain masih rendah, pada bulan berikutnya terjadi peningkatan jumlah komplain pada bulan juni tetapi selanjutnya terjadi penurunan secara berturut-turut. Hal ini membuktikan bahwa tingkat kesadaran dari korban tindakan

spamming untuk melakukan komplain atau bentuk respon rata-rata masih sangat rendah walaupun terjadi kenaikan pada bulan tertentu.

Berdasarkan kedua gambar diatas maka dapat dirangkum secara lengkap mengenai grafik pada tahun 2010 yang dapat dijelaskan pada gambar dibawah ini

Gambar 4.6

Data grafik trend rata-rata secara total pada 2010



Sumber: Data Sekunder diolah, 2012

Dari gambar diatas dapat dirangkum bahwa pada tahun 2010 tindakan *spamming* berada pada level teratas untuk kejahatan dunia maya yang terjadi di Indonesia dengan rata-rata laporan yang diterima mengalami sejumlah penurunan hingga akhir tahun, hal ini dapat dikatakan bahwa walaupun telah menjadi korban tindakan *spamming* tetapi terjadi penurunan tingkat pelaporan terhadap *spamming* ini sehingga tinggkat kesadaran semakin lama semakin berkurang, hal ini di khawatirkan semakin menurunnya tingkat pelaporan atau

respon yang dilakukan oleh korban *spamming*, maka semakin berkembangnya tingkat kejahatan *spamming* tersebut. Pada hasil penelitian yang dilakukan oleh *Cisco* yaitu *Cisco 2010 Annual Security Report*[69] pada tahun 2011 ditemukan bahwa sampai september 2011 negara India menjadi pengirin *spam* tertinggi dengan jumlah persentase 13,9%, pada tahun 2010 Amerika Serikat yang menduduki peringkat kedua dari januari sampai september 2011 turun dari 10,1% menjadi 3,2% dan menuduki peringkat sembilan, sebagai gantinya peringkat kedua sekarang diduduki oleh Rusia dengan jumlah persentase yang semula 7,6% menjadi 7,8% pada pertengahan 2011. Pada peringkat ketiga diduduki olek negara Vietnam dengan jumlah persentase yang naik dari 6% pada agustus menjadi 8% pada bulan september, sedangkan peringkat berikutnya dengan jumlah persentase yang sama yaitu Indonesia dan Korea Selatan dengan jumlah persentase sebesar 6%. Sedangkan negara lain yang pada awal tahun menduduki peringkat teratas seperti China dan Brazil mengalami penurunan persentase pada pertengahan 2011 tetapi masih dalam urutan 10 negara teratas dalam penyebaran *spam*.

Data statistik tersebut kemudian telah dibuktikan dengan hasil *Report Spam Evolution 2011* yang dilakukan oleh Kapersky yang menyebutkan bahwa Indonesia menduduki peringkat tiga teratas disamping India dan Brasil dimana pada tahun 2010 Indonesia yang menduduki peringkat 16 kemudian pada tahun 2011 terjadi kenaikan drastis menjadi 3 teratas.

[69] *Cisco, Cisco 2011 Annual Security Report Highlighting Global Security Threats And Trends,* hal.30.

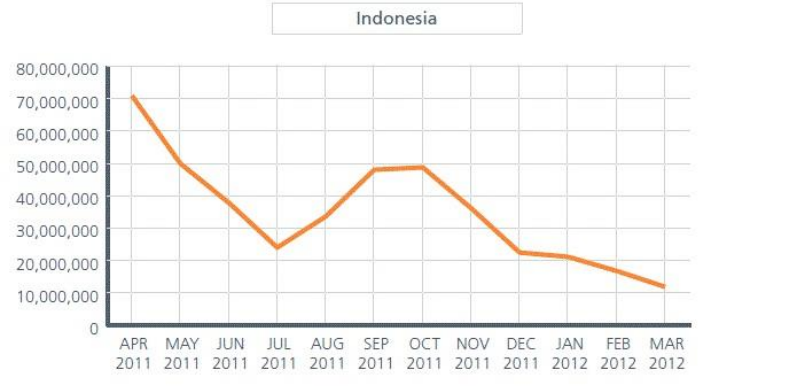
Sedangkan menurut hal ini membuktikan bahwa faktor kesadaran terhadap *spamming* ini misalnya dengan bentuk pelaporan masih kurang dimiliki selain itu perlu adanya suatu peraturan khusus untuk mengatasi masalah *spamming* di Indonesia.

Lain halnya pada tahun berikutnya, pada tahun 2012 walaupun terjadi penurunan peringkat dari yang sebelumnya 4 teratas, pada tahun 2012 menjadi peringkat 4 seimbang dengan Rusia dengan persentase sebagai produsen *spam* terbesar yaitu sebesar 5.0 % dari jumlah seluruh produsen *spam* di seluruh dunia. Indonesia dijadikan sebagai peringkat 4 sedangkan Rusia sebagai peringkat 5 walaupun memiliki persentase sama yaitu sebesar 5.0 % tetapi apabila dilihat secara rinci maka Indonesia menjadi peringkat 4 dikarenakan dilihat dari banyaknya terkena dampak kerugian dari *spamming*.

McAfee sebuah perusahaan anti virus yang terkenal pada tahun 2012 juga melakukan penelitian terhadap perkembangan *cyber crime* di dunia yang bernama *McAfee Threats Report 2011* yang terbagi dalam 2 quarter dimana disebutkan bahwa penyebaran *spam* di Indonesia pada quarter pertama bulan april 2011 sampai bulan maret 2012 terjadi penurunan yang signifikan pada bulan juli kemudian naik pada bulan september dan diakhiri dengan penurunan kembali pada bulan desember 2011, lebih lengkapnya dapat dilihat pada data grafik berikut:

Gambar 4.7

Data laporan *spamming* McAfee quarter pertama



Sumber: Data Sekunder diolah, 2012

Pada quarter pertama ini ditemukan bahwa negara Indonesia mengalami penurunan pada penyebaran *spam* dengan paling banyak adalah tipe penyebaran *spam* melalui *spam* dengan maksud untuk menawarkan *drugs* (obat-obatan). Kemudian quarter berikutnya dapat dilihat sebagai berikut:

Gambar 4.8

Data laporan *spamming* McAfee quarter kedua

Sumber: Data Sekunder diolah, 2012

Pada data grafik diatas menunjukkan bahwa terjadi penurunan volume penyebaran *spam* pada awal tahun 2012 sampai dengan bulan juni walaupun

sebelumnya pada akhir tahun 2011 terjadi lonjakan dratis pada volume penyebaran *spam* di Indonesia.

Securelist sebuah situs resmi yang masih bernaung pada *Kaspersky Lab* salah satu antivirus terkemuka di dunia yang khusus meneliti mengenai perkembangan *cyber crime* di dunia baru-baru ini melakukan sebuah riset mengenai perkembangan *spam* yang telah dimulai pada bulan januari 2012 dan telah menghasilkan data-data sebagai berikut:

1) Januari

Pada bulan januari Indonesia menduduki peringkat kedua setelah India dengan jumlah persentase 8.1% sedangkan India sebesar 11,6%, perinhgkat ketiga diduduki oleh Korea dengan 7.7%, keempat Brasil dengan 7.6 % dan kelima Peru dengan 3.9%. sedangkan kategori *spam* 3 teratas pada bulan januari yaitu *Computer Fraud*, *Personal Finances* dan *Education*.[70]

2) Februari

Pada bulan februari Indonesia tetap menduduki peringkat kedua dengan jumlah persentase sebesar 8.3%, peringkat pertama masih diduduki oleh India dengan 11.9%, peringkat ketiga dan keempat diduduki Brasil dan Korea dengan 6.6%, kelima Vietnam yang sebelumnya 3.5% menjadi 4.9%. Kategori *spam* 3

[70] Kaspesky Lab, *Spam report: January 2012*, http://www.securelist.com/en/analysis/204792220/Spam_report_January_2012, diakses pada tanggal 15 September 2012.

teratas yaitu *Computer Fraud*, *Personal Finances* dan *Computers and the Internet*.[71]

3) Maret

Pada bulan Maret Indonesia tetap menduduki peringkat kedua dengan jumlah persentase sebesar 7.5%, peringkat pertama masih berturut-turut ditempati oleh India dengan 12.3%, ketiga Brasil dengan 6.7%, keempat Vietnam naik menjadi 6.1%, dan keima ditempati oleh Korea dengan 4.2%. Sedangkan kategori *spam* 3 teratas yaitu *Computer Fraud, Personal Finances* dan *Gambling*.[72]

4) April

Pada bulan April peringkat pertama ditempati oleh India dengan 11.2%, kedua USA dengan 8.5%, ketiga Vietnam 7.1%, keempat Korea dengan 6.5% dan kelima ditempati oleh China dengan 6.1%, sedangkan Indonesia turun menjadi peringkat ke-12 dengan jumlah persentase sebesar 2.1%. dengan kategori *spam* 3 teratas yaitu *Computer Fraud, Personal finances* dan *Interior Design*.[73]

---

[71] Kaspersky Lab, *Op.Cit.*, http://www.securelist.com/en/analysis/204792224/Spam_report_February_2012#1, diakses pada tanggal 15 September 2012.

[72] Kaspersky Lab, *Op.Cit.*, http://www.securelist.com/en/analysis/204792226/Spam_report_March_2012#fig, diakses pada tanggal 15 September 2012.

[73] Kaspersky Lab, *Op.Cit.*, http://www.securelist.com/en/analysis/204792230/Spam_Report_April_2012#1, diakses pada tanggal 15 September 2012.

5) Mei

Pada bulan Mei peringkat pertama ditempati oleh China dengan 25.4%, kedua adalah India yang sebelumnya menempati peringkat pertama dengan jumlah persentase 12.3%, ketiga Brasil dengan 5.1%, keempat USA 4% dan kelima Vietnam dengan 3.6%, sedangkan Indonesia menempati peringkat ke-13 dengan jumlah persentase 1.5%. dengan kategori *spam* teratas yaitu *Computer Fraud, Personal finances* dan *Legal and Audit Services.*[74]

6) Juni

Pada bulan juni terbagi menjadi 2 yaitu *spam* yang dikirim ke Eropa user dan US user, *spam* yang dikirim ke Eropa user peringkat pertama ditempati oleh China dengan 36.6%, kedua India dengan 12.6%, USA menempati peringkat ketiga dengan 4.9%, keempat Brasil dengan 4.8% dan kelima Argentina dengan 2.8%, sedangkan Indonesia menduduki peringkat ke-14 dengan 1.1%. pada US user peringkat pertama ditempati USA dengan 39.2%, kedua China dengan 9.1&, ketiga Brasil dengan 6.6%, keempat India dengan 3.7% dan kelima Korea Selatan dengan 2.9%, sedangkan Indonesia pada US user menempati peringkat 11 sebesar 1.5%. Kategori *spam* teratas yaitu *Personal finances*,

[74] Kaspersky Lab, *Op.Cit.*, http://www.securelist.com/en/analysis/204792234/Spam_report_May_2012#1, diakses pada tanggal 15 September 2012.

