Jurnal Cakrawala Hukum, Vol.7, No.2 Desember 2016, hlm. 169–182
E-mail:jurnalcakrawalahukum@unmer.ac.id
Website: http://jurnal.unmer.ac.id/index.php/jch

ISSN (Cetak): 2356-4962
ISSN (Online): 2598-6538

PENGIRIMAN E-MAIL *SPAM* SEBAGAI KEJAHATAN *CYBER* DI INDONESIA

Eka Nugraha Putra
Fakultas Hukum Universitas Merdeka Malang
Jl. Terusan Raya Dieng 62-64 Malang
eka.nugraha@unmer.ac.id

ABSTRACT

The Internet is part of the development of technology, where the internet provides many impacts, both positive and negative. Currently, privacy issues on the internet have also become a complicated legal issue, this is due to quite a number of privacy-related issues, but not all countries in the world manage privacy issues on the internet. As a means of communicating the Internet has introduced e-mail that provides convenience and practicality. But in its development e-mail has an adverse impact on its users in the form of e-mail spam. In terms of its actions, sending spam e-mail is quite a disadvantage, even violate the privacy. Some countries have also set it to one type of cybercrime (cybercrime). This research will discuss e-mail spam in Indonesia, how the legislation in Indonesia see the action of this spam e-mail, is there any possibility of spam e-mail is criminalized as a cybercrime. The research will also look at how spam e-mails violate privacy and review and analyze internet privacy settings in Indonesia in relation to the criminalization of spam e-mail.

***Keywords**: Spam E-mail, CyberMedia, Crime.*

ABSTRAK

Internet merupakan bagian dari perkembangan teknologi, dimana internet memberikan banyak dampak, baik positif maupun negatif. Saat ini masalah privasi di internet juga telah menjadi sebuah permasalahan hukum yang pelik, hal ini dikarenakan cukup banyak permasalahan terkait privasi, namun tidak semua negara di dunia mengatur masalah privasi di internet.Sebagai sarana berkomunikasi internet telah mengenalkan e-mail yang memberikan kemudahan dan kepraktisannya. Namun pada perkembangannya e-mail ini memiliki dampak merugikan bagi para penggunanya dalam bentuk e-mail spam. Segi perbuatannya, pengiriman e-mail spam ini cukup banyak merugikan, bahkan melanggar privasi. Beberapa negara juga telah mengaturnya sebagai salah satu jenis kejahatan cyber (cybercrime). Penelitian ini akan membahas tentang e-mail spam di Indonesia, bagaimana peraturan perundang-undangan di Indonesia melihat perbuatan e-mail spam ini, apakah ada kemungkinan e-mail spam dikriminalisasi sebagai sebuah kejahatan cyber. Penelitian ini juga akan melihat bagaimana e-mail spam melanggar privasi dan mengkaji serta menganalisis pengaturan privasi internet di Indonesia dalam kaitannya dengan kriminalisasi e-mail spam tersebut.

***Kata Kunci**: E-mail Spam, Media Cyber, Tindak Kejahatan.*

Internet telah membawa dampak perubahan yang sangat besar bagi masyarakat. Dimana segala kegiatan manusia telah berganti menjadi aktivitas digital di dunia internet. Sebagai bagian dari konvergensi telematika, dimana terdapat tiga unsur yaitu telekomunikasi, media dan informatika, internet telah menjadi bagian tak terpisahkan dalam kehidupan manusia.

Pemanfaatan e-mail sebagai kemudahan yang diberikan internet ini pun berpeluang terjadinya penyalahgunaan dimana dalam penggunaan e-mail dikenal pula e-mail *spam*. E-mail *spam*, merujuk pada definisi kata *spam* adalah email yang berisi konten "*junk*" (sampah) atau tidak relevan dengan keperluan penggunanya (Anonim, 2015, www.techterms.com). Pengiriman e-mail *spam* dalam jumlah banyak, tentu menimbulkan ketidak nyamanan atau bahkan kerugian karena tak jarang konten dari e-mail *spam* tersebut berisi link-link yang mengarahkan penerima email untuk mengklik link-link tertentu yang berisi konten berbahaya.

Di Indonesia, e-mail *spam* juga menjadi masalah dalam penggunaan internet yang telah ada cukup lama. Bahkan pada tahun 2012, berdasarkan rilis data dari Kaspersky Lab, Indonesia termasuk pada peringkat ketujuh sebagai negara pengirim *spam* terbanyak dengan jumlah 3,1 persen (Riyandi Andesma, 2013, www.techno.okezone.com).

Internet merupakan dunia yang berbeda dengan dunia fisik yang kita kenal sehari-hari, hampir semua hal yang berhubungan dengan pelanggaran atau bahkan kejahatan tidak mampu disentuh oleh hukum positif yang berlaku di dunia fisik kita sehari-hari. Itulah mengapa dunia internet dan segala aktivitas yang terlibat di dalamnya dinamakan dengan *cyberspace* dan aturan hukum yang mengaturnya disebut *cyberlaw*.

Di Indonesia regulasi terkait *cyberspace* sendiri telah diatur dalam Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE). Dimana Undang-undang tersebut mengatur aspek-aspek hukum terkait internet baik perdata maupun pidana. UU ITE juga telah mengatur mengenai tindak pidana di internet dari Pasal 27 sampai Pasal 37, namun pengaturan mengenai penyebaran e-mail *spam* memang belum diatur secara spesifik. Beberapa tindak pidana dalam UU ITE antara lain baru mengatur mengenai pencemaran nama baik (Pasal 27 Ayat 3), penipuan konsumen (Pasal 28 Ayat 1), *hacking* (Pasal 30 Ayat 1) dan intersepsi (Pasal 32 Ayat 1).

Berbicara tentang perbuatan *spamming*, atau lebih spesifiknya pengiriman e-mail *spam* sebenarnya berkaitan dengan pelanggaran privasi dari pengguna internet. Meskipun secara etika di internet (netiket) e-mail *spam* termasuk perbuatan yang tidak beretika, namun tentu saja netiket belum mampu secara tegas mengurangi penyebaran e-mail *spam* tersebut. Di beberapa negara, *spamming* telah menjadi salah satu bagian dari *cyber crime*, bahkan di negara Australia telah diatur regulasi khusus mengenai *spamming* dalam *Spam* Act 2003. Hal ini terjadi karena privasi merupakan hal yang perlu dilindungi juga oleh *cyberlaw*. Privasi dalam hal ini berkaitan dengan pemahaman bahwa setiap pribadi di internet juga memiliki hak untuk tidak diganggu.

