

BAB I PENDAHULUAN

A. LATAR BELAKANG

Manusia adalah makhluk yang dianugerahi akal dan pikiran oleh Tuhan Yang Maha Esa. Pemikiran manusia senantiasa berkembang mengikuti pola perkembangan jaman. Dengan berkembangnya manusia, maka berkembang pula kebutuhannya. Karena pada dasarnya, keinginan manusia itu tidak terbatas, walaupun pada kenyataannya alat pemuas kebutuhannya yang terbatas. Oleh sebab itu, manusia dituntut untuk banyak melakukan berbagai terobosan dan inovasi untuk mencapai tingkat kepuasan maksimum dalam rangka pemenuhan kebutuhannya. Namun manusia selalu tidak pernah merasa puas. Melalui pengetahuannya, manusia selalu ingin terus melakukan inovasi yang lebih dan lebih jauh lagi, hal seperti inilah yang sering kita kenal sebagai perkembangan teknologi.

Perkembangan teknologi sejalan dengan perkembangan pengetahuan manusia. Pada zaman dahulu manusia hanya menggunakan peralatan seadanya dan sederhana untuk menunjang kehidupannya. Namun sekarang, peralatan-peralatan penunjang kehidupan manusia jauh lebih canggih dan lebih kompleks. Teknologi merupakan salah satu ciri khusus kemuliaan manusia bahwa dirinya tidak hidup dengan makanan semata. Teknologi adalah sebuah manifestasi langsung dari bukti kecerdasan manusia.¹

¹Aji Dedi Mulawarman, 2008, *Pengertian Teknologi (online)*, <http://ajidedim.wordpress.com/teknologi-islami/technology/>, di akses pada tanggal 22 Februari 2011.

Teknologi Informatika pada periode ini telah berkembang dengan pesat sehingga menyebabkan dunia yang tanpa batas dan secara langsung maupun tidak langsung mengubah pola hidup dan perilaku masyarakat di dunia yang dapat menyebabkan perubahan dalam hidup mereka misalnya perubahan sosial, ekonomi, budaya dan tidak menutup kemungkinan dalam hal penegakan hukum di dunia. Khususnya di dalam dunia maya yang sangat mudah diakses oleh setiap orang di seluruh dunia untuk dimanfaatkan sebagai sarana kebutuhan sehari-hari dari kebutuhan sosial misalnya pembuatan website, sarana informasi, sarana hiburan, tempat untuk mempublikasikan karya mereka maupun yang paling sering di gunakan adalah untuk sarana perdagangan.

Karena sifatnya yang sangat luas, dunia maya juga menjadi sarana untuk tempat terjadinya suatu kejahatan-kejahatan yang disebut juga sebagai kejahatan siber atau *Cyber Crime*, bagi beberapa orang kejahatan siber ini hanya dalam ruang lingkup kejahatan penipuan, hacker, penyebaran berita palsu maupun penyebaran suatu hal yang mengandung unsur pornografi, tetapi bukan hal tersebut saja yang dapat dikatakan sebagai *Cyber Crime* banyak sekali bentuk kejahatan lain yang masih asing yang juga termasuk di dalam kategori *Cyber Crime*, salah satu dari kejahatan tersebut adalah kejahatan *Spam* atau disebut sebagai *Spamming*. *Spam* sendiri memiliki arti sebagai penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi para pengguna web, *Spam* ini biasanya datang dengan cara bertubi-tubi tanpa diminta dan sering kali tidak

dikehendaki oleh penerimanya. Banyak memberikan pengertian pada *spam* misalnya pada situs <http://spam.abuse.net/overview/whatisspam.shtml> yaitu:²

“Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.”

Kebanyakan orang di seluruh dunia menganggap *spam* hanya terdapat pada Email namun sesuai dengan perkembangan teknologi yang semakin hari semakin tidak terkendali, dan dunia maya pun semakin meluas. Sehingga *spam* tidak hanya terbatas pada email saja namun juga terdapat pada situs-situs, blog dan lain-lain. *Spam* pada Blog biasanya berisi iklan menjengkelkan dan mengarahkan pada situs yang berkualitas rendah atau situs berbahaya yang mengandung penipuan atau berita bohong.