Medications, Health-related goods and services dan *Computer Fraud*.[75]

7) Juli

Pada bulan juli yang dikirim ke Eropa user peringkat pertama diduduki oleh China dengan 32.21%, peringkat kedua India dengan 13.95%, ketiga USA 6.43%, keempat Brasil dengan 4.89%, kelima Vietnam dengan 3.01% dan Indonesia menjadi peringkat ke-12 dengan 1.54%, sedangkan US user peringkat pertama ditempati USA dengan 41.13%, kedua China dengan 7.92%, ketiga Brasil 5.69%, keempat India sebesar 4.06%, kelima UK dengan 3.96% dan Indonesia menenpati peringkat 16 dengan 0.91%. Kategori *spam* teratas yaitu *Personal finances, Medications, Health-related goods and services* dan *Computer Fraud*.[76]

Apabila dilihat dari hasil persentase yang dilakukan berbagai golongan maka pihak pemerintah Indonesia perlu khawatir mengenai dampak yang nantinya akan terjadi hal ini di karenakan tindakan *spamming* yang dilakukan oleh para *spammer* yang tidak bertanggung jawab, misalnya dalam hal pengiriman sms massal, email maupun jenis-jenis tindakan *spamming* yang

[75] Kaspersky Lab, *Op.Cit.*, http://www.securelist.com/en/analysis/204792236/Spam_report_June_2012#1, diakses pada tanggal 15 September 2012.
[76] Kaspersky Lab, *Op.Cit.*, http://www.securelist.com/en/analysis/204792243/Spam_in_July_2012#1 , diakses pada tanggal 15 September 2012.

lain khususnya menyangkut penyebaran iklan-iklan maupun promosi yang dilakukan oleh *spammer*.

Kita tahu bahwa pada masa yang serba teknologi canggih ini banyak terbuka peluang untuk terjadinya suatu bentuk kejahatan, termasuk juga penyebaran iklan yang sangat sering terjadi di berbagai tempat, karena di zaman yang serba mahal dan sulit ini kemudian digunakan salah satu cara yang dapat menyebarkan iklan atau promosi secara massal dengan mudah, cepat dan gratis walaupun mereka para *spammer* tidak tahu bahwa banyak yang merasa dirugikan oleh tindakannya tersebut.

2. Urgensi Kriminalisasi

Pertama mengenai kebijakan kriminalisasi terhadap tindakan *spamming*, seperti yang telah di jelaskan di atas bahwa kebijakan kriminalisasi merupakan suatu kebijakan dalam rangka menetapkan suatu perbuatan yang semula bukan merupakan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana).

Bila dikaitkan dengan tindakan *spamming* ini, dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik dapat dikatakan masih belum dapat menjerat para pelaku tindakan *spamming* ataupun peraturan yang terdapat dalam undang-undang tersebut belum sempurna untuk semua kejahatan dunia maya.

Apabila dibandingkan dengan negara-negara lain maka sebagian besar negara lain telah memiliki suatu peraturan khusus untuk mengatasi *spamming*

karena tindakan ini telah menjadi suatu permasalahan yang sangat serius, negara-negara tersebut misalnya:

a. Amerika

Amerika telah mengeluarkan peraturan khusus mengenai *cyber crime* yaitu *Uniform Electronic Transaction Act (UETA).* yang diadopsi oleh *National Conference of Commissioners on Uniform State Laws (NCCUSL)* pada tahun 1999.

Pada tahun 2003 Amerika sekali lagi membuat peraturan khusus mengenai tindakan *spamming*, peraturan tersebut bernama CAN-*SPAM* Act *(Controlling the Assault of Non-Solicited Pornography and Marketing)* yang dibuat oleh *Federal Trade Commission* (FTC) Amerika dan kementrian hukum (*Departement of Justice*).

b. Sebagian negara-negara Eropa

Sebagian dari negara-negara di Eropa memiliki peraturan mengenai *spamming* dalam *European E-Commerce Directive*. Negara Jerman memiliki peraturan mengenai *spam* tersendiri yang bernama *Information and Communication Service Act.*

c. Sebagian negara-negara Asia

Negara-negara yang memiliki peraturan khusus mengenai *spam* adalah negara Singapore yang merupakan satu-satunya negara di ASEAN yang memberlakukan hukum secara tegas terhadap *spammer*s dengan *Spam Control Act 2007*. Kemudian Hongkong dengan *Anti-Spam Code of Practices.*

d. Australia

Negara Australia yang telah berupaya membuat kebijakan kriminalisasi yang berkaitan dengan *spamming* sejak tahun 1998 dengan adanya kesepakatan dari *Internet Service Providers* (ISPs) dalam *the Internet Industry Association code of practice contained optout spamming provisions (IIA)* tahun 1998 yang mengeluarkan aturan yang mengikat setiap providers dalam *spamming*, terutama yang berkaitan dengan bisnis, yang isinya sebagai berikut:[77]

> *(1) IIA members and code subscribers must not spam, and must not encourage spam, with exceptions in the case of pre-existing relationships (that is, it does not prevent acquaintance spam).*
> *(2) IIA members and code subscribers who do use acquaintance spam must provide recipients with the capability to opt-out, and must include opt-out instructions in the spam.*
> *(3) IIA members and code subscribers must not send even acquaintance spam containing prohibited content.*
> *(4) IIA member and code subscriber Internet Service Providers should have an Acceptable Use Policy that prohibits spam, and further prohibits services that depend on spam.*
> *(5) ISPs should have a working contact address for spam complaints - that is, an "abuse@" email address.*
> *(6) ISPs should install relay protection on their mail servers, to prevent spammers from using the relay to evade detection or penalty.*

[77] Alan Davidson, "*Spamming in Cyberspace*", Journal of the Queensland Law Society, 2002, di akses dari http://www.uq.edu.au/davidson/cyberlaw/april2002.html. di kutip dari Philemon Ginting, *Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana, Op.Cit.*, 2008, hal.208.

Pada bulan Nopember 2000 pemerintah Australia mengkriminalisasikan perbuatan *spammer* kedalam *section* 76 E *Crimes Code* 1995 yang berisikan:[78]

> *"an offence intentionally and without authority interfere with, interrupt or obstruct the lawful use of a computer or to impair the usefulness or effectiveness of data stored in a computer by means of a carrier, such as email. This case related to the relay of a spam through a third party computer system" The maximum penalty is 10 years imprisonment."*

Dalam pasal 28 Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi elektronik yang dapat dikatakan mendekati *spamming* masih belum bisa di karenakan unsur-unsur yang sedikit berbeda dari tindakan *spamming* ini yang telah dijelaskan di atas.

Suatu kejahatan pasti dapat menimbulkan suatu dampak atau kerugian pada korbannya, kerugian tersebut dapat berupa immateriil atau juga materiil, sedangkan pada *spamming* juga terdapat kerugian immaterril dan juga materiil. Mengenai bentuk-bentuk kerugian maupun dampak dari *spamming* dapat dijelaskan sebagai berikut:

1) Immateriil

Sebagian besar tindakan *spamming* menimbulkan kerugian yang berbentuk immateriil bagi korbannya, kerugian tersebut misalnya:

a) *Spamming* dapat memakan atau membuang waktu dan tenaga dari si penerima email untuk membaca, menyortir atau memilah-milah, menghapus dan menolak di kemudian hari, hal ini

[78] Sumber http://www.qscl.org.au/ di kutip dari Philemon Ginting, *Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana, Op.Cit.*, hal.208-209.

sangatlah mengganggu, bayangkan apabila email spam yang datang perharinya mencapai puluhan, ratusan atau bahkan ribuan sedangkan pengguna sedang menunggu email yang sangat penting misalnya menyangkut pekerjaan apalagi dalam keadaan mengejar waktu atau dalam keadaan terburu-buru. Karena itu hal ini sangat mengganggu bagi pengguna email apalagi *spammer* memang memiliki niat untuk membanjiri dengan email yang dinamakan dengan "bom email" hal ini sangatlah merugikan. Misalnya saja terdapat suatu perusahaan yang berniat untuk mengganggu saingan bisnisnya dengan cara mengirim email secara massal sehingga perusahaan yang menjadi korban akan terganggu.

b) *Spam* yang datang bertubi-tubi dapat memenuhi mailbox sehingga mengakibatkan mailserver sibuk sehingga memperlambat layanan yang lain selain itu *spam* juga menghabiskan resource jaringan internet sehingga dikatakan *spam* sebagai *"the biggest waste of bandwidth on the Internet and Usenet."*

c) Dapat menyulitkan seseorang untuk menggunakan internet (*web browsing)* secara normal, misalnya banyaknya iklan atau *advertising* yang memenuhi halaman web ataupun blog-blog yang ingin dicari, hal ini sangat mengganggu pengguna internet apalagi ketika iklan tersebut memenuhi halaman web yg dicari,

selain itu ketika membuka halaman web yang lain keluar jenis iklan promosi yang sama hal ini juga sangat menjengkelkan apabila iklan tersebut sulit untuk di hilangkan.

d) Bagi sesama pemasang iklan. Dimana Pemasang iklan lainnya tentu merasa dirugikan dengan adanya *spamming* karena iklannya tertutup oleh *spam*.

2) Materiil

Selain menimbulkan kerugian immateriil tindakan *spamming* juga dapat merugikan secara materiil misalnya:

a) Karena *spam* dapat dikatakan sebagai *"the biggest waste of bandwidth on the Internet and Usenet"* banyak uang terkuras setiap harinya karena bandwidth yang diperlukan untuk mengirimkan jutaan email *spam*, padahal akhirnya *spam* tersebut akan di *bounce* atau langsung dihapus. Menurut sumber wikipedia, *Internal Market Commision* Uni Eropa memperkirakan pada tahun 2001 biaya penggunaan *spam* surat elektronik adalah 10 milyar Euro per tahun di seluruh dunia, sedangkan di Amerika, *Legislatif California* menemukan bahwa biaya *spam* organisasi Amerika Serikat lebih dari 13 milyar dollar pada tahun 2007, termasuk di dalamnya kehilangan produktivitas dan peralatan, perangkat lunak, dan tenaga kerja yang dibutuhkan untuk memecahkan masalah.

b) Walaupun tidak terlihat tetapi *spam* juga sebagai media penyebaran virus, apabila komputer pengguna telah terjangkit virus yang di bawa oleh *spam* maka dapat menyebabkan kerusakan-kerusakan pada sistem komputer tersebut. Sehingga apabila telah terjadi kerusakan maka diperlukan biaya untuk memperbaiki komputer tersebut, hal ini dapat dikatakan termasuk dalam kerugian materiil.

c) Kerugian yang berikutnya adalah dapat berujung pada penipuan yang dapat merugikan korban dari segi materiil, hal ini disebut juga sebagai akibat tidak langsung korban tindakan *spamming*. Banyak sekali contoh mengenai *spam* penipuan ini misalnya saja berdasarkan Penelitian yang dilakukan oleh *Cisco Security Intelligence Operations* menunjukkan tren meningkatnya serangan-serangan terarah yang terkustomisasi, berisikan malware yang ditujukan bagi pengguna atau kelompok yang spesifik untuk mencuri aset-aset intelektual berharga dimana dalam waktu yang singkat, pelaku kejahatan *cyber* mampu mengeruk keuntungan lebih dari 50 persen dari USD1,1miliar di bulan Juni 2010 menjadi USD 500 juta di bulan Juni 2011, hanya karena menyebar kejahatan dari kiriman email personal korban.[79]

[79] Sumber Sismi Priguna, *Cisco Menganalisis Strategi Baru Spam Telah Merajai Dunia Kejahatan Cyber*,http://chip.co.id/news/read/2011/07/08/930424/Cisco.Menganalisis.Strategi.Baru.Spam.Telah.Merajai.Dunia.Kejahatan.Cyber, di akses pada tanggal 28 Mei 2012.