Apabila kembali kepada UU ITE pengaturan privasi sendiri di Pasal 26 kurang komprehensif mengingat masih terkait dengan pengaturan di Undang-undang lain, Pasal 26 UU ITE sendiri berbunyi: "*Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan. (2) Setiap orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-undang ini.*" Melihat uraian bunyi pasal di atas sebenarnya masih kurang tegas mengatur mengenai privasi di internet. Hal ini dapat menjadi kelemahan dari penegakan *cyberlaw* di Indonesia melalui UU ITE. E-mail *spam* kemudian tidak hanya berbicara masalah pelanggaran privasi di internet, namun bagaimana kemudian e-mail *spam* dapat menuntun atau menyesatkan pengguna internet kepada konten-konten di internet yang berbahaya, pada konteks inilah semestinya *cyberlaw* di Indonesia mampu mengaturnya secara tegas.

Penelitian ini akan memfokuskan pada kriminalisasi e-mail *spam* dalam *cyberlaw* Indonesia, dimana perbuatan e-mail *spam* akan dikaji apakah di Indonesia dapat dikategorikan sebagai bagian dari *cybercrime*, melihat bentuk-bentuk *spam* untuk kemudian menentukan apakah e-mail *spam* perlu untuk dikriminalisasi. Pembahasan ini juga akan dikorelasikan dengan pelanggaran privasi di internet, mengkajinya dalam UU ITE sejauh mana privasi di internet dilindungi oleh Undang-undang tersebut sehingga dapat ditemukan apakah e-mail *spam* perlu diatur sebagai *cybercrime* dari bentuk pelanggaran privasi. Berdasarkan uraian latar belakang di atas, maka Penulis mengangkat penelitian mengenai *spam* dan *cybercrime* dalam judul penelitian "*Pengiriman E-mail Spam sebagai Kejahatan Cyber di Indonesia*".

Meskipun di beberapa negara e-mail *spam* telah diklasifikasikan dalam kejahatan *cyber*, Namun di Indonesia belum diatur dalam Peraturan Perundang-Undangan terkait, untuk itu berdasarkan latar belakang di atas maka fokus penelitian ini adalah mengenai *spam* dan kejahatan *cyber*, sehingga menimbulkan beberapa permasalahan yaitu berkaitan dengan apakah e-mail *spam* dapat didefinisikan sebagai kejahatan *cyber*, dan bagaimana UU ITE mengatur mengenai privasi yang digangu oleh e-mail *spam*, serta bagaimana sebaiknya pengaturan e-mail *spam* dalam kaitannya dengan perlindungan privasi pada hukum pidana *cyber* Indonesia.

Metode Penelitian

Pendekatan yang digunakan adalah metode pendekatan normatif, dengan alasan penelitian ini hendak menganalisa doktrin hukum dan isu hukum dari perbuatan e-mail *spam* untuk kemudian memberikan perspektif dalam sistem norma, apakah dapat diatur ke dalam norma hukum tersebut khususnya hukum pidana *cyber*. Penelitian ini juga menggunakan pendekatan *Statute Approach* (Pendekatan Perundang-undangan) untuk melihat pengaturan terkait e-mail *spam* sebagai bagian dari kejahatan *cyber* serta *Comparative Approach* (Pendekatan Perbandingan) untuk melihat pengaturan e-mail *spam* di beberapa negara yang memiliki regulasi terkait.

Data primer merupakan data yang didapatkan Peraturan Perundang-undangan terkait ruang *cyber* (*cyberspace*) asas-asas dan pengaturan mengenai privasi di internet dan pengaturan mengenai e-mail *spam*. Sedangkan untuk data sekunder merupakan buku literatur terkait dan jurnal-jurnal hukum yang membahas mengenai kejahatan *cyber* dan pengaturan yang terkait. Data sekunder juga digunakan untuk mencari referensi terkait pengaturan *spam* di beberapa negara untuk mengetahui kenapa di negara tersebut e-mail *spam* dianggap sebagai sebuah aktivitas kejahatan serta kaitannya dengan pengaturan privasinya.

Teknik pengumpulan data dalam penelitian ini mempergunakan beberapa cara yaitu inventarisasi data-data yang menjadi sumber referensi penelitian ini. Kemudian melakukan klasifikasi terhadap seluruh data tersebut dan membaginya menjadi data primer dan data sekunder dan melakukan sistematisasi data primer dan data sekunder agar sesuai dengan kebutuhan penelitian ini.

Teknik analisa data dilakukan dalam penelitian ini menggunakan teknik analisa deskriptif kualitatif dan kuantitatif, yaitu peneliti mendiskripsikan data primer berupa Peraturan Perundang-undangan serta mencari fakta yang mendukung gambaran pada data primer yang bertujuan untuk memberikan gambaran dan menjabarkan permasalahan yang ada kemudian dianalisa lebih lanjut dengan teori-teori dan penjelasan-penjelasan yang berkaitan dengan permasalahan yang ada berdasarkan data sekunder, hasil dari analisa inilah yang kemudian dipakai untuk merumuskan suatu kesimpulan.

E-mail *Spam* sebagai Kejahatan *Cyber*

Spam bisa terjadi dalam beragam bentuk, informasi menganggu yang berbentuk iklan secara halus, informasi yang menjadi titik masuk bagi kejahatan *cyber* seperti pemalsuan data, penipuan atau pencurian data (Mamoun Alazab dan Roderic Broadhurst, 2015, 2). Aktivitas *spam* pada dasarnya relatif mudah apabila melihat definisinya yang merupakan tindakan yang dilakukan bertubi-tubi atau berulang-ulang. Artinya pengirim informasi yang dikatakan melakukan *spam (spammer)* bisa berada pada dua ciri yang memang dengan sengaja mengirimkan *spam* untuk berbuat kejahatan atau pengirim *spam* yang tidak mengetahui bahwa dirinya telah melakukan *spam*.

E-mail *spam*, selain berisi informasi tidak penting atau tidak relevan, tak jarang pula e-mail *spam* menggiring penerima untuk mengklik link-link tertentu atau URL (*Unique Related Location*) dimana ketika di klik URL ini akan mengarah kepada website tertentu atau URL tersebut mengandung malware atau virus yang dapat merusak sistem komputer penerima e-mail atau mencuri data penerima e-mail. Sisipan malware atau virus ini biasanya berbentuk pesan atau informasi dalam e-mail *spam* tersebut yang bersifat sosial atau kode-kode rumit.

Privasi memang merupakan sebuah konsep yang sampai hari ini sulit ditentukan batas-batasnya, mengingat konsep privasi akan banyak dipengaruhi oleh berbagai faktor seperti sosial, ekonomi dan budaya dari masing-masing wilayah. Namun secara prinsip privasi merupakan hak dasar manusia yang sangat penting karena menyangkut otonomi atau cara manusia mengatur dan mengekspresikan apa yang ada dalam dirinya.