Biasanya *spam* dikirim dengan tujuan tertentu misalnya sebagai media publikasi dan promosi untuk produk-produk perusahaan si pengirim email sampah ataupun *spammer* (sebutan untuk pengirim *spam*). misalnya sebuah perusahaan tertentu ingin menjual barang produksi mereka, jika melalui advertising atau periklanan tentu akan memakan biaya yang cukup mahal, dengan menggunakan cara ini maka perusahaan tersebut akan dapat mengirim email sebanyak-banyaknya ke seluruh pemilik email yang ada di dunia ini. Tujuan yang kedua yaitu *spam* biasanya di gunakan sebagai “Bom email”, jika anda memiliki musuh di internet atau saingan perusahaan biasanya dengan cara bom email ini dilakukan agar anda repot menerima email yang tidak di perlukan dalam jumlah yang besar dan secara

²Sumber Scott Hazen Mueller, *What is Spam ?*, <http://spam.abuse.net/overview/whatisspam.shtml>, di akses pada tanggal 10 November 2011.

terus menerus. *Spamming* juga sering digunakan sebagai media penyebaran virus & worm, yang merupakan karakter dari virus dan worm untuk menyebarkan filenya secara otomatis ke seluruh pemilik email yang ada di dunia ini, dengan tujuan akan mendapatkan korban yang sebanyak-banyaknya. *Spam* bisa menjadi tidak terkendali karena sebagian besar spam tidak dibuat secara manual oleh *spammer* manusia. *Spammer* tersebut biasanya menggunakan program komputer yang disebut dengan *Autobots*, yang secara otomatis mengisi formulir Web untuk menciptakan *spam*, dan ini yang membuat spam bots jauh lebih cepat daripada kemampuan kita dalam melakukan pengecekan.

Contohnya di dalam kehidupan sehari-hari, kita juga sering mendapatkan perlakuan spamming ini, misalnya seseorang yang mempromosikan sesuatu hal dengan cara menyebarkan brosur, pamflet maupun yang lainnya dalam jumlah yang banyak di halaman rumah, di sweeper kaca mobil, dan yang baru-baru ini gencar terjadi adalah kasus “SMS MAMA” dimana kronologinya adalah si pengirim sms mengaku sebagai ibu, anak ataupun kenalan dari si penerima sms, dan kasus-kasus yang lainnya. Kasus macam ini saya sebut sebagai *spam* karena mereka tidak meminta izin terlebih dahulu apakah kita mau diberi brosur atau tidak. Lain halnya jika mereka menawarkan terlebih dahulu brosur tersebut dan menanyakan apakah mau menerima brosur ataupun tidak.

Mengenai kerugian *spamming* menurut sumber wikipedia, *Internal Market Commision* Uni Eropa memperkirakan pada tahun 2001 biaya penggunaan *spam* surat elektronik adalah 10 milyar € per tahun di seluruh dunia. Legislatif California menemukan bahwa biaya *spam* organisasi Amerika Serikat saja lebih

dari \$ 13 milyar pada tahun 2007, termasuk di dalamnya kehilangan produktivitas dan peralatan, perangkat lunak, dan tenaga kerja yang dibutuhkan untuk memecahkan masalah. Efek langsung *spam* mencakup konsumsi dari komputer dan jaringan sumber daya, dan biaya terkait waktu dan perhatian untuk mengabaikan pesan yang tidak diinginkan. Selain itu, *spam* memiliki biaya yang berasal dari jenis-jenis pesan *spam* yang dikirim, dari cara *spammers* mengirim pesan, dan dari perlombaan antara *spammers* dan mereka yang mencoba untuk menghentikan atau mengendalikan *spam*. Selain itu, ada biaya kesempatan dari mereka yang melupakan penggunaan sistem *spam*. Ada biaya langsung, serta biaya tidak langsung yang ditanggung korban keduanya yang berkaitan dengan *spam* itu sendiri, dan untuk kejahatan lain yang biasa menyertainya, seperti pencurian keuangan, pencurian identitas, pencurian data, dan pencurian kemampuan intelektual, virus dan infeksi perangkat lunak, pornografi anak, penipuan, dan pemasaran yang menjurus penipuan.