Gambar 4.9

Contoh iklan promosi *spamming* yang berujung penipuan

Produk Bisnis 5MILYAR

Produk Bisnis 5MILYAR adalah berupa **7 buah buku elektronik** (dalam format EXE dan PDF) yang memuat rahasia-rahasia besar dalam **menghasilkan uang** yang belum pernah terpikirkan bagi sebagian besar orang selama ini. 7 buku elektronik tersebut adalah:

1. **Menciptakan E-Book Penghasil Uang**
   Leonard Setijadi, MBA
2. **Panduan Menjadi Kaya sebagai Karyawan**
   Safiruddin Aziz, MM
3. **Bagaimana Memulai Bisnis di Internet**
   Bryan Winters
4. **Strategi Berburu Uang secara Digital**
   Jeff Mulligan
5. **Rahasia "Making Money" di Internet**
   Bryan Winters
6. **Kiat Sukses Berbisnis Online**
   Bryan Winters
7. **Meraup Dollar dari Menjual Tulisan di Internet**
   Bryan Winters

Anda bisa **download** 7 buku elektronik diatas pada member area setelah bergabung dengan Program Bisnis 5MILYAR.

Ketujuh buku yang sangat berharga diatas bisa anda peroleh dengan harga yang sangat murah sekali, hanya **Rp 180.000**,- saja.

Disamping 7 produk di atas, anda juga akan mendapatkan bonus berupa:

1. **Software Pencari Email**
   Software ini sangat membantu anda mendapatkan ribuan alamat email dalam hitungan detik

Sumber: Data Sekunder diolah, 2012

Gambar diatas adalah salah satu dari sekian banyaknya contoh *spam* yang dapat berujung penipuan, *spam* seperti inilah yang dapat memperbanyak *spammer* karena iklan ini juga menyediakan suatu program untuk membantu mengirim email *spamming*.

d) Selain di dalam dunia maya *spamming* juga sering dilakukan dengan media SMS (*Short Message System*) yang berujung penipuan sehingga mengalami kerugian materiil, di Indonesia *spamming* sendiri dapat dikatakan telah menjadi "*Trendsetter*"

banyak sekali contoh kasus dari penipuan ini dan tidak sedikit pula yang menjadi korban yang mengalami kerugian materiil. Contoh dari SMS *spam* adalah sebagai berikut:

- Pesan Model yang dikirim secara massal hanya untuk promosi semata misalnya:
  - "Pameran Online 2012 Disc 50%, Dapatkan produk dari Blackberry, Nokia, Samsung dll U/INFO HUB:0853-1091-8111. Klik www.planet-ponsel.yolasite.com."
  - "Ajukan pinjaman 100 s/d 750 juta. Tanpa jaminan bebas provisi & potongan. Berhadiah BLACKBERRY. Syarat Fotocopy KTP & Kartu Kredit, Hub: Deko 081807862XXX. Abaikan jika tidak berminat"
- Pesan yang bertujuan untuk penipuan

  Penipuan dengan dalih sebagai kenalan maupun keluarga si korban misalnya:
  - "Ini mama, tolong beliin pulsa 10 ribu aja soalnya penting, nanti kalu sudah masuk hubungi di nomor 0856xxxxxx"
  - "Uangnya transfer ke Bank Mandiri a/n Ahmad Jacky S No rek: 900 000 487 1xxx SMS aja kalo sudah transfer."

Penipuan dengan dalih mendapatkan suatu hadiah

- "Selamat anda mendapatkan hadiah Rp.75 Juta dari Telkomsel Poin di undi di RCTI tadi malam Pukul 23.30 WIB. Hubungi Direktur Kantor Pusat Telkomsel: 081389527xxx Drs.H. Mulyadi. Info pemenang: http://kejutan-poin.webs.com"

- Pesan yang bertujuan untuk penipuan dengan unsur ancaman

  - "aku tahu apa yang anda perbuat, anda telah melanggar hukum, kalau tidak mau perbuatan anda terbongkar, kirimkan uang sejumlah 3 juta ke nomor rekening ini No rek: 900 000 487 1xxx"

Selain beberapa macam-macam kerugian tersebut, terdapat kasus nyata yang terjadi di Indonesia misalnya:

a) Penipuan yang dialami oleh seorang konsumen atau pengguna situs TOKOBAGUS.com yaitu telah terjadi 2 kasus penipuan, kasus tersebut adalah:[80]

- Kasus yang bersumber dari *postingan* F David Talalo, di Forum fotografer.net, dimana korban memberikan informasi mengenai dirinya yang telah menjadi korban penipuan yaitu:

  "Baru baru ini saya tergiur dengan iklan penawaran kamera digital SLR di situs tokobagus.com disitu ditawarkan oleh seorang pengiklan bernama charles

[80] Sumber Kadri, *Penipuan Di Toko Bagus, http://kadri-blog.blogspot.com/2011/03/penipuan-di-tokobagus.html?utm_source=twitterfeed&utm_medium=twitter_083,* di akses pada tanggal 28 Mei 2012.

zhang yg berdomisili di medan, kamera Nikon D200 body only hanya seharga 2,8jt. pengiklan menyertakan alamat lengkap beserta nama toko - Miracle Komputer di Shopping Centre YUKI Suka Ramai Lt.2 no.29 dan nomor telepon 061-76503903. Bodohnya, saya terlanjur mentransfer uang sejumlah 2,8jt ke rekening milik bpk.Syukran. baru kemudian setelah itu konfirmasi dari pihak mall di medan menyatakan bahwa toko itu sudah tutup. barang tidak sampai, nota pembelian pun tidak difax."

- Kasus yang bersumber dari Facebook toko bagus beralamat Facebook.com/tokobagus, dimana korban memberikan informasi mengenai dirinya yang telah menjadi korban penipuan yaitu:

  "Saya di tipu saya kemaren membeli BB torch 9800 dan sudah mentransfer sejumlah Rp.800.000,- Ke BRI dengan NO REK 530601012007534 AN. RICKY EDISYAH PUTRA dengan nomor HP 0857 6086 8349 setelah uang di tranfer HP tidak aktif dan barang pun tidak di trima, saya sangat kecewa steleh belanja OL di situs toko bagus.com"

b) Penipuan yang terjadi terhadap seorang rektor Universitas swasta di Jakarta dengan kerugian sejumlah 1,8 miliar.[81]

Kasus tersebut bermula ketika pada tanggal 3 September 2007 rektor tersebut menerima sebuah email yang berisi penugasan seorang warga Nigeria yang bernama Prince Shanka Moye yang membawa barang senilai US$ 25 Juta ke Indonesia. Barang yang bernilai mahal tersebut milik seorang pengusaha Jerman yang telah mengalami kecelakaan pesawat di Prancis, namun terdapat syarat

[81] Sumber Nala Edwin, *Dikirimi Email, Rektor di Jakarta Tertipu Rp 1,8 Miliar*, http://news.detik.com /read/2007/09/26/162802/834770/10/dikirimi-email-rektor-di-jakarta-tertipu-rp-18-miliar, di akses pada tanggal 28 Mei 2012.

untuk mendapatkan barang berharga tersebut dimana rektor tersebut diminta untuk menyetorkan uang senilai Rp 1,8 miliar untuk biaya administrasi.

Untuk lebih meyakinkan sang korban, Prince Shanka Moye menggunakan sebuah tipu muslihat dimana pelaku mengetahui secara detil mengenai pekerjaan sang rektor, *"Dia tahu betul pekerjaan saya. Dia tahu saya pernah kerja di PBB dan membantu proyek kemanusiaan. Makanya saya tertarik dan percaya,"* kata rektor yang minta agar nama dan universitasnya dirahasiakan ini di Polda Metro Jaya, Jakarta, Rabu (26/9/2007). Setelah masuk perangkap si pelaku, rektor tersebut mentransfer sejumlah uang ke rekening Moye. Rektor tersebut diperintahkan untuk mentransfer uang RP 56,7 juta ke BCA Cabang Mandala pada 6 September 2007.

Kemudian pada hari yang sama, rektor juga bertemu dengan Moye dan dimintai uang Rp 350 juta. Pertemuan tersebut berlanjut, rektor dan Moye bertemu kembali pada 7 September di Hotel Mulia, Senayan Jakarta. Korban mengatakan *"Sudah menjual 2 rumah dan hasil kerja 40 tahun musnah. Saya terlalu menggebu-gebu mendapatkan barang itu. Saya ingin membangun kampus yang membutuhkan dana besar,"*. Setelah uang Rp 1,8 miliar selesai ditransfer, karena barang berharga yang dijanjikan tidak kunjung di dapatkan, kemudian rektor tersebut akhirnya melaporkan modus penipuan ini ke Polda Metro Jaya. Rektor yang dibantu kepolisian

mengatur siasat meringkus Moye dimana keduanya sepakat bertemu di parkiran Hotel Atlet Century Park, Senayan, Jakarta pada 11 September. Saat rektor tersebut akan menyerahkan uang sebesar Rp 100 juta si pelaku Moye kemudian di sergap dan hasilnya Moye berhasil ditangkap, kini Prince Shanka Moye mendekam di Resmob Polda Metro Jaya.

Karena itu melihat sejarah kasus *spamming* di Indonesia dengan jumlah persentase dari tahun ketahun semakin mengkhawatirkan dan melihat macam-macam kerugian atau dampak yang di timbulkan maka wajar apabila jenis kejahatan ini seharusnya di kriminalisasikan.

Suatu peristiwa hukum atau suatu bentuk tindakan dapat di kriminalisasikan harus melalui tahap-tahap dan syarat-syarat yang harus terpenuhi sehingga hasil yang di dapat akan sempurna. Mengenai tahap perumusan suatu tindak pidana adalah berdasarkan kebijakan hukum pidana.

Barda Nawawi Arief memberikan definisi kebijakan hukum pidana (*penal policy / criminal law policy / straf rechts politiek*) yaitu, bagaimana mengusahakan atau membuatan merumuskan suatu perundang-undangan pidana yang baik.[82]

[82] Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana*, *Op.Cit*., hal.25.