Sebelum perkembangan teknologi yang demikian cepat dan pesat khususnya internet saat ini, ruang lingkup privasi terbatas pada gangguan yang secara subjektif dialami oleh masing-masing privasi, contohnya adanya penerobosan rumah orang tanpa ijin atau gangguan terhadap kehidupan pribadi seseorang. Saat ini dengan keberadaan internet, ruang lingkup privasi menjadi lebih luas. Internet dengan sifat *ubiquotus* dan *borderless* membuat ruang lingkup privasi tidak hanya masalah gangguan kehidupan pribadi seseorang namun juga melibatkan beberapa aspek lain, sebagaimana disampaikan oleh Lawrence Lessig yang dikutip oleh Sinta Dewi Rosadi (2015, 2) yaitu; a) Privasi sebagai suatu konsep bahwa individu tidak mau diganggu oleh orang lain, b) Konsep bahwa privasi berkaitan dengan kehormatan seseorang, c) Konsep bahwa wewenang pemerintah harus dibatasi sehingga tindakannya tidak akan menganggu privasi warga negaranya.

Konsep privasi yang disampaikan Lawrence Lessig ini kemudian berhubungan dengan kebebasan atas ekspresi pribadi dan terhindar dari penyalahgunaan data pribadi di internet, yang sampai saat ini masih menjadi permasalahan dalam rangka aturan hukum terkait privasi di internet. Salah satu contoh kasus terkait dengan privasi di internet adalah pembobolan foto pribadi beberapa artis Hollywood di ICloud yang menyebabkan foto-foto pribadi para artis tersebut tersebar di Internett, diketahui bahwa pelaku pembobolan akun Icloud tersebut membobol 572 akun termasuk akun para artis tersebut (Jeremy, Diamond, 2016, www.cnn.com).

Terdapat pandangan tradisional bahwa masalah privasi terlepas dari struktur hukum, sehingga privasi secara alamiah terancam oleh cepatnya perkembangan teknologi, di sinilah kemudian seharusnya hukum mengintervensi pengaturan privasi (Daniel J. Solove, 2003,14). Sebagaimana salah satu contoh kasus di atas, hukum dituntut untuk lebih dinamis terhadap perkembangan teknologi agar hukum mampu menjerat pelaku kejahatan berteknologi, karena teknologi tidak mungkin dipandang hanya sebagai alat atau instrumen semata. Sebagaimana diuraikan oleh Arthur Cockfield dan Jason Pridmore (2007,483) bahwa dalam rangka menjelaskan sintesis antara hukum

dengan teknologi terdapat teori subsantif yang menyatakan bahwa perkembangan teknologi juga memuat nilai-nilai sosial, ekonomi, politik yang kemudian akan melahirkan kekuatan dan otoritas pada siapa yang menguasai perkembangan teknologi tersebut.

Saat ini masalah privasi di internet juga telah menjadi sebuah permasalahan hukum yang pelik, hal ini dikarenakan cukup banyak permasalahan terkait privasi, namun tidak semua negara di dunia mengatur masalah privasi di internet. Tercatat bahwa Swedia merupakan negara pertama yang mengatur perlindungan privasi dan data pribadi sejak tahun 1973 melalui Sweden Data Act 1973, dimana hingga hari ini terdapat 76 negara yang secara spesifik mengatur privasi dan perlindungan data pribadi dalam sebuah peraturan perundang-undangan di negara mereka (Graham Greenleaf, 2012, 2).

Di Uni Eropa sejak 1995 telah disusun mengenai pedoman untuk privasi dan perlindungan data pribadi yang dapat diadopsi oleh negara-negara Uni Eropa dalam "*Directive 95/46/EC/ of the Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data*." Directive tersebut disusun bertujuan untuk melindungi hak-hak dasar dan kebebasan dari setiap orang khususnya hak-hak privasi dalam kaitanya dengan proses data pribadi.

Di Indonesia sendiri belum terdapat peraturan perundang-undangan yang secara khusus mengatur masalah perlindungan data pribadi dan privasi, khususnya di internet. Beberapa peraturan perundang-undangan terkait hal tersebut masih diatur secara sporadis. Pasal 1 Angka 3 dan Angka 4 Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan yang mengatur dan membedakan arsip dinamis dan arsip vital, Pasal 29 Undang-Undang Nomor 36 Tahun 1999 Tentang Hak Asasi Manusia yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat dan hak miliknya, Pasal 40 Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan dimana bank diwajibkan untuk merahasiakan keterangan tentang nasabah penyimpan dan simpanannya, kecuali untuk kepentingan perpajakan, penyelesaian piutang bank, kepentingan peradilan dan perkara pidana, Pasal 40 Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi yang menyatakan bahwa setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.

Berkaitan privasi dengan kejahatan *cyber* yang merupakan fenomena global dan baru pada ranah hukum, khususnya hukum pidana, pelanggaran privasi juga dapat dikatakan sebagai salah satu dari modus-modus baru pada kejahatan *cyber*. Awal perkembangannya, terminologi untuk kejahatan yang menggunakan sarana teknologi adalah "kejahatan computer". Hal ini wajar dikarenakan kejahatan yang berhubungan dengan teknologi informasi pada awalnya hanya berhubungan dengan komputer saja (*computer related crime*). Andi Hamzah dan Boedi D. Marsita (1987, 24) mengungkapkan bahwa munculnya kejahatan terkait komputer tidak bisa dilepaskan dari "*The man behind the machine*", bahwa terdapat kesalahan yang disengaja mengarah pada penyalahgunaan komputer yang dilakukan secara melawan hukum untuk keuntungan sendiri atau kelompoknya.

Pengiriman e-mail *spam* sesuai dengan definisi yang telah dijelaskan sebelumnya dapat mengakibatkan gangguan pada sistem atau data komputer. Karena e-mail *spam* biasanya berbentuk phising, phising sendiri pada *Convention On Cybercrime* 2001 tergolong ke dalam *Offences Against Confidentiality, Integrity and Availibility of Computer Data and System* dalam modus gangguan sistem atau gangguan data komputer. Secara umum terdapat dua tujuan pengiriman *spam* yaitu (Hendry Chohwanandi, 2012, 2-3); a) Pengiriman *spam* biasanya bertujuan sebagai media publikasi dan promosi untuk produk-produk perusahaan pengirim e-mail *spam*

misalnya sebuah perusahaan tertentu ingin menjual barang produksi mereka, jika melalui 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, b) *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 diperlukan dalam jumlah yang besar dan secara terus menerus. *Spamming* juga sering digunakan sebagai media penyebaran *virus* dan *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*.