Misalnya saja dalam hal penipuan, baru-baru ini telah terjadi suatu modus baru dalam hal penipuan yaitu bermodus jual beli obat lewat internet dimana obat-obat yang di perjual belikan adalah obat-obat ilegal termasuk obat palsu. Tahun lalu Satuan Tugas Pemberantasan Obat dan Makanan Ilegal melalui Operasi Pangea IV telah mengidentifikasi 30 situs yang mempromosikan obat ilegal dimana operasi ini adalah aksi internasional penertiban obat ilegal, termasuk obat palsu yang dipromosikan melalui internet tidak hanya dalam situs-situs tertentu tetapi juga jejaring sosial maupun layanan pesan singkat misalnya email, dan aksi ini dikoordinasikan *International Criminal Police Organization*, dalam operasi

tersebut disita 43 jenis obat ilegal dan semuanya merupakan produk impor terutama dari China.³

Di Indonesia mengenai kejahatan-kejahatan di dunia maya diatur di dalam Undang-Undang Republik Indonesia nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, lebih spesifik di dalam pasal 28 ayat 1 disebutkan bahwa “*Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik*”.

Dalam pasal 28 ayat 1 ini dapat dikatakan masih belum sempurna atau masih kabur untuk digunakan sebagai dasar acuan untuk tindakan *spamming*, hal ini dikarenakan *spamming* sendiri memiliki berbagai bentuk untuk melakukan kejahatan atau luasnya kualifikasi pengertian dari *spamming* itu sendiri, dari pasal 28 ayat 1 dapat dikatakan hanya untuk tindakan penyebaran berita bohong dan menyesatkan, tetapi apabila pasal ini digunakan dalam tindakan *spamming* pasal tersebut masih terlalu kabur dan dirasa masih belum mencukupi untuk menjerat pelaku *spamming*. Hal ini juga dikarenakan belum tercantumnya definisi *spamming* dalam Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, dalam undang-undang tersebut hanya mencantumkan unsur-unsur dan kualifikasi dari cyber crime hanya secara umum semata sehingga tidak membedakan apakah kualifikasi dari cyber crime tersebut termasuk kategori dari *cracking, hacking, carding, phishing, spamming* ataupun yang lain.

³ Kompas, 1 Februari 2012, Hati-hati Membeli Obat Lewat Internet, hal.13.

Sehingga dikarenakan hal tersebut di atas sangat penting untuk melakukan kriminalisasi terhadap tindakan *spamming* ini dimana kebijakan kriminalisasi menurut Barda Nawawi Arief adalah suatu kebijakan dalam menetapkan suatu perbuatan yang semula bukan tindak pidana (tidak dipidana) menjadi suatu tindak pidana (perbuatan yang dapat dipidana). Jadi pada hakekatnya, kebijakan kriminalisasi terhadap tindak pidana teknologi informasi merupakan bagian dari kebijakan kriminal (*criminal policy*) dengan menggunakan sarana hukum pidana (*penal*), dan oleh karena itu termasuk bagian dari “kebijakan hukum pidana” (*penal policy*), khususnya kebijakan formulasinya. Kebijakan kriminalisasi tersebut bukan sekedar kebijakan menetapkan, merumuskan atau memformulasikan perbuatan apa yang dapat dipidana (termasuk sanksi pidananya), melainkan juga mencakup masalah bagaimana kebijakan formulasi atau legislasi itu disusun dalam satu kesatuan sistem hukum pidana (kebijakan legislatif) yang harmonis dan terpadu.⁴