Kebijakan hukum pidana atau dalam hal ini secara "*penal*" (pidana) dibagi menjadi 3 tahap yaitu:[83]

a. Tahap kebijakan formulatif atau legislatif

Tahap kebijakan ini berwenang dalam hal menetapkan atau merumuskan perbuatan apa yang dapat dipidana yang berorientasi pada permasalahan pokok dalam hukum pidana meliputi perbuatan yang bersifat melawan hukum, kesalahan atau pertanggungjawaban pidana dan sanksi apa yang nantinya dapat dikenakan oleh pembuat undang-undang.

b. Tahap kebijakan aplikatif atau yudikatif

Tahap kebijakan ini merupakan kekuasaan dalam hal menerapkan hukum pidana oleh alat-alat penegak hukum yaitu misalnya aparat penegak hukum atau pengadilan.

c. Tahap kebijakan eksekutif atau administratif

Tahap kebijakan ini dalam hal melaksanakan hukum pidana oleh aparat pelaksana/eksekusi pidana.

Sedangkan menurut Prof. Sudarto masalah kriminalisasi harus memperhatikan hal-hal yang pada intinya sebagai berikut:[84]

1. Penggunaan hukum pidana harus memperhatikan tujuan pembangunan nasional yaitu mewujudkan masyarakat adil dan makmur yang merata materiil daan spirituil berdasarkan Pancasila. Dalam hal ini penggunaan hukum pidana bertujuan untuk menanggulangi kejahatan dan juga mengadakan penenguhan terhadap

[83] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana Prenada Media Group, Jakarta, 2007, hal.78-79.
[84] Hamdan, *Politik Hukum Pidana*, Raja Garindo, Jakarta, 1997, hal.30-31.

tindakan penanggulangan itu sendiri, demi kesejahteraan daan pengayoman masyarakat.

2. Perbuatan yang diusahakan untuk dicegah atau ditanggulangi dengan hukum pidana harus merupakan perbuatan yang tidak dikehendaki, yaitu perbuatan yang mendatangkan kerugian (materiil dan/atau spirituil) atas warga masyarakat.
3. Penggunaan hukum pidana harus pula memperhitungkan prinsip "biaya dan hasil" (*cost-benefit principle*). Untuk itu perlu diperhitungkan antara besarnya biaya yang dikeluarkan dengan hasil yang diharapkan akan dicapai.
4. Penggunaan hukum pidana harus pula memperhatikan kapasitas atau kemampuan daya kerja dari badan-badan penegak hukum, yaitu jangan sampai ada kelampauan bebas tugas (*over blasting*).

Dari penjelasan Prof. Sudarto dapat diketahui bahwa Kriminalisasi harus memperhatikan hal-hal khusus untuk dapat di kriminalisasikannya tindakan *spamming*, *spamming* sendiri apabila di sesuaikan dengan pernyataan Prof. Sudarto maka dapat dijabarkan yaitu:

1. Dengan di kriminalisasikannya tindakan *spamming* ini otomatis membantu untuk mewujudkan masyarakat adil dan makmur yang merata secara materiil dan spiritual berdasarkan pancasila, melihat dampak yang di timbulkan oleh *spamming* itu sendiri.

2. Perbuatan *spamming* ini berdasarkan data statistik di atas maka dapat dikatakan bahwa tindakan ini adalah "perbuatan yang tidak dikehendaki" yang dapat mendatangkan kerugian.
3. *Spamming* sendiri adalah salah satu kejahatan dunia maya maka harus badan pemerintahan yang khusus untuk menangani masalah ini misalnya Kementerian Komunikasi dan Informatika Republik Indonesia (KEMKOMINFO) yang khusus untuk masalah yang menyangkut dunia maya, sehingga tidak terjadi kelampauan beban tugas (*overblasting*). Dengan cara ini juga meringankan biaya yang akan digunakan karena sudah termasuk bagian kerja dari kementerian ini.

Berdasarkan hal diatas sebagai tambahannya maka untuk melakukan kriminalisasi harus berdasarkan faktor-faktor kebijakan tertentu yang mempertimbangkan bermacam-macam faktor, termasuk:[85]

1. Keseimbangan sarana-sarana yang digunakan dalam hubungannya dengan hasil yang ingin dicapai:
2. Analisa biaya terhadap hasil-hasil yang diperoleh dalam hubungannya dengan tujuan-tujuan yang dicari;
3. Penilaian atau penafsiran tujuan-tujuan yang dicari itu dalam kaitannya dengan prioritas-prioritas lainnya dalam pengalokasian sumber daya manusia;

[85] M. Cherif Bassiouni, *Substantive Criminal Law*, Charles Thomas Publisher, Springfield. Illionis, USA, 1978, hlm 82, dengan menunjuk B, Malinowski,*Crime and Custom in Savage Society*, 1964: dan E. Hoebel, *The Law of Primitive Man*, 1961. Di kutip dari Teguh Prasetyo, *Kriminalisasi Dalam Hukum Pidana*, Nusa Media, Bandung, 2011, hal.39.

4. Pengaruh sosial dari kriminalisasi dan dekriminalisasi yang berkenaan dengan atau dipandang dari pengaruh-pengaruhnya yang sekunder.

Dalam hal ini apabila nantinya tindakan *spamming* dapat di kriminalisasi menjadi suatu tindak pidana maka dirasa penting sekali mencari atau menganalisa sumber bahan yang nantinya akan dipergunakan dalam kebijakan kriminalisasi yang harus didasarkan pada hal-hal sebagai berikut:[86]

1. Masukan dari berbagai penemuan ilmiah
2. Masukan dari beberapa penelitian dan pengkajian mengenai perkembangan delik-delik khusus dalam masyarakat dan perkembangan iptek.
3. Masukan dari pengkajian dan pengamatan bentuk-bentuk serta dimensi baru kejahatan dalam pertemuan/kongres internasional.
4. Masukan dari konvensi internasional.
5. Masukan dari pengkajian perbandingan berbagai KUHP asing.

Mengenai penyebaran *spamming* ini menjadi salah satu *cyber crime* yang dapat dibilang sangat mengkhawatirkan dimana dari tahun ketahun dampak yang ditimbulkan oleh *spam* semakin parah, karena itu sebagian negara-negara besar di dunia menjadikan tindakan *spamming* ini sebagai salah satu yang diutamakan dengan membentuk suatu aturan yang khusus mengawasi dan mengatasi masalah *spamming* ini. Seringkali diadakan konvensi maupun

[86] *Ibid*, hal.42.

pertemuan mengenai perkembangan teknologi saat ini, salah satu yang dibicarakan adalah mengenai penyebaran *spam*.

Di region Asia sendiri dibentuk suatu organisasi atau tim yang dibentuk dari berbagai kelompok yang dikumpulkan dari masing-masing negara asia pasifik, tim ini bernama *Asia Pasific Computer Emergency Response Team* (APCERT), APCERT ini adalah bentuk dari kerjasama atau koalisi dari CERTs (*Computer Emergency Response Teams*) and CSIRTs (*Computer Security Incident Response Teams*) yang dibentuk pada bulan Februari 2003.

Tugas dari tim ini adalah untuk mengumpulkan data-data dari tindakan *cyber crime* yang terjadi di setiap anggota dari APCERT itu sendiri kemudian data tersebut diolah dan dianalisis sehingga gampang untuk dimonitor, selain itu membantu dan bekerja sama untuk mengatasi masalah tersebut dan lain-lan.

> *APCERT akan mempertahankan kontak terpercaya dari ahli jaringan keamanan komputer di wilayah Asia-Pasifik untuk meningkatkan kesadaran daerah dan kompetensi dalam kaitannya dengan insiden keamanan komputer melalui:*
> 1. *meningkatkan Asia-Pasifik regional dan kerjasama internasional terhadap keamanan informasi;*
> 2. *bersama-sama mengembangkan langkah-langkah untuk menangani insiden keamanan jaringan berskala besar atau regional;*
> 3. *memfasilitasi berbagi informasi dan teknologi, termasuk keamanan informasi, virus komputer dan kode berbahaya, antara para anggotanya;*
> 4. *mempromosikan kolaborasi penelitian dan pengembangan mata pelajaran yang menarik bagi anggotanya;*
> 5. *membantu CERT lainnya dan CSIRT di wilayah ini untuk melakukan respon darurat komputer efisien dan efektif;*

6. *memberikan masukan dan / atau rekomendasi untuk membantu menyelesaikan isu-isu hukum terkait dengan keamanan informasi dan tanggap darurat melintasi batas-batas daerah.*[87]

Sehingga dapat dikatakan bahwa telah banyak pihak-pihak yang melakukan berbagai macam penelitian mengenai *cyber crime* yang nantinya dapat digunakan sebagai bahan atau dasar untuk melakukan kriminalisasi, selain itu telah banyak kajian-kajian dan penelitian yang dilakukan oleh peneliti di Indonesia yang menghasilkan berbagai macam data-data yang menyangkut tindakan *spamming* misalnya berupa data statistik atau hasil riset yang dibuat oleh Ahmat Khalil Alkazimy, ST dengan didukung oleh KEMKOMINFO, ID-CERT dan PANDI serta sejumlah responden telah menghasilkan suatu riset independen yang berjudul STATISTIK *ABUSE* INTERNET INDONESIA 2010, dan apabila melihat dampak yang ditimbulkan oleh *spam* ini maka dirasa perlu melakukan kriminalisasi.

Kriminalisasi tidak harus membuat baru Undang-undang mengenai *spamming* tetapi dapat dilakukan dengan tujuan untuk memperbaiki dan menyempurnakan yang telah ada karena dirasa masih "kabur" untuk dapat menjerat pelaku. Muladi dalam bukunya "*Proyeksi Hukum Pidana Material Indonesi di Masa Datang"* menyebutkan bahwa ada tiga metode pendekatan untuk melakukan kriminalisasi, yaitu:[88]

[87] Sumber APCERT Secretariat, *APCERT Annual Report 2009*, di akses pada tanggal 28 Mei 2012
[88] Muladi,Proyeksi Hukum Pidana Material Indonesia di Masa Datang, Pidato Pengukuhan Guru Besar Hukum Pidana, FH-UNDIP, Semarang, 1990, hal.30, di kutip dari Teguh Prasetyo, *Op.Cit.*, hal.42.

1. Metode Evolusioner (*Evolutionary Approach*)

   Metode ini memberikan perbaikan, penyempurnaan dan amandemen terhadap peraturan-peraturan yang sudah lama ada dalam KUHP, misalnya dengan penambahan pasal-pasal tertentu dengan koefisien a, b, c dan seterusnya atau dengan koefisien 'bis' dan 'ter'.

2. Metode Global (*Global Approach*)

   Metode ini dilakukan dengan membuat peraturan tersendiri di luar KUHP, misalnya Undang-Undang Tindak Pidana Korupsi, Undang-Undang Lingkungan Hidup dan lain-lain.