Kedua tujuan pengiriman *spam* di atas terdapat ciri utama yaitu pengiriman pesan atau e-mail yang tidak diinginkan oleh penerimanya, hal ini dikarenakan pengiriman *spam* memang tidak memperhatikan privasi penerimanya, dalam konteks pelanggaran privasi menurut William Prosser sebagaimana dikutip oleh Shinta Dewi (2009, 19) bentuk pengiriman e-mail *spam* ini termasuk ke dalam mengganggu hak orang untuk menyendiri dimana ruang lingkup gangguan tidak hanya secara fisik tetapi mental seseorang baik perseorangan, swasta maupun negara.

Sehubungan dengan dua tujuan pengiriman e-mail *spam* di atas, pengirim e-mail *spam* yang bertujuan untuk kepentingan promosi bisnis memang berpegang pada prinsip membangun pasar sendiri (*If we built it, they will come*), sehingga banyak pengiriman e-mail *spam* yang menggunakan bot untuk mempermudah proses *spam*ming tersebut.

Beberapa peraturan perundang-undangan di negara di dunia yang sudah mengatur e-mail *spam* sebagai sebuah kejahatan antara lain di Kanada yang mengaturnya dalam beberapa peraturan perundang-undangan yaitu *Personal Information Protection and Electronic Documents Act (PIPEDA), Competition Act, Charter of Rights Freedoms, The Criminal Code and the Competition Act, Canadian Code of Practice for,* dan *Consumer Protection in Ecommerce*. Sementara di Australia diatur dalam *Spam Act of 2003, Telecommunications Act of 1997 dan Australia Parts IVA, V, and VC of the Trade Practices Act of 1974*.

Pasal 4 dan Pasal 5 Convention On *Cybercrime* Tahun 2001 *spam* merujuk kepada *data interference* dan *system interference* dimana bersifat standar minimum dari rumusan perbuatan yang diatur di dalam Convention tersebut, sehingga setiap negara anggota dapat mengadopsi rumusan perbuatan tersebut untuk diatur sesuai dengan hukum domestik yang berlaku di negara mereka.

Menetapkan sebuah perbuatan merupakan kejahatan ciber, terdapat beberapa hal yang harus diperhatikan terkait kriminalisasi kejahatan *cyber*, yaitu (Widodo, 2013, 60-61); a) Kriminalisasi dan merupakan upaya yang mendukung tujuan akhir kebijakan kriminal, melindungi dan menyejahterakan masyarakat, b) Perbuatan yang akan dikriminalisasi tersebut benar-benar dicela oleh masyarakat, c) Perlu diperhitungkan tentang keuntungan dan kerugian kriminalisasi, d) Perlu diupayakan agar tidak terjadi over-kriminalisasi yang dapat berpengaruh secara sekunder terhadap kepentingan masyarakat, e) Perlu disesuaikan antara kemampuan penegak hukum dengan penegakan hukum.

Mengkriminalisasikan pengiriman e-mail *spam* sebagai kejahatan *cyber* dan menyesuaikan apa yang diatur di dalam *Convention Cybercrime* 2001 maka penulis akan merujuk pada tindak pidana *data interference* dan *system inteference* yang diatur di dalam hukum nasional, yaitu UU ITE.

Pengaturan Pelanggaran Privasi melalui E-Mail *Spam* dalam Undang – Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Apabila merujuk pada pembahasan sub bab sebelumnya, maka pengiriman e-mail *spam* tidak diatur secara tegas, bahkan rumusan terkait privasi hanya diatur pada Pasal 26 yang berbunyi sebagai berikut; (*1) Kecuali ditentukan lain oleh Peraturan Perundang-undangan,penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.*

Rumusan pasal di atas pun hanya berbicara pada aspek perdata saja, terkait dengan kerugian dan gugatan dari pihak yang merasa dirugikan atas pelanggaran privasi yang terjadi. Sementara berkaitan dengan penelitian ini aspek pidana terkait pelanggaran privasi dapat dilihat pada Pasal 32 (*Data Interference*) dan Pasal 33 (*System Interference*). Penulis akan membahas unsur-unsur dalam Pasal-Pasal UU ITE ini satu-persatu diantaranya Pasal 32 Ayat 1 berbunyi sebagai berikut; "*Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik".*

Sebagaimana rumusan pada Pasal 27 sampai dengan Pasal 37 UU ITE tentang tindak pidana dalam UU ITE unsur kesalahan ada pada frasa "*dengan sengaja*" dan unsur melawan hukum ada pada frasa "*tanpa hak atau melawan hukum*". Hal ini menunjukkan bahwa tindak pidana dalam UU ITE adalah tindak pidana yang memiliki unsur utama kesengajaan (*dolus*) bukan kelalaian (*culpa*). Hal ini menunjukkan bahwa kejahatan *cyber* yang diatur dalam UU ITE merupakan tindak pidana yang mengutamakan unsur kesengajaan. Dikatakan perbuatan tersebut melawan hukum karena terkait dengan objek pada rumsan Pasal ini yaitu "*Informasi Elektronik dan/atau Dokumen Elektronik milik orang lain atau milik publik*". Hal ini berarti perbuatan yang dirumuskan dalam Pasal ini ditujukan pada Informasi Elektronik dan/atau Dokumen Elektronik yang dilakukan tanpa ijin.

Unsur perbuatan dalam Pasal 32 Ayat 1 (*Data Interference*) adalah "*mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan dengan cara apapun*." Namun dari rumusan 8 perbuatan ini tidak diterangkan cara melakukan perbuatan secara limitatif, sehingga terpenuhinya rumusan perbuatan ini sangat fleksibel karena telah menimbulkan akibat dari perbuatan.

Mengubah, menambah dan mengurangi di sini berarti perbuatan tersebut berakibat isi dari Informasi/Dokumen Elektronik isinya berubah atau lain isinya dengan tujuan sesuai maksud dari pemilik atau pembuat Informasi/Dokumen Elektronik tersebut. bertambahnya dan berkurangnya isi Informasi/Dokumen Elektronik tersebut juga diketahui oleh si pembuat sebagai syarat terpenuhinya tindak pidana tersebut (Adami Chazawi dan Ardi Ferdian, 2011, 164-165).