Apabila dibandingkan Negara lain, dapat dikatakan tindakan *cybercrime* khususnya tindakan *spamming* telah menjadi suatu permasalahan yang sangat serius yang dapat merugikan individu, kelompok tertentu misalnya perusahaan maupun Negara itu sendiri, sehingga diatur secara khusus mengenai *cybercrime* tersebut misalnya di Amerika telah dikeluarkan peraturan khusus mengenai *cybercrime* yaitu *Uniform Electronic Transaction Act (UETA)*. yang diadopsi oleh *National Conference of Commissioners on Uniform State Laws (NCCUSL)* pada tahun 1999, Eropa dengan *European E-Commerce Directive*, sejauh ini mengenai

⁴ Barda Nawawi Arief, *Kapita Selekta Hukum Pidana*, PT.Citra Aditya Bakti, Bandung, 2003, hal.259.

spamming telah ditetapkan di level negara bagian. Misalnya, di California pesan iklan tertentu harus mengawali subjek mereka dengan *ADV:* atau *ADV:ADLT*. Karena pesan seperti ini mudah difilter/dibedakan secara manual, maka harapannya motivasi melakukan *spamming* akan berkurang. Atau di Nevada negara bagian yang paling awal sadar akan spam, kita dilarang mengirim email komersial sama sekali, kecuali jika email tersebut menyertakan nama asli dan alamat fisik pengirim, ditandai agar langsung dapat dikenali sebagai iklan, negara Jerman dengan *Information and Communication Service Act*, Australia dengan *Digital Copyright Act 2000* dimana mengenai *spam* telah dibuat undang-undang anti spam, Hongkong dengan *Anti-Spam Code of Practices*, Negara Singapore dengan *The Electronic Transactions Act (ETA) 1998*, negara Singapore ini merupakan satu-satunya negara di ASEAN yang memberlakukan hukum secara tegas terhadap *spammers* dengan *Spam Control Act 2007*.⁵

Misalnya pada 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.⁶

⁵ Sumber dwiedogawa, *Peraturan dan Regulasi (perbedaan cyberlaw diberbagai negara)*, <http://blogkublogku.blogspot.com/2011/03/peraturan-dan-regulasi-perbedaan.html>, di akses pada tanggal 25 November 2011

⁶ 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*, Semarang, Fakultas Hukum Universitas Diponegoro, 2008, hal.208.

- (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.

Pada bulan Nopember 2000 pemerintah Australia mengkriminalisasikan perbuatan *spammer* kedalam *section 76 E Crimes Code 1995* yang berisikan:⁷

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.

Atas uraian latar belakang diatas maka sangat menarik untuk dapat menguraikan problematika aspek hukum pengaturan mengenai *spamming* dan pentingnya pengaturan mengenai *spamming* dalam hukum pidana di Indonesia dengan melihat sisi normatif di Indonesia dan aspek hukum secara luas karena tidak terbatasnya ruang lingkup dari dunia maya yang mempengaruhi terjadinya kejahatan dalam dunia maya, karena pengaturan mengenai *spamming* ini sangat berguna terutama berkaitan dengan keamanan dalam "cyber space", untuk itu dibutuhkan suatu kebijakan baik yang bersifat peraturan pemerintah maupun kebijakan khusus lainnya yang mengatur dalam perbuatan *spammer* sebagai upaya

⁷ 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.

memberikan kenyamanan penggunaan internet dan menghindari perbuatan-perbuatan yang mengarah ke penipuan.

Sehingga penelitian ini diharapkan dapat memberikan informasi yang berarti bagi perkembangan ilmu pengetahuan dan hukum di bidang *cyber crime* di Indonesia. Karena hal tersebut diatas maka penulis tertarik untuk mengangkat masalah **URGENSI KRIMINALISASI TERHADAP TINDAKAN "SPAMMING" DALAM HUKUM PIDANA DI INDONESIA.**

B. Rumusan Masalah

Berdasarkan uraian latar belakang diatas, maka dapat ditarik rumusan masalah sebagai berikut :

1. Bagaimanakah Urgensi Krimininalisasi terhadap tindakan *spamming* dalam hukum pidana di Indonesia?
2. Bagaimanakah pengaturan hukum tentang *spamming* dalam sistem hukum pidana di Indonesia?