3. Metode Kompromis (*Compromize Approach*)

   Metode ini dilakukan dengan cara menambah bab tersendiri dalam KUHP mengenai tindak pidana tertentu, misalnya tambahan Bab XXIX A dalam KUHP tentang Kejahatan Penerbangan dan Sarana/Prasarana Penerbangan.

Selain dengan metode yang sedemikian rupa dan bahan-bahan serta dasar-dasar yang telah dikumpulkan maka penting untuk mempertimbangkan lebih lanjut dan menganalisanya dengan cermat agar nantinya peraturan yang telah dibuat tidak dibawah standar maupun terlalu mengkriminalisasikan (*under and overcriminalization*) tindak pidana tersebut. Hai ini juga searah dengan bentuk model law yang dibuat oleh *Organization for Economic Co-Operation and Development* (OECD) yang dapat dijadikan dasar acuan dalam

rangka menghindarkan "*under and overcriminalization"* tersebut, prinsip-prinsip dari model law itu mencakup beberapa hal, yaitu:[89]

1. *Ultima Ratio Principl*e

   Hukum pidana disiapkan sebagai sarana terakhir atau senjata pamungkas. Namun dalam kenyataannya, kecenderungan dunia internasional kini sudah mengarah hukum pidana sebagai primum remidium atau dikedepankan, dan juga dalam hal ini mengutamakan pidana denda yang sekaligus dapat digunakan sebagai dana bagi pembangunan di suatu negara.

2. *Precision Principle*

   Ketentuan hukum pidana harus tepat dan teliti menggambarkan suatu tindak pidana. Dalam hal ini harus dihindari perumusan hukum pidana yang bersifat samar dan umum.

3. *Clearness Principle*

   Tindakan yang dikriminalisasikan harus digambarkan secara jelas dalam ketentuan hukum pidana.

4. *Principle of Differentiation*

   Harus jelas perbedaan yang satu dengan yang lain. Hindarkan perumusan yang bersifat global atau terlalu luas, *multipurpose* atau *all embracing*.

[89] S.R. Sianturi dan Mompang L. Panggabean, *Hukum Penitensia di Indonesia,* Alumni Ahaem-Petehaem,Jakarta, 1996, hal.172-173. Lihat juga Muladi dan Barda, *Op.Cit*., hal.34. di kutip dari Teguh Prasetyo, *Op.Cit.*, hal.41.

5. *Principle of Intent*

   Tindakan yang dikriminalisasikan harus dengan dolus (*intention*), sedangkan untuk tindakan culpa (*negligence*) harus dinyatakan dengan syarat khusus untuk memberikan pembenaran kriminalisasinya.

6. *Principle of Victim Application*

   Penyelesaian perkara pidana harus memperhatikan permintaan atau kehendak korban.dalam hal ini kepentingan korban harus diatur dalam rangka pidana dan pemidanaan.

Mengenai bentuk kriminalisasi yang tepat untuk digunakan dalam *spamming* ini penulis dapat menguraikan berdasarkan melihat secara utuh mengenai sebab akibat dari *spam* dengan melihat unsur-unsur yang terdapat dalam peraturan perundang-undangan sampai dengan sanksi yang tepat digunakan untuk tindakan *spamming* ini.

Apabila berbicara mengenai *penal policy* atau maka dapat dikatakan terdapat dua masalah sentral yaitu menetapkan dan merumuskan perbuatan apa yang seharusnya dijadikan tindak pidana dan sanksi apa yang sebaiknya digunakan atau dikenakan pada pelaku.

Dilihat dari bentuk *spamming* yang bermacam-macam maka bentuk pemidanaan terhadap pelaku juga akan berbeda pula dilihat dari bentuk kejahatannya, dimana bentuk-bentuk dari tindakan *spamming* misalnya

a) Sebagai Media Promosi

b) Sebagai media untuk meningkatkan popularitas

c) Sebagai media penipuan

d) Sebagai alat untuk menyebarkan virus maupun Malware

e) Sebagai "Bom Email"

Berdasarkan bentuk diatas maka ancaman hukuman atau jenis pidananya pun seharusnya berbeda, hal ini dikarenakan tingkat kerugian yang akan di derita oleh para korban tindakan *spamming*. Tetapi bentuk perbuatan yang di teliti oleh penulis adalah mengenai tindakan *spamming* yang memiliki pengertian yaitu penyalahgunaan sistem pesan elektronik (termasuk media penyiaran dan sistem pengiriman digital) untuk mengirim berita iklan dan keperluan lainnya secara massal, bertubi-tubi tanpa diminta dan sering kali tidak dikehendaki oleh penerimanya. Sehingga dalam hal ini hanya mengacu pada pengertian tersebut saja.

Sedangkan sanksi pidana yang sebaiknya digunakan atau dikenakan dalam spamming ini pertama-tama mengenai jenis pidana dapat dilihat dalam pasal 10 KUHP dimana:

a. Pidana pokok terdiri atas:
    1) Pidana mati
    2) Pidana penjara
    3) Kurungan
    4) denda
b. Pidana tambahan terdiri atas:
    1) Pencabutan hak-hak tertenu
    2) Perampasan barang-barang tertentu

3) Pengumuman putusan hakim

Sedangkan dalam RUU KUHP tahun 2007 ditentukan jenis-jenis pidana yang dicantumkan dalam pasal 65 sampai dengan pasal 67 yaitu:

Pasal 65 ditentukan mengenai jenis pidana yaitu:

(1) Pidana Pokok terdiri atas
    a. Pidana Penjara;
    b. Pidana Tutupan;
    c. Pidana Pengawasan;
    d. Pidana Denda; dan
    e. Pidana Kerja Sosial.
(2) Urutan Pidana sebagaimana dimaksud pada ayat (1) menentukan berat ringannya pidana.

Pasal 66 yaitu Pidana Mati merupakan pidana pokok yang bersifat khusus dan selalu diancamkan secara alternatif.

Pasal 67 yang berbunyi:

(1) Pidana Tambahan terdiri atas
    a. Pencabutan hak tertentu;
    b. Perampasan barang tertentu dan/atau tagihan;
    c. Pengumuman putusan hakim;
    d. Pembayaran ganti kerugian; dan
    e. Pemenuhan kewajiban adat setempat dan/atau kewajiban menurut hukum yang hidup dalam masyarakat.

(2) Pidana Tambahan dapat dijatuhkan bersama-sama dengan Pidana Pokok, sebagai pidana yang berdiri sendiri atau dapat dijatuhkan bersama-sama dengan pidana tambahan yang lain.

(3) Pidana Tambahan berupa pemenuhan kewajiban adat setempat dan/atau kewajiban menurut hukum yang hidup dalam masyarakat atau pencabutan hak yang diperoleh korporasi dapat dijatuhkan walaupun tidak tercantum dalam perumusan tindak pidana.

(4) Pidana Tambahan untuk percobaan dan pembantuan adalah sama dengan pidana tambahan untuk tindak pidananya.

Dari semua jenis-jenis pidana yang dicantumkan pada KUHP dan RUU KUHP 2007 terdapat perbedaan mendasar mengenai jenis-jenis pidana tersebut sehingga dapat dikatakan bahwa jenis pidana RUU KUHP tahun 2007 dapat dilihat lebih sempurna dari pada KUHP saat ini, maka penulis mencoba memberikan sanksi yang digunakan atau dikenakan berdasarkan RUU KUHP tahun 2007 tersebut. Apabila mempertimbangkan mengenai pidana yang cocok untuk pelaku *spamming*, Barda Nawawi Arief menjelaskan bahwa seyogyanya dalam penjatuhan pidana harus cermat, hati-hati, manusiawi (*humanely*), dan hanya digunakan sebagai *ultimum remedium*.[90]

Berdasarkan hasil studi dalam hukum pidana di 56 negara asing yang dilakukan oleh Widodo, diperoleh kesimpulan bahwa pidana penjara adalah

[90] Widodo, *Sistem Pemidanaan Dalam Cyber Crime Alternatif Ancaman Pidana Kerja Sosial Dan Pidana Pengawasan Bagi Pelaku Cyber Crime*, Laksbang Mediatama, Yogyakarta, 2009, hal.148.

jenis pidana pokok yang paling banyak diancamkan terhadap pelaku *cyber crime*.[91] Pidana penjara (lebih dari 6 bulan) dalam hal ini dirasa terlalu berat digunakan sebagai tolak ukur pemidanaan karena pidana penjara seharusnya dijatuhkan kepada pelaku kejahatan yang secara pantas atau proposional. Shain, seorang Direktur Penelitian dari *judicial Council of California* mengemukakan bahwa perlu adanya pedoman bagi hakim untuk menjatuhkan pidana penjara secara efektif, persyaratan yang membuat tidak layak penjatuhan pidana penjara antara lain:[92]

(1) Terdakwa tidak termasuk penjahat profesional, dan tidak mempunyai riwayat kejahatan yang buruk;
(2) Banyak faktor subjektif yang meringankan terdakwa;
(3) Terdakwa tidak melakukan ancaman maupun menyebabkan penderitaan atau kerugian yang serius terhadap korban;
(4) Ada bukti bahwa terdakwa melakukan tindak pidana karena provokasi dari pihak korban;
(5) Terdakwa bersedia memberikan ganti kerugian atas kerugian material maupun nonmaterial yang diderita korban;
(6) Tidak terdapat cukup alasan yang menunjukkan bahwa terdakwa akan melakukan tindak pidana lagi, atau tidak terdapat cukup indikasi bahwa sifat-sifat jahat terdakwa akan muncul lagi.

Menurut penulis ada beberapa alternatif pidana yang dapat digunakan dalam tindakan *spamming* dalam RUU KUHP tahun 2007 yaitu untuk pidana

[91] *Ibid*, hal.147.
[92] H. Eddy Djunaadi Kamasudirdja, *Beberapa Pedoman Pemidanaan dan Pengamatan Narapidana*, Tanpa Penerbit, 1983, hal.92, lihat dalam *Ibid*, hal.149.

pokok dapat digunakan atau dijatuhkan pidana pengawasan, pidana kerja sosial dan juga pidana denda, selain itu juga dapat digunakan pidana tambahan misalnya pencabutan hak-hak tertentu dll.

Digunakannya pidana-pidana tersebut dikarenakan dilihat dari beberapa faktor dari tindakan *spamming* itu sendiri, hal ini dikarenakan *spamming* berbeda dengan bentuk kejahatan lain (kejahatan konvensional maupun kejahatan *cyber crime* yang lain), misalnya saja karakteristik pelaku biasanya orang-orang yang terpelajar yang menguasai komputer, terhormat, kreatif dan ulet untuk menyebarkan *spam*, lain dengan pelaku kejahatan yang lain karena itu perlu penanganan tersendiri. Hal ini didasarkan pada konsep individualisasi pemidanaan dimana pidana harus sesuai dengan kondisi terpidana dengan memperhatikan asas keseimbangan monodualistik.[93]

Selain itu dampak yang di timbulkan oleh *spamming* ini lebih banyak dampak immaterial walaupun ada beberapa yang berujung penipuan yang menyebabkan kerugian material tetapi dirasa pelaku tindakan *spamming* masih belum pantas untuk dijatuhi pidana penjara, karena itu penentuan jenis pidana yang nantinya dijatuhkan akhirnya tergantung pada faktor-faktor tertentu misalnya kondisi pelaku, kerugian yang nantinya ditimbulkan, dan perasaan hukum dalam masyarakat.

a. Pidana kerja sosial

Pidana kerja sosial adalah jenis pidana berupa pelaksanaan pekerjaan tertentu oleh terpidana di masyarakat tanpa mendapatkan upah yang

[93] *Ibid*, hal.150-151.

diputuskan oleh pengadilan dalam jangka waktu tertentu dan ditentukan tempat pelaksanaannya.