Merusak, menghilangkan dan menyembunyikan memiliki akibat yang hampir sama dimana isi dari Informasi/Dokumen Elektronik kemudian tidak dapat digunakan lagi karena kerusakan atau lenyapnya isi dari Informasi/Dokumen Elektronik tersebut. Melakukan transmisi dan memindahkan sama-sama berakibat beralihnya Informasi/Dokumen Elektronik ke pihak lain. Namun transmisi bersifat langsung kepada pihak yang dituju sementara memindahkan beralih ke sistem atau media penyimpanan lainnya.

Tindak pidana pada Pasal 32 UU ITE ini selain dikenal sebagai *data interference* juga dikenal

dengan *defacing*, dimana *defacing* biasanya menyerang sebuah website dengan cara mengubah atau merusak sebuah website, secara umum tujuan *defacing* adalah semata-mata untuk popularitas dan untuk unjuk kemampuan di antara sesama hacker (Budi Suhariyanto, 2012, 140).

Apabila dibandingkan dengan pengiriman e-mail *spam* maka dari segi tujuan terdapat perbedaan dari segi tujuan, dimana pengiriman e-mail *spam* biasanya bertujuan untuk promosi, meskipun juga ada yang bertujuan untuk mencuri data. 8 rumusan perbuatan yang dibahas di atas dalam konteks pengiriman e-mail *spam* bisa diakomodir oleh seluruh perbuatan tersebut meskipun unsur utama adalah berkaitan dengan hal melakukan transmisi yang bersifat pengiriman. Apabila dibandingkan dengan bentuk pengiriman e-mail *spam* pun semestinya rumusan Pasal 32 UU ITE merumuskan perbuatan terlebih dahulu dan merumuskan frasa "*yang mengakibatkan hilangnya data, rusaknya data*" sebagai unsur akibat konstitutif dari tindak pidana pengiriman e-mail *spam*. Namun mengingat dalam rumusan pasal ini tidak diatur secara limitatif, maka menurut penulis pasal 32 UU ITE tidak mengakomodir pengiriman e-mail *spam* sebagai sebuah tindak pidana.

Pasal lain dalam UU ITE yang juga dianggap berhubungan dengan tindak pidana *spam*ming adalah Pasal 33 UU ITE (*System Interference*) yang berbunyi sebagai berikut; "*Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.*"

Sebagaimana pembahasan Pasal 32 di atas, unsur kesalahan pada Pasal tersebut ada pada frasa "*dengan sengaja*" dan unsur melawan hukumnya ada pada frasa "*tanpa hak*". Berbeda dengan unsur perbuatan pada Pasal 32 yang merumuskan 8 bentuk perbuatan sebagai syarat terpenuhinya tindak pidana tersebut. Pada rumusan Pasal 33 ini unsur perbuatan dirumuskan dengan "*melakukan tindakan apapun*" yang tidak merumuskan perbuatan tertentu mengenai gangguan sistem elektronik secara konkret. Hal ini berarti setiap bentuk perbuatan yang konkret akan masuk ke dalam pengertian "melakukan kegiatan apapun" pada Pasal ini, asalkan perbuatan tersebut ditujukan pada suatu sistem elektronik (Adami Chazawi dan Ardi Ferdian, 2011, 174).

Apabila rumusan Pasal 33 UU ITE dibandingkan dengan rumusan *system interference* dalam *Convention Cybercrime* 2001, dari segi rumusan tidak jauh berbeda, namun *Convention Cybercrime* 2001 mempertegas dalam penjelasannya bahwa definisi "gangguan terhadap sistem komputer" adalah campur tangan terhadap sistem komputer yang berupa semua tindakan yang dapat menyebabkan gangguan pada fungsi sistem komputer, gangguan tersebut dapat berupa memasukkan, memancarkan, merusak, menghapus, mengubah atau menghalangi sistem komputer. Perbuatan-perbuatan yang mengganggu sistem komputer dijelaskan di dalam penjelasan *Convention Cybercrime* 2001 namun tidak di dalam UU ITE. Secara spesifik gangguan atau campur tangan terhadap sistem komputer dapat berupa tindakan penyebaran virus (*worm*), serangan terhadap sistem atau jaringan komputer (*Denial of Service atau DoS*), *Distributed Denial of Service Attack* dan *spamming* (Widodo, 2012, 62).

Meninjau apakah benar Pasal 33 UU ITE sudah mengakomodir *spam* sebagai tindak pidana, maka perlu ditinjau pula 3 unsur utama dari *spam* yaitu *bulk, unsolicited* dan *commercial*. *Bulk* dalam konteks pengiriman e-mail *spam* tidak hanya ditentukan dari jumlah e-mail yang banyak namun juga pada konteks "ijin" sebagai kriteria penentu dari e-mail yang dikirimkan (Anonim, 2009, 4). Konteks Pasal-Pasal tindak pidana di UU ITE hampir seluruh modus kejahatan *cyber* rumusan tindak pidananya diawali oleh akses ilegal atau dengan kata lain selesainya tindak pidana dalam UU ITE karena diawali oleh akses ilegal terlebih dahulu. Namun berbeda dengan *spamming*, sebagaimana *worming* dan

phising modus kejahatan *cyber* ini tidak diawali oleh akses ilegal terlebih dahulu (Widodo, 2012, 55), hal ini karena unsur ijin di sini lebih kepada tidak diinginkan atau tidak relevannya e-mail *spam* yang dikirim.

Ketidak relevanan dari e-mail yang dikirimkan kepada penerima e-mail *spam* akan berhubungan dengan unsur kedua dari e-mail *spam* yaitu "*unsolicited*", dalam E-Privacy Directive diatur pelarang terhadap memasukkan alamat e-mail orang lain pada sebuah website layanan kontes, jual beli untuk kepentingan promosi. Pada dasarnya makna "*unsolicited*" di sini sangat subjektif (Tanpa Penulis, 2009, 5), karena hampir semua pengiriman informasi di internet antara pengguna belum tentu relevan di antara sesama pengguna, sebagai contoh update status sosial media atau forward e-mail yang mengandung konten humor. Hal ini berarti dalam menentukan apakah unsur "*unsolicited*" sudah terpenuhi atau tidak dalam kejahatan *cyber* pengiriman e-mail *spam*, maka akibatnya harus terjadi dulu. Sifatnya yang subyektif maka sebagaimana pencemaran nama baik atau pengancaman hanya korban yang bisa merasakan akibat dari unsur "*unsolicited*" tersebut.

Unsur yang ketiga yaitu "*commercial*" di sini tentu bermakna bahwa kepentingan komersial digunakan oleh pengirim e-mail *spam*, meskipun unsur komersial tidak selalu menjadi tujuan pengiriman e-mail *spam*, sebagai contoh e-mail *spam* yang berisi *spyware*, virus atau propaganda politik tentu tidak bisa dikategorikan komersial. Hal ini berarti ketiga unsur e-mail *spam* tersebut bersifat gabungan untuk merumuskan definisi e-mail *spam*.