C. Tujuan Penelitian

Berkaitan dengan permasalahan di atas, maka tujuan dari penulisan skripsi ini adalah:

1. Mengetahui dan menganalisis bagaimanakah Urgensi Krimininalisasi terhadap tindakan *spamming* dalam hukum pidana di Indonesia.
2. Mengetahui dan menganalisis bagaimanakah pengaturan hukum tentang *spamming* dalam sistem hukum pidana di Indonesia

D. Manfaat Penelitian

Penulisan skripsi ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Secara Teoritis
 - a. Dengan adanya penelitian ini diharapkan terdapat perkembangan dalam Ilmu Hukum khususnya dalam bidang Informasi dan Transaksi Elektronik (ITE) dan *cyber crime* di Indonesia, selain itu pula diharapkan terdapat penambahan, penyempurnaan ataupun penjelasan aturan mengenai *spamming* di dalam Undang-Undang Republik Indonesia nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.
 - b. Sebagai bahan kajian bagi kalangan akademis untuk terus mengkaji aspek-aspek hukum yang berkaitan dengan *cyber crime*, sehingga lebih menjamin terhadap kepastian hukum di bidang ITE.

2. Secara Praktis

a. Bagi Penulis

Untuk menambah wawasan mengenai jenis-jenis perbuatan yang dikategorikan sebagai tindak pidana komputer khususnya menambah pengetahuan mengenai tindakan *spamming*.

b. Bagi Pemilik Domain (Website) dan Penyedia Jasa Internet (*Internet Service Provider*)

Sebagai bahan masukan dan kontribusi pemikiran bagi para pemilik website maupun penyedia jasa internet atau ISP (*Internet Service Provider*) agar lebih memperhatikan isi website miliknya atau yang dibawahinya.

c. Bagi Aparat Penegak Hukum

Sebagai bahan informasi atau referensi berkaitan dengan segala tindakan pidana *cyber crime* yang di kategorikan sebagai *spamming*.

d. Bagi Masyarakat

Memberi informasi bahwa *spamming* merupakan salah satu tindakan *cyber crime*, sehingga masyarakat menjadi lebih berhati-hati ketika melakukan Transaksi Elektronik karena selama ini masih banyak masyarakat cenderung tidak peduli selama dirinya sendiri tidak di rugikan.

E. Sistematika Penulisan

Adapun sistematika penulisan yang disusun oleh penulis dalam skripsi antara lain:

BAB I PENDAHULUAN

Dalam Bab ini penulis menjelaskan tentang latar belakang pengangkatan permasalahan mengenai pengaturan tentang tindakan *spamming*, serta alasan penulis mengambil judul penelitian ini yang kemudian dilanjutkan dengan penulisan rumusan permasalahan yang akan dibahas hingga tujuan penelitian, manfaat penelitian serta sistematika penulisan.

BAB II KAJIAN PUSTAKA

Dalam bab ini penulis menguraikan tentang tinjauan pustaka yang akan digunakan untuk menganalisis dan menyelesaikan permasalahan dalam penelitian ini. Dalam tinjauan pustaka ini diuraikan tentang tinjauan umum mengenai kebijakan kriminalisasi, tinjauan umum tentang tindak pidana, tinjauan umum mengenai komputer, tinjauan umum mengenai internet, tinjauan umum mengenai *cyber crime*, serta tinjauan umum mengenai *spamming*.

BAB III METODE PENELITIAN

Pada bab ini penulis membahas mengenai jenis metode pendekatan yang digunakan peneliti dalam melakukan penelitian, jenis dan sumber data di dapat dan digunakan peneliti dalam melakukan

penelitian, metode penelusuran bahan hukum, teknik analisa bahan hukum dan definisi konseptual.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini berisi tentang hasil pembahasan mengenai permasalahan yang dikaji dalam penelitian ini.

BAB V PENUTUP

Bab ini merupakan bab yang berisi tentang kesimpulan dan saran yang dapat penulis berikan kepada pihak-pihak yang terkait dengan permasalahan dalam skripsi ini.