Di berikannya jenis pidana ini mempertimbangkan dari berbagai sisi antara lain hal ini selaras dengan sila kelima pancasila yang didalamnya terkandung nilai bekerja keras dan juga sila ke 2 mengenai kemanusiaan yang adil dan beradap dimana terkandung nilai-nilai pengakuan terhadap martabat manusia sehingga manusia dituntut untuk berlaku adil dan menghormati hak asasi manusia lainnya. Pidana kerja sosial juga dapat digunakan sebagai sarana pencapaian tujuan pemidanaan sebagaimana yang diatur RUU KUHP dalam bagian ke satu paragraf 1 pasal 51, yaitu

(3) Pemidanaan bertujuan:

e. Mencegah dilakukannya tindak pidana dengan menegakkan norma hukum demi pengayoman masyarakat;

f. Memasyarakatkan terpidana dengan mengadakan pembinaan sehingga menjadi orang yang baik dan berguna;

g. Menyelesaikan konflik yang ditimbulkan oleh tindak pidana, memulihkan keseimbangan, dan mendatangkan rasa damai dalam masyarakat; dan

h. Membebaskan rasa bersalah pada terpidana.

(4) Pemidanaan tidak dimaksudkan untuk menderitakan dan merendahkan martabat manusia.

Dalam *Convention on cyber crime* diatur tentang asas-asas pidana dan tindakan, yaitu proposional, mendidik, mengutamakan perlindungan hak asasi terpidana, dan mengarah pada kemanfaatan bagi terpidana.

b. Pidana pengawasan

Mengenai pidana pengawasan tentang penjatuhan pidana bersyarat sebagai pengganti pidana penjara Widodo yang juga selaras dengan hasil penelitian Muladi dimana pidana bersyarat (pidana pengawasan) memiliki keunggulan sebagai berikut:[94]

1. Memberikan kesempatan kepada terpidana untuk memperbaiki diri sendiri dalam masyarakat.
2. Memungkinkan terpidana melanjutkan kegiatan sehari-hari sebagai manusia, sesuai dengan nilai-nilai yang ada dalam masyarakat.
3. Mencegah terjadinya stigma negatif.
4. Memberikan kesempatan kepada terpidana untuk berpartisipasi dalam pekerjaan, yang secara ekonomis menguntungkan masyarakat dan keluarganya.
5. Biaya yang ditanggung oleh negara untuk membina nara pidana lebih murah dibandingkan dengan pidana penjara.
6. Petugas pemasyarakatan sebagai salah satu agen pelaksana pidana pengawasan dapat menggunakan segala fasilitas yang tersedia di masyarakat untuk melakukan rehabilitasi terpidana.

[94] *Ibid*, hal.205.

Dalam *spamming* yang banyaknya hanya menimbulkan kerugian imaterial dan hanya dilakukan untuk motif-motif tertentu misalnya hanya mencoba kemampuan menyebarkan *spam*, menyebarkan *spam* dengan tujuan tertentu missalnya bertujuan menyebarkan bom email dan penyebaran *malware* layak untuk dijatuhi pidana pengawasan

Sedangkan mengenai pelaku tindakan *spamming* tidak hanya dilakukan oleh perorangan tetapi juga dapat dilakukan oleh korporasi, misalnya karena sifatnya *spamming* yang sangat menguntungkan dalam kegiatan promosi iklan maka *spam* banyak digunakan oleh korporasi untuk mengembangkan usahanya, dengan banyaknya kesempatan yang ada untuk mengembangkan korporasi maka juga terbuka kemungkinan untuk terjadinya pelanggaran atau kejahatan.

Mengenai pertanggungjawaban korporasi bukan hanya diarahkan pada pengurus korporasi tersebut, tetapi juga pada korporasi yang melakukan tindak pidana, sehingga dapat dikatakan bahwa ancaman pidana terhadap korporasi yang melakukan kejahatan seharusnya lebih berat dari pada kejahatan yang dilakukan oleh perorangan atau manusia.

Dwidja Priyatno mengemukakan bahwa selain diancam dengan pidana denda, dalam RUU KUHP perlu juga dituangkan ketentuan tentang ancaman sanksi yang tegas terhadap korporasi, yaitu berupa pidana pengawasan (*corporate probation*) dengan disertai syarat membayar ganti kerugian

kepada korban.[95] Untuk pidana denda atau ganti kerugian memang jarang sekali terjadi dalam *spamming*, hal ini bisa saja terjadi apabila telah terjadi penipuan yang menimbulkan kerugian berupa materil sehingga korban merasa dirugikan. Misalnya apabila korporasi menyebarkan promosi berupa iklan produk korporasi tersebut, tetapi berujung pada penipuan yang mengakibatkan kerugian material maka dapat dijatuhi pidana tersebut

Selain pidana denda dan pidana tambahan ganti kerugian penulis juga berpendapat bahwa korporasi juga perlu dijatuhi pidana tambahan berupa pencabutan hak tertentu kepada korporasi misalnya hak untuk menggunakan sarana komputer untuk menyebarkan promosi iklan sehingga nantinya diharapkan apabila hal tersebut dilakukan maka korporasi yang melakukan tindak pidana akan memiliki efek penjera bagi korporasi-korporasi yang lain, karena itu apabila ancama pidana untuk korporasi semakin berat maka pemilik atau pengelola korporasi akan berfikir dua kali jika akan melakukan kebijakan yang dapat mengarah pada tindak pidana dengan segala resiko yang akan di terima oleh korporasi tersebut. Hal ini juga memiliki pertimbangan tertentu dimana korporasi lebih terorganisir daripada perorangan, memiliki modal yang tinggi, dan fasilitas yang mumpuni dari pada perorangan sehingga dapat dikatakan bahwa kejahatan yang dilakukan oleh korporasi akan menimbulkan hasil kejahatan atau kerugian yang lenbih besar dalam masyarakat.

[95] Dwidja Priyatno, *Rancangan KUHP Tak Atur Sanksi Kejahatan Korporasi*, Pikiran Rakyat, 2005. Lihat dalam *Ibid*, hal 212.

C. Pengaturan *Spamming* Dalam Hukum Pidana Di Indonesia

Tindakan *spamming* dapat dikatakan telah menjadi suatu peristiwa pidana karena bersifat merugikan khalayak umum, walaupun memiliki nama yang sama tetapi ternyata *spamming* dapat dikelompokkan menjadi beberapa macam perbuatan secara umum. Pengelompokan ini didasarkan pada dampak akhir atau bentuk kerugian yang di derita oleh korban.

Dalam hukum pidana Indonesia sulit untuk menentukan peraturan mana yang dapat dipergunakan dalam tindakan *spamming*, terlebih dengan adanya asas *"lex specialis derogat lex generalis"* yang memiliki arti peraturan yang khusus mengesampingkan peraturan yang umum, sesuai dengan adanya asas ini maka metode penerapannya terhadap kasus kongret harus ditelusuri mulai dari sumber hukum pidana yang paling khusus hingga paling umum.

Dalam ilmu hukum dikenal berbagai metode interpretasi, mulai dari penafsiran gramatikal hingga penafsiran analogi, berkaitan dengan asas legalitas (*nullum delictum*) pada pasal 1 (1) KUHP yang berbunyi *"Suatu perbuatan tidak dapat dipidana, kecuali berdasarkan kekuatan ketentuan-ketentuan perundang-undangan pidana yang telah ada"*

Asas tersebut merupakan sendi utama dalam hukum pidana, maka diupayakan agar dihindari penafsiran yang bersifat analogi (paling banter penafsiran ekstensif masih dapat dipakai).[96]

[96] Wisnubroto, *Strategi Penanggulangan Kejahatan Telematika,* Atma Jaya Yogyakarta, Semarang, 2010. Hal.122.

spamming sendiri adalah salah satu kejahatan dunia maya dan seharusnya terdapat didalam peraturan yang mengatur mengenai *cyber crime* yaitu Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Apabila dilihat kebelakang dari penjelasan mengenai unsur-unsurnya maka tindakan *spamming* ini masih terlihat kabur didalam Undang-Undang tersebut, maka dalam hal ini akan dicari atau dianalisis peraturan-peraturan didalam hukum pidana Indonesia yang sekiranya mampu untuk mengatasi masalah *spamming* ini.

1. Ketentuan dalam Kitab Undang-Undang Hukum Pidana (KUHP)

Sebenarnya dalam KUHP tidak ada suatu peraturan yang dapat digunakan untuk tindakan *spamming* ini, tetapi apabila dilihat mengenai bentuk kerugian yang diterima maka terdapat peraturan yang dapat digunakan dalam tindakan *spamming* peraturan tersebut yaitu pada pasal 378 dalam BAB XXV tentang perbuatan curang yang berbunyi:

> *"Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun."*

Pasal ini dipergunakan karena apabila melihat dampak yang ditimbulkan oleh tindakan *spamming*, dimana salah satunya *spamming* ini dapat berujung pada tindakan penipuan walau tidak setiap *spamming* mengandung penipuan.

Disebut penipuan dalam *spamming*, dimana pelaku berhasil memperdaya korban untuk percaya akan tipu muslihat pelaku. Hasil yang diharapkan dari tipu muslihat ini adalah korban ditipu dengan cara iklan promosi yang mengandung penipuan disebarkan sehingga korban merasa tertarik dengan iklan promosi tersebut akhirnya korban akan mudah dikelabui. Unsur penipuan menurut pasal 378 KUHP adalah:

1. Unsur obyektif
    a) Menggerakkan
    b) Orang lain
    c) Untuk menyerahkan suatu barang / benda
    d) Untuk memberi hutang
    e) Untuk menghapuskan piutang
    f) Dengan menggunakan daya upaya seperti
        1) Memakai nama atau
        2) Martabat palsu
        3) Dengan tipu muslihat, dan
        4) Rangkaian kebohongan
2. Unsur subyektif
    a) Dengan maksud
    b) Untuk menguntungkan diri sendiri atau orang lain
    c) Secara melawan hukum

Menggerakkan dapat didefinisikan sebagai perbuatan mempengaruhi atau menanamkan pengaruh pada orang lain, dimana obyek yang dipengaruhi adalah kehendak seseorang. Unsur menggerakkan orang lain berarti penggunaan tindakan-tindakan, baik berupa perbuatan-perbuatan maupun perkataan-perkataan yang bersifat menipu.[97]

Bila dikaitkan dengan *spamming*, maka unsur menggerakkan orang lain terdapat pada saat pelaku mengirimkan e-mail iklan promosi palsu sehingga nantinya korban akan terperdaya sehingga tujuan dari pelaku yaitu penipuan akan terlaksana.