Uraian di atas penulis dapat menyimpulkan bahwa Pasal 33 UU ITE juga belum mampu mengakomodir pengiriman e-mail *spam* hal ini dikarenakan ketiga unsur *spam* yaitu *bulk, unsolicited* dan *commercial* tidak diatur secara utuh. Urgensi kriminalisasi *spam*ming kemudian dibutuhkan mengingat ada masalah pelanggaran privasi dalam kaitannya dengan pengambilan data, serta pelanggaran hak konsumen terkait dengan promosi yang dilakukan oleh produsen.

Namun dalam UU ITE hanya ada 1 Pasal yang berhubungan dengan hak konsumen, yaitu Pasal 28 Ayat 1 yang berbunyi; "*Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik.*" Tindak pidana pada Pasal 28 Ayat 1 ini hanya berhubungan dengan penipuan konsumen, terlihat dari frasa "kerugian konsumen". Hal ini berarti Pasal 28 Ayat 1 hanya mengatur tentang konsumen yang sudah melakukan transaksi, sementara dalam pengiriman e-mail *spam*, modusnya masih pada tahapan pra-transaksi atau promosi. Berdasarkan pembahasan pada UU ITE di atas, maka di dalam UU ITE belum ada pengaturan terkait pengiriman e-mail *spam*, sehingga dibutuhkan pengaturan yang lebih spesifik dan ideal untuk mengakomodir pengiriman e-mail *spam* sebagai kejahatan *cyber*.

Pengaturan Ideal Terkait E-Mail *Spam* Sebagai Kejahatan *Cyber* untuk Perlindungan Privasi

Sebagaimana telah diuraikan di atas, kejahatan *cyber* telah memberikan bentuk baru pada kejahatan yang tidak dapat dijangkau oleh hukum pidana positif. Dalam kaitan dengan pengiriman e-mail *spam*, beberapa negara juga telah mengatur pengiriman e-mail *spam* sebagai bentuk kejahatan *cyber*.

Pembahasan substansi UU ITE sebelumnya, diketahui bahwa pengiriman e-mail *spam* tidak secara tegas diatur dalam UU ITE. Oleh karena itu, menjadi urgen sifatnya agar pengiriman e-mail *spam* diatur sebagai salah satu bentuk kejahatan atau dikriminalisasi.

Teguh Prasetyo (2010, 45) menjelaskan bahwa terdapat beberapa alasan yang dapat menjadi dasar suatu perbuatan untuk dikriminalisasi, yaitu; a) Adanya korban, b) Kriminalisasi bukan semata-

mata ditujukan untuk pembalasan, c) Harus berdasarkan asas *ratio principle*, d) Adanya kesepakatan sosial. Selanjutya dibahas alasan-alasan tersebut satu-persatu berdasarkan unsur-unsur dan modus dalam pengiriman e-mail *spam* diantranya:

a. Adanya korban

   Suatu tindak pidana, korban menjadi syarat utama dari adanya kejahatan. Hal ini dikarenakan kejahatan pasti akan menimbulkan kerugian dalam perbuatannya, kerugian inilah yang dialami oleh korban. Dalam pengiriman e-mail *spam*, terdapat kerugian yang dialami penerima e-mail *spam* sebagai korbannya yaitu privasi yang dilanggar, dimana e-mail *spam* tersebut tidak diinginkan oleh si penerima dan adanya *phising* yang kemudian mengambil data pribadi dari penerima e-mail *spam* tersebut. Di Indonesia tercatat bahwa pada pertengahan tahun 2015 jumlah e-mail *spam* adalah 23,5 juta meningkat dari jumlah 18,5 juta (Deliusno, 2016, www.kompas.com).

   Sementara berdasarkan hasil riset dari ID CERT sampai bulan Desember 2015 pengaduan mengenai *spam* tercatat pada jumlah 41,7 % atau terdapat 16.087 pengaduan (ID CERT, 2016, www.cert.or.id). Berdasarkan data yang diuraikan di atas, maka jelas bahwa pengiriman e-mail *spam* menimbulkan kerugian dan sebagai sebuah perbuatan yang akan dikriminalisasi pengiriman e-mail *spam* menimbulkan korban.

   Mengkriminalisasikan pengiriman e-mail *spam*, maka bentuk akibat konstitutif yang harus diperhatikan adalah bagaimana kemudian e-mail *spam* dijadikan sarana promosi yang melanggar privasi, khususnya yang terkait dengan *phising*.

b. Kriminalisasi Bukan Semata-mata Ditujukan Untuk Pembalasan

   Awal perkembangannya tujuan hukum pidana adalah untuk pembalasan atas kerugian yang dialami oleh korban. Namun pada konteks sekarang, khususnya yang berkaitan dengan kejahatan *cyber*, maka tujuan pembalasan atau retributif tentu harus ditinjau ulang. Hukum pidana dan pemidanaannya saat ini idealnya juga berpijak pada tujuan restoratif.

   Widodo menyatakan bahwa mengingat karakteristik kejahatan *cyber* yang yurisdiksinya memungkinkan lintas batas negara, maka dibutuhkan strategi kebijakan non-penal dalam rangka memerangi kejahatan *cyber* secara non-penal antara lain kerjasama internasional dan rencana aksi nasional dalam memerangi kejahatan *cyber* (Widodo, 2013, 147-148). Hal ini menunjukkan bahwa ada upaya untuk pencegahan tak hanya semata-mata pembalasan.

   Pengiriman e-mail *spam* juga dapat mengakomodir hal tersebut, mengingat gangguan yang muncul dalam bentuk kerugian dari privasi korban tidak ada ukuran pastinya dan bersifat sangat subjektif, maka bentuk kriminalisasinya tidak tepat apabila menggunakan tujuan pembalasan.

c. Harus berdasarkan asas *ratio principle*

   Prinsip rasio di sini adalah terkait dengan perlindungan kepentingan yang ditujukan atas pembuatan hukum pidana tersebut. Pada dasarnya setiap peraturan perundang-undangan yang terkait dengan hukum pidana bertujuan untuk melindungi kepentingan tiga pihak, yaitu kepentingan individu, kepentingan golongan dan kepentingan negara. Di sinilah kemudian kriminalisasi atas sebuah perbuatan akan menunjukkan kepentingan mana yang dilindungi dengan memperhatikan prinsip rasio tersebut.

   Pengiriman e-mail *spam* terdapat kepentingan individu yang dilanggar yakni terkait dengan pelanggaran privasi yang kemudian dapat dijadikan alasan bahwa pengiriman e-mail *spam* dapat dikriminalisasi sebagai sebuah kejahatan *cyber* tersendiri.

d. Adanya kesepakatan sosial

   Kesepakatan sosial di sini berasal dari pemerintah, dimana kriminalisasi merupakan ke-

wenangan pemerintah dalam rangka menetapkan sebuah perbuatan diatur sebagai sebuah kejahatan dalam Undang-Undang. Terkait dengan pengiriman e-mail *spam*, banyaknya pengaduan sebagaimana diuraikan sebelumnya, menunjukkan bahwa ada kerugian yang berdampak nyata di masyarakat secara sosial dan dapat dijadikan legitimasi pemerintah untuk mengkriminalisasikan pengiriman e-mail *spam* sebagai sebuah kejahatan *cyber*.

Mengkriminalisasikan pengiriman e-mail *spam* sebagai sebuah kejahatan *cyber*, dapat dilihat pula dari permasalahan yang ditimbulkan, khususnya bagi para pihak atau pengguna teknologi informasi yaitu;

Berdasarkan permasalahan di atas maka dalam pengaturan terkait pengiriman e-mail *spam* yang ideal didasarkan pada unsur perbuatan pengiriman e-mail *spam* tersebut yaitu unsur "*bulk*", "*unsolicited*" dan "*commercial*". Unsur "*bulk*" dan "*unsolicited*" sebagaimana dibahas pada sub bab sebelumnya belum dapat diakomodir di dalam UU ITE baik pada Pasal 32 maupun pada Pasal 33. Sementara unsur "*commercial*" berarti berhubungan dengan aktivitas jual beli online dalam transaksi elektronik. Namun dalam UU ITE Pasal yang berhubungan dengan transaksi elektronik hanya mengatur tentang penipuan yang berhubungan dengan penyebaran berita bohong dan menyesatkan.

Tabel 1 Permasalahan yang Ditimbulkan oleh *Spam* (Diolah kembali dari Evangelos Moustakas, C. Ranganathan dan Penny Duquenoy, 2005, 2)

Pihak atau Pengguna Teknologi Informasi	**Masalah terkait dengan *Spam***
Konsumen	- *Spam* bersinggungan pada karyawan dan privasi pengguna - "*E-mail harvesting*" dengan tujan untuk mengumpulkan alamat-alamat e-mail yang dikirimi e-mail "sampah" - E-mail biasanya berisi kode program berbahaya yang dapat merusak komputer atau jaringan komputer - Mencuri informasi penting konsumen seperti informasi kartu kredit - *Phising* (Pemalsuan Identitas)
Karyawan dan Perusahaan	- Waktu dihabiskan untuk menghapus e-mail *spam* tersebut - Tambahan biaya untuk biaya koneksi internet - Kehilangan produktivitas
ISP (Internet Service Provider)	- Biaya tambahan untuk mengembangakan infrastruktur anti - Biaya untuk extra bandwith dan extra penyimpanan untuk menghadapi jumlah *spam* - Kinerja bandwith yang buruk - Sistem Operasi (OS) yang rusak karena jumlah *spam* - Ketidakpuasan konsumen
Pelaku Usaha E-Commerce	- Kehabisan kepercayaan konsumen - Pengeluaran yang terlalu berlebihan - Produk abal-abal (palsu) yang menggeser keunggulan produk yang asli - Pembajakan software atau produk digital lainnya
Pemerintah	- Pelanggaran Netiket (Etika di Internet) - *Spam* dapat mengandung konten yang melanggar hukum (pornografi dll)

Pengiriman e-mail *spam*, gangguan privasi terkait dengan transaksi elektronik memang masih pada tahapan promosi, namun dapat diatur dimana gangguan data atau sistem elektronik kemudian dihubungkan dengan proses pengumpulan data konsumen tanpa ijin atau melanggar privasi konsumen. Uraian pada tabel di atas pun dapat dilihat bahwa terdapat bentuk kerugian materiil dan kerugian immateriil. Penulis berpendapat, mengingat UU ITE merupakan satu-satunya peraturan perundang-undangan yang berhubungan dengan teknologi informasi, maka perlu diatur revisi terkait kriminalisasi pengiriman e-mail *spam*.

Penulis mengusulkan perubahan terkait pengaturan yang ideal dalam UU ITE tentang pengiriman e-mail *spam*, yaitu perubahan atau penambahan Pasal terkait kerugian konsumen dalam transaksi elektronik, penyebaran berita bohong tetap ada namun lebih menonjolkan unsur gangguan data dan sistem elektronik yang dapat menyebabkan hilang, rusaknya data konsumen sebagai unsur akibat konstitutifnya. Sehingga rumusan Pasalnya kurang lebih berbunyi sebagai berikut "*Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong atau informasi elektronik yang mengakibatkan berubahnya, hilangnya atau rusaknya data atau sistem elektronik dari konsumen dalam Transaksi Elektronik*."

Akibat konstitutif tersebut diatur untuk mengakomodir unsur phising yang dijadikan salah satu modus dalam pengiriman e-mail *spam*, sementara berita bohong atau informasi elektronik diatur sebagai salah satu unsur perbuatan mengingat *spam* memiliki unsur "*bulk*" dan "*unsolicited*", selain itu modus e-mail *spam* biasanya menggunakan header e-mail yang seolah-olah nyata sehingga penerimanya pun terjebak dengan e-mail *spam* tersebut (Evangelos Moustakas, Ranganathan dan Penny Duquenoy, 2005, 5). Perubahan dan penambahan Pasal ini setidaknya akan menjamin perlindungan privasi, khususnya dalam kaitan dengan pengiriman e-mail *spam* yang digunakan untuk promosi namun justru berbentuk pelanggaran privasi.

Penutup

Pengiriman *spam* biasanya bertujuan pada dua hal sebagai media promosi dan berbentuk "bom email" (*e-mail blast*) yang dapat digunakan untuk menyebarkan virus, sehingga merusak data atau sistem komputer target, selain kemudian adanya pelanggaran privasi dan pencurian data pribadi dari target.

Hukum pidana positif di Indonesia belum terdapat pengaturan secara spesifik mengenai pengiriman e-mail *spam*. Baik Pasal 32 maupun Pasal 33 UU ITE secara rumusan belum mampu mengakomodir unsur-unsur dalam *spam* yaitu "*bulk*", "*unsolicited*" dan "*commercial*". Unsur komersial yang diartikan transaksi elektronik berdasarkan UU ITE pun masih sebatas penipuan konsumen dalam konteks berita bohong dan menyesatkan pada Pasal 28 Ayat 1 UU ITE.