Mengenai menyerahkan suatu benda dapat diartikan sebagai menyerahkan suatu barang berwujud. Namun pada perkembangannya, pengertian benda atau barang tidak hanya terbatas pada barang atau benda bergerak saja, tetapi juga termasuk barang tidak berwujud atau tidak bergerak.[98] Menyerahkan suatu benda tidak harus dilakukan sendiri secara langsung oleh korban kepada pelaku. Tetapi juga dapat dilakukan oleh korban kepada suruhan dari pelaku. Penyerahan barang merupakan akibat langsung dari upaya pelaku, sebagai akibat dari adanya unsur kesengajaan si pelaku. Oleh karena itu, perbuatan menyerahkan yang dilakukan oleh korban dan daya upaya dari pelaku harus merupakan suatu hubungan kausal.

Begitu juga mengenai memberikan hutang maupun menghapuskan piutang, dalam hal ini pelaku mencoba untuk menipu korban dengan cara

[97] Tongat, *Hukum Pidana Materiil*, UMM Press, Malang, 2003, hal.73. lihat dalam Skripsi Ki Jagat Tomara, Kajian *Yuridis Pertanggungjawaban pidana Penyedia Jasa Internet dan Pemilik Domain Kasus Phising*, Malang, 2011, hal.72-73.
[98] *Ibid*, hal.73

seolah-olah membuat suatu bentuk perikatan yang nantinya mengharuskan korban untuk menyerahkan ataupun memberikan sejumlah uang atau barang tertentu, sedangkan mengenai menghapuskan piutang akan berkebalikan dengan memberikan hutang yaitu meniadakan perikatan.

Apabila dihubungkan dengan tindakan *spamming* maka dapat dikatakan bahwa perbuatan *spamming* akan menjadi sebuah bentuk penipuan apabila korban terpedaya oleh pelaku dengan cara menyerahkan, memberikan hutang maupun menghapuskan piutang, misalnya apabila didalam penyebaran *spam* yang berbentuk iklan promosi, apabila korban tertarik untuk membeli suatu barang pada iklan tersebut, setelah uang terkirim ternyata barang yang dijanjikan dalam iklan tersebut bukanlah barang yang dijanjikan atau bisa saja barang tersebut tidak terkirim. Maka dalam hal telah terjadi sebuah penipuan yang berkedok iklan promosi pada e-mail, contoh lain pada kasus sms massal yang mengharuskan korban untuk mengirim ataupun mentrasfer sejumlah uang ataupun barang kepada pengirim sms.

Mengenai penipuan dengan menggunaan nama palsu, atau martabat palsu dimaksudkan untuk menyebutkan jati dirinya dalam suatu keadaan yang tidak benar, yang bertujuan untuk membuat korban percaya, sehingga dengan kepercayaan itu ia akan menyerahkan suatu barang atau memberikan hutang maupun menghapuskan piutang. Memakai nama palsu terjadi apabila pelaku menggunakan nama yang bukan namanya. Sedangkan penggunaan martabat palsu terjadi apabila pelaku menggunakan pangkat, atau jabatan, atau kedudukan yang bukan sebenarnya.

Dalam kasus *spamming* sering dijumpai hal-hal seperti ini misalnya dalam kasus sms *spam*, pelaku mengaku sebagai anggota keluarga ataupun sebagai kenalan korban kemudian mencoba meminta sejumlah uang ataupun meminta untuk mengisikan sejumlah pulsa sehingga korban akan mengira bahwa pengirim sms memang benar kenalannya sehingga telah terjadi penipuan. Hal ini juga sering dilakukan dengan cara tipu muslihat dan rangkaian kebohongan dimana pelaku bertujuan untuk menipu korban sehingga dengan cara ini maka akan menimbulkan suatu kepercayaan kepada pelaku sehingga seolah-olah apa yang diungkapkan oleh pelaku itu adalah benar adanya.

Dalam RUU KUHP tahun 2007 sebenarnya terdapat pasal yang kemungkinan dapat dipergunakan dalam *spamming* yaitu dalam pasal 26 ayat 1 yang berbunyi:

> *"Setiap orang yang dengan sengaja dan melawan hukum menggunakan surat elektronik untuk mengumumkan, menawarkan atau menjual barang dan atau jasa yang sifatnya melanggar hukum atau dilarang oleh Undang-Undang, dipidana penjara paling singkat 1 (satu) tahun dan paling lama 3 (tiga) tahun."*

Dalam pasal 26 (1) RUU KUHP tahun 2007 ini dirasa paling mendekati dalam kaitannya dengan tindakan *spamming*, apabila dijabarkan pasal ini diperuntukkan untuk penyebaran iklan promosi yang berujung pelanggaran sehingga rumusan unsur-unsur dari *spamming* itu sendiri dirasa lebih pas dan mendekati.

2. Ketentuan dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Telah dijelaskan di bab sebelumnya dimana dalam Undang-undang ITE Indonesia masih belum jelas atau dirasa masih kabur mengenai *spamming*, tetapi dalam pembahasan ini akan dijelaskan mengenai pasal-pasal yang mendekati tindakan *spamming* ini.

Dalam Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik pasal yang paling mendekati tindakan *spamming* ini adalah pasal 28 yang berbunyi sebagai berikut:

> *(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).*

Dari pasal 28 tersebut Drs. Adami Chazawi, S.H. dalam bukunya menyebutkan bahwa dalam ayat (1) terdiri dari unsur-unsur sebagai berikut:[99]

1. Kesalahan : *dengan sengaja;*
2. Melawan hukum : *tanpa hak;*
3. Perbuatan : *menyebarkan;*
4. Objek : *berita bohong dan menyesatkan;*
5. Akibat konstitutif : *mengakibatkan kerugian konsumen dalam transaksi elektronik.*

[99] Adami Chazawi dan Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik: Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik*, Bayumedia Publishing, Malang, 2011, hal.128.

Sedangkan ayat (2) terdiri dari unsur-unsur sebagai berikut :

1. Kesalahan : *dengan sengaja;*
2. Melawan hukum : *tanpa hak;*
3. Perbuatan : *menyebarkan;*
4. Objek : *informasi;*
5. Tujuan : *untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras dan antar golongan (SARA).*

Apabila dibandingkan dengan tindakan *spamming* maka akan didapatkan unsur-unsur dari tindakan *spamming* sebagai berikut:

1. Kesalahan : *dengan sengaja*;
2. Melawan hukum : *tanpa hak*;
3. Perbuatan : *menyebarkan secara massal*;
4. Objek : *informasi berupa promosi ataupun berita*;
5. Akibat : *dapat mengakibatkan kerugian konsumen dalam transaksi elektronik.*

Dalam tindakan *spamming* memang sangat kontradiktif apabila digunakan pasal 28 ayat 1 ini, apabila dijabarkan mengenai unsur-unsurnya maka akan didapati sebagai berikut

Pertama didalam unsur kesalahaan pelaku memang sadar akan perbuatannya atau memiliki kesengajaan untuk menyebarkan *spamming* tersebut dimana dengan cara yang ilegal atau dengan tanpa hak, tanpa hak ini

berarti pelaku memang tidak memiliki hak untuk mengirimkan *spam* sehingga dapat dikatakan tidak berhaknya pelaku disebabkan karena pelaku memang secara nyata bukanlah orang yang berhak atau berwenang menyebarkan berita tersebut.

Mengenai jenis perbuatannya maka dalam pasal 28 ayat 1 jenis perbuatannya adalah menyebarkan berita bohong dan tidak benar dengan ditambah unsur menyesatkan pada rumusan pasal tersebut, sehingga pelaku berusaha untuk menggerakkan korban untuk melakukan sesuatu. Dalam pasal ini dapat dikatakan bahwa objek yang disebarkan adalah hanya dalam ruang lingkup suatu berita kebohongan dan menyesatkan belaka.

Dalam tindakan *spamming* memang juga perbuatannya menyebarkan, tetapi apabila di telaah secara lebih mendalam maka bentuk penyebaran ini bersifat lebih luas dari pada bentuk penyebaran dalam pasal 28 ayat (1). Sehingga penyebaran dalam *spamming* ini bersifat massal. Yang paling kontradiktif dalam perbandingan ini adalah mengenai objeknya, dalam pasal 28 ayat (1) objeknya adalah berita bohong dan menyesatkan sedangkan dalam ayat (2) dari pasal 28 menyebutkan bahwa objeknya adalah berupa informasi, sedangkan dalam tindakan *spamming* objeknya adalah suatu berita iklan ataupun informasi yang lain sehingga apabila dibandingkan maka objek yang didapati adalah berbeda dari pasal 28 ayat (1).

Sedangkan ayat (2) walaupun objeknya adalah informasi tetapi informasi tersebut hanya ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan

atas suku, agama, ras dan antar golongan (SARA) lain halnya dengan *spamming* yang bertujuan untuk menyebarkan suatu iklan promosi ataupun informasi lain.

Dalam hal akibatnya pasal 28 ayat (1) memiliki akibat konstitutif mengakibatkan kerugian konsumen dalam transaksi elektronik, sehingga dapat dikatakan bahwa dalam hubungannya dengan unsur-unsur yang lain bahwa pelaku memang sengaja atau menghendaki menyebarkan berita bohong dan juga menyesatkan sehingga menyadari nantinya akan timbul akibat kerugian pada korbannya, sedangkan dalam *spamming* pelaku dengan sengaja atau menghendaki menyebarkan berita iklan atau promosi serta informasi yang lain dengan tujuan mempermudah promosi suatu iklan tertentu. Kaitannya dengan bentuk kerugian, tindakan ini dapat menimbulkan kerugian pada korban termasuk juga terdapat unsur penipuan, telah dijelaskan di atas mengenai kerugian dalam tindakan *spamming* dimana kerugian yang dimaksud, tidak hanya kerugian yang dapat dinilai dengan uang, tetapi juga segala bentuk kerugian. Misalnya timbulnya perasaan cemas, malu, kesusahan, hilangnya harapan mendapatkan kesenangan atau keuntungan dan sebagainya.[100]

Contohnya dalam *spamming* pelaku memang berniat atau sengaja untuk menyebarkan iklan promosi tersebut secara massal dengan tujuan untuk promosi, dengan cara ini akan mempermudah dalam menyebarkan secara luas atau massal, tidak mengeluarkan biaya dan mudah, sehingga dapat dikatakan

[100] *Ibid*, hal.131.

bahwa *spam* digunakan sebagai media penjualan tetapi dalam perkembangannya *spam* tidak lagi digunakan hanya sebagai media promosi tetapi juga dengan alasan-alasan yang lain misalnya iklan *spam* yang memang sengaja bersifat penipuan dimana tujuan dari pelaku hanya ingin keuntungan belaka.