Diperlukan perubahan pada UU ITE khususnya terkait kriminalisasi pengiriman e-mail *spam*, khususnya dengan mengakomodir aspek *phising* dan pencurian data korban dalam hal promosi terkait transaksi elektronik. Perubahan atau revisi UU ITE ini akan memberikan jaminan perlindungan pada privasi pengguna internet di Indonesia, khususnya terkait dengan data pribadi dari para pengguna.

DAFTAR PUSTAKA

Buku

Chazawi, Adami dan Ferdian, Ardi., 2011, *Tindak Pidana Informasi & Transaksi Elektronik*, Bayumedia Publishing, Malang.

Dewi, Shinta, 2009, *Cyberlaw Perlindungan Privasi Atas Informasi Pribadi dalam E-Commerce Menurut Hukum Internasional*, Widya Padjajaran, Bandung.

Hamzah, Andi dan Marsita, Boedi D., 1987, *Aspek-Aspek Pidana di Bidang Komputer*, Sinar Grafika, Jakarta.

Lessing, Lawrence, 2006, *Code*, Basic Books, New York.

Prasetyo, Teguh, 2010, *Kriminalisasi dalam Hukum Pidana*, Nusamedia, Bandung.

Rosadi, Sinta Dewi, 2015, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Refika Aditama, Bandung.

Sitompul, Josua, 2012, *Cyberspace Cybercrimes Cyberlaw Tinjauan Aspek Hukum Pidana*, Tatanusa, Jakarta.

Sudarto, 1981, *Hukum dan Hukum Pidana*, Alumni, Bandung.

Suhariyanto, Budi, 2012, *Tindak Pidana Teknologi Informasi (Cyber Crime): Urgensi Pengaturan dan Celah Hukumnya*, Raja Grafindo Persada, Jakarta.

Widodo, 2012, *Hukum Pidana di Bidang Teknologi Informasi (Cybercrime Law): Telaah Teoritik dan Bedah Kasus*, Aswaja Pressindo, Yogyakarta.

Widodo, 2013, *Aspek Hukum Pidana Kejahatan Mayantara*, Aswaja Pressindo, Yogyakarta.

Widodo, 2013, *Memerangi Cybercrime: Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi*, Aswaja Pressindo, Yogyakarta.

Artikel dan Jurnal Ilmiah

Alazab, Mamoun, dan Roderic Broadhurst, 2015, *Spam and Criminal Activity*, *Trends and Issues (Australian Institute of Criminology) 2015* RegNet Research Paper No. 2014/44.

Chohwanadi, Hendry, 2012, *Urgensi Kriminalisasi Terhadap Ketentuan Pidana Tentang "Spamming" Dalam Hukum Pidana Di Indonesia*, Artikel Ilmiah Fakultas Hukum Universitas Brawijaya, Malang.

Clayton, Richard, 2007, *Email Traffic: A Quantitative Snapshot*, Makalah dipresentasikan pada Fourth Conference on Email and Anti *Spam* 2-3 Agustus 2007, Mountain View California.

Cockfield, Arthur, dan Jason Pridmore, 2007, *A Synthetic Theory of Law and Technology*, Minnersota Journal of Law, Science and Technology Vol 8 Number 2 Queens University.

Greenleaf, Graham, 2012, *Global Data Privacy Laws: 89 Countries and Accelerating,* Privacy Laws & Business International Report Issue 115, Queen Mary School of Law Legal Studies Research Paper No. 98/2012.

McCusker, Rob, 2005, *Spam: Nuisance or Menace, Prevention or Cure?*, Trends & Issues In Crime and Criminal Justice No. 294, Canberra.

Moustakas, Evangelos, Ranganathan dan Penny Duquenoy, 2005, *Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches*, Proceedings In Second Conference On Email And Anti-*Spam* (CEAS 2005).

Solove, Daniel J., 2003, *Identity Theft, Privacy, and The Architecture of Vulnerability*, Hastings Law Journal Vol. 54.

T Ngo, Fawn, dan Raymond Paternoster, 2011, *Cybercrime Victimization: An Examination Of Individual And Situational Level Factors*, International Journal of *Cyber* Criminology Vol 5 Issue 1.

Zavrsnik, Alex, 2008, *Cybercrime: Definitional Challenges and Criminological Particularities*, Masaryk University Journal of Law and Technology.

Peraturan Perundang-undangan

Convention *Cyber*crime 2001.

Directive *95/46/EC/ of the Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.*

The Statutes of The Republic of Singapore *Spam* Control Act Act 21 of 2007.

Undang-Undang Republik Indonesia Nomor: 10 Tahun 1998 tentang Perbankan.

Undang-Undang Republik Indonesia Nomor: 36 Tahun 1999 tentang Telekomunikasi.

Undang-Undang Republik Indonesia Nomor: 39 Tahun 1999 tentang Hak Asasi Manusia.

Undang-Undang Republik Indonesia Nomor: 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Republik Indonesia Nomor: 43 Tahun 2009 Tentang Kearsipan.

Internet

Adhi Nugroho S, Christian, Samsudi, Dwi Endah Nurhayati, 2013, *Kebijakan Hukum Pidana Terhadap Perbuatan Penyebaran Spam Melalui Short Messaging Service (SMS)*, www.repository.unej.ac.id (diakses pada 4 Maret 2015).

Andesma, Riyandi, 2013, *Wah Indonesia Masuk 10 Besar Negara Penghasil Spam*, www.techno.okezone.com (diakses pada 3 Maret 2015).

Boneh, Dan., 2004, *The Difficulties of Tracing Spam Email*, www.ftc.gov (diakses pada 27 Februari 2015).

Deliusno, 2016, *Begini Cara Peretas Curi Foto Bugil Jennifer Lawrence,* www.kompas.com (diakses 25 Maret 2016).

Diamond, Jeremy, 2015, *FBI Seized Tech from Home Linked to Celebrity Hack*, www.cnn.com (diakses 14 Maret 2016).

ID CERT, 2015, *Laporan Dwi Bulanan VI 2015*, www.cert.or.id (diakses 17 Maret 2016).

Nistanto, Reska K 2015, *Jumlah E-mail "Sampah" di Indonesia Meningkat*, www.kompas.com (diakses 21 Maret 2016).

Tanpa Penulis, 2009, *EU Study on the Legal Analysis of a Single Market for the Information Society New Rules for a New Age* www.ec.europa.eu (diakses 13 Januari 2016).

Tanpa Penulis, Tanpa Tahun, *Spam*, www.techterms.com (diakses pada 3 Maret 2015).