Mengenai sanksi pidana dalam Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Infomasi dan Transaksi Elektronik terdapat dalam pasal 45 ayat (2) yang berbunyi:

> *"Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 28 ayaty (1) atau ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp.1.000.000.000,00 (satu miliar rupiah)."*

Tindakan *spamming* dilakukan juga oleh korporasi sehingga sanksi pidananya pun berbeda, dalam Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Infomasi dan Transaksi Elektronik mengenai sanksi terhadap korporasi diatur dalam pasal 52 ayat (4) yang berbunyi:

> *"Dalam hal tindak pidana sebagaimana dimaksud dalam pasal 27 sampai dengan pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga."*

3. Ketentuan dalam Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen

Sebenarnya dalam hal *spamming* peraturan yang digunakan seharusnya adalah Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik karena *spamming* adalah salah satu dari kejahatan dunia maya, tetapi apabila ditelaah maka peraturan *spamming* dapat

dikatakan masih belum jelas atau terdapat kekaburan. Dalam kaitannya dengan ini maka penting untuk melihat dalam Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen karena berkaitan dengan kerugian yang diderita oleh konsumen yang terkena suatu bentuk penipuan didalam iklan *spamming*. Pasal-pasal dalam undang-undang ini yang sekiranya dapat digunakan apabila telah terjadi suatu tindakan penipuan adalah sebagai berikut:

1. Pasal 8

   1 Pelaku usaha dilarang memproduksi dan/atau memperdagangkan barang dan/atau jasa yang:
   a. tidak memenuhi atau tidak sesuai dengan standar yang dipersyaratkan dan ketentuan peraturan perundang-undangan;
   b. tidak sesuai dengan berat bersih, isi bersih atau neto, dan jumlah dalam hitungan sebagaimana yang dinyatakan dalam label atau etiket barang tersebut;
   c. tidak sesuai dengan ukuran, takaran, timbangan dan jumlah dalam hitungan menurut ukuran yang sebenarnya;
   d. tidak sesuai dengan kondisi, jaminan, keistimewaan atau kemanjuran sebagaimana dinyatakan dalam label, etiket atau keterangan barang dan/atau jasa tersebut;
   e. tidak sesuai dengan mutu, tingkatan, komposisi, proses pengolahan, gaya, mode, atau penggunaan tertentu sebagaimana dinyatakan dalam label atau keterangan barang dan/atau jasa tersebut;
   f. tidak sesuai dengan janji yang dinyatakan dalam label, etiket, keterangan, iklan atau promosi penjualan barang dan/atau jasa tersebut;
   g. tidak mencantumkan tanggal kadaluwarsa atau jangka waktu penggunaan/ pemanfaatan yang paling baik atas barang tertentu;
   h. tidak mengikuti ketentuan berproduksi secara halal, sebagaimana pernyataan "halal" yang dicantumkan dalam label;
   i. tidak memasang label atau membuat penjelasan barang yang memuat nama barang, ukuran, berat/isi bersih atau netto, komposisi, aturan pakai, tanggal pembuatan, akibat sampingan, nama dan alamat pelaku usaha serta keterangan lain untuk penggunaan yang menurut ketentuan harus dipasang/dibuat;

j. tidak mencantumkan informasi dan/atau petunjuk penggunaan barang dalam bahasa Indonesia sesuai dengan ketentuan perundang-undangan yang berlaku.

2 Pelaku usaha dilarang memperdagangkan barang yang rusak, cacat atau bekas, dan tercemar tanpa memberikan informasi secara lengkap dan benar atas barang dimaksud.

3 Pelaku usaha dilarang memperdagangkan sediaan farmasi dan pangan yang rusak, cacat atau bekas dan tercemar, dengan atau tanpa memberikan informasi secara lengkap dan benar.

4 Pelaku usaha yang melakukan pelanggaran pada ayat (1) dan ayat (2) dilarangmemperdagangkan barang dan/atau jasa tersebut serta wajib menariknya dari peredaran

2. Pasal 9

1 Pelaku usaha dilarang menawarkan, memproduksikan, mengiklankan suatu barang dan/atau jasa secara tidak benar, dan/atau seolah-olah:
   a. barang tersebut telah memenuhi dan/atau memiliki potongan harga, harga khusus, standar mutu tertentu, gaya atau mode tertentu, karakteristik tertentu, sejarah atau guna tertentu;
   b. barang tersebut dalam keadaan baik dan/atau baru;
   c. barang dan/atau jasa tersebut telah mendapatkan dan/atau memiliki sponsor, persetujuan, perlengkapan tertentu, keuntungan tertentu, ciri-ciri kerja atau aksesori tertentu;
   d. barang dan/atau jasa tersebut dibuat oleh perusahaan yang mempunyai sponsor, persetujuan atau afiliasi;
   e. barang dan/atau jasa tersebut tersedia;
   f. barang tersebut tidak mengandung cacat tersembunyi;
   g. barang tersebut merupakan kelengkapan dari barang tertentu;
   h. barang tersebut berasal dari daerah tertentu;
   i. secara langsung atau tidak langsung merencahkan barang dan/atau jasa lain;
   j. menggunakan kata-kata yang berlebihan, seperti aman, tidak berbahaya, tidak mengandung risiko atau efek sampingan tampak keterangan yang lengkap;
   k. menawarkan sesuatu yang mengandung janji yang belum pasti.

2 Barang dan/atau jasa sebagaimana dimaksud pada ayat (1) dilarang untuk diperdagangkan.

3 Pelaku usaha yang melakukan pelanggaran terhadap ayat (1) dilarang melanjutkan penawaran, promosi, dan pengiklanan barang dan/atau jasa tersebut.

3. Pasal10

Pelaku usaha dalam menawarkan barang dan/atau jasa yang ditujukan untuk diperdagangkan dilarang menawarkan, mempromosikan, mengiklankan atau membuat pernyataan yang tidak benar atau menyesatkan mengenai:

a. harga atau tarif suatu barang dan/atau jasa;
b. kegunaan suatu barang dan/atau jasa;
c. kondisi, tanggungan, jaminan, hak atau ganti rugi atas suatu barang dan/atau jasa;
d. tawaran potongan harga atau hadiah menarik yang ditawarkan;
e. bahaya penggunaan barang dan/atau jasa.

4. Pasal 11

Pelaku usaha dalam hal penjualan yang dilakukan melalui cara obral atau lelang, dilarang mengelabui/menyesatkan konsumen dengan;

a. menyatakan barang dan/atau jasa tersebut seolah-olah telah memenuhi standar mutu tertentu;
b. menyatakan barang dan/atau jasa tersebut seolah-olah tidak mengandung cacat tersembunyi;
c. tidak berniat untuk menjual barang yang ditawarkan melainkan dengan maksud untuk menjual barang lain;
d. tidak menyediakan barang dalam jumlah tertentu dan/atau jumlah yang cukup dengan maksud menjual barang yang lain;
e. tidak menyediakan jasa dalam kapasitas tertentu atau dalam jumlah cukup dengan maksud menjual jasa yang lain;
f. menaikkan harga atau tarif barang dan/atau jasa sebelum melakukan obral.

5. Pasal 12

Pelaku usaha dilarang menawarkan, mempromosikan atau mengiklankan suatu barang dan/atau jasa dengan harga atau tarif khusus dalam waktu dan jumlah tertentu, jika pelaku usaha tersebut tidak bermaksud untuk melaksanakannya sesuai dengan waktu dan jumlah yang ditawarkan, dipromosikan, atau diiklankan.

6. Pasal 13

1. Pelaku usaha dilarang menawarkan, mempromosikan, atau mengiklankan suatu barang dan/jasa dengan cara menjanjikan

pemberian hadiah berupa barang dan/atau jasa lain secara cuma-cuma dengan maksud tidak memberikannya atau memberikan tidak sebagaimana yang dijanjikannya.

2. Pelaku usaha dilarang menawarkan, mempromosikan atau mengiklankan obat, obat tradisional, suplemen makanan, alat kesehatan, dan jasa pelayanan kesehatan dengan cara menjanjikan pemberian hadiah berupa barang dan/atau jasa lain.

7. Pasal 14

Pelaku usaha dalam menawarkan barang dan/atau jasa yang ditujukan untuk diperdagangkan dengan memberikan hadiah melalui cara undian, dilarang untuk:

a. tidak melakukan penarikan hadiah setelah batas waktu yang dijanjikan;
b. mengumumkan hasilnya tidak melalui media massa;
c. memberikan hadiah tidak sesuai dengan yang dijanjikan;
d. mengganti hadiah yang tidak setara dengan nilai hadiah yang dijanjikan.

8. Pasal 15

Pelaku usaha dalam menawarkan barang dan/atau jasa yang dilarang melakukan dengan cara pemaksaan atau cara lain yang dapat menimbulkan gangguan baik fisik maupun psikis terhadap konsumen.

9. Pasal 16

Pelaku usaha dalam menawarkan barang dan/atau jasa melalui pesanan dilarang untuk:

a. tidak menepati pesanan dan/atau kesepakatan waktu penyelesaian sesuai dengan yang dijanjikan;
b. tidak menepati janji atas suatu pelayanan dan/atau prestasi.

10. Pasal 17

1 Pelaku usaha periklanan dilarang memproduksi iklan yang:
   a. mengelabui konsumen mengenai kualitas, kuantitas, bahan, kegunaan dan harga barang dan/atau tarif jasa serta ketepatan waktu penerimaan barang dan/atau jasa;
   b. mengelabui jaminan/garansi terhadap barang dan/atau jasa;

c. memuat informasi yang keliru, salah, atau tidak tepat mengenai barang dan/atau jasa;
d. tidak memuat informasi mengenai risiko pemakaian barang dan/atau jasa;
e. mengeksploitasi kejadian dan/atau seseorang tanpa seizin yang berwenang atau persetujuan yang bersangkutan;
f. melanggar etika dan/atau ketentuan peraturan perundang-undangan mengenai periklanan.

2 Pelaku usaha periklanan dilarang melanjutkan peredaran iklan yang telah melanggar ketentuan pada ayat (1).

Bentuk pelarangan yang disebutkan dari pasal 8 sampai dengan pasal 17 Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen diharapkan dapat melindungi hak-hak dari seseorang sebagai konsumen dimana apabila terjadi suatu pelanggaran maka dapat digunakan salah satu dari sepuluh pasal ini.

Hubungannya dengan tindakan *spamming*, sebagai korban *spamming* yang dapat dikatakan sebagai konsumen karena objek dari tindakan *spamming* itu sendiri yaitu menyebarkan secara massal iklan promosi suatu barang, sehingga apabila terjadi pelanggaran ataupu penipuan terjadi pada kasus *spamming*, maka masih dapat dimungkinkan dipergunakannya salah satu dari pasal yang tercatum di dalam Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen tergantung dari macam pelanggaran dan akibat atau bentuk kerugian yang diderita oleh korban atau konsumen